universität wien

MASTERARBEIT

Titel der Masterarbeit:

„The Digital Currency Phenomenon“

Verfasst von:

Rares Codrin PEICU BSc

angestrebter akademischer Grad

Master of Science (MSc)

Wien, 2014

Studienkennzahl lt. Studienblatt:	A 066 914
Studienrichtung lt. Studienblatt:	Masterstudium Internationale Betriebswirtschaft
Betreuer:	ao. Univ.-Prof. Mag. Dr. Karl Anton Fröschl

Acknowledgments

I would like to express my gratitude to everyone who has accompanied me through my studies at the university and assisted in the completion of this thesis.

I am grateful to my advisor, ao. Univ.-Prof. Mag. Dr. Karl Anton Fröschl, for the encouragement and guidance in writing this thesis, especially for his expertise and stimulating suggestions.
I would also like to thank Dipl.-Ing. Dr. Natalia Kryvinska for her guidance in finding the subject of this thesis and other organizational aspects.

Special thanks to my wife, Irina, who supported me tremendous in writing the thesis, and had enough patience and understanding during my work.
I am also grateful to my sister, Tamara, who helped me in proofreading the thesis, and for my parents who were very supportive during my studies.

Further, I would like to mention the Bitcoin community in Vienna, whose openness and friendliness provided me with many informations much needed in the research phase.

Vienna, 2014
Peicu Rares Codrin

Abstract

The rise of the internet as a global communication platform opened new possibilities of communication, and fundamentally changed the way people interact. In that regard, one of the most interesting developments is the rise of digital currencies, a fairly new phenomenon that promises to revolutionize the way we think about finance. This thesis will analyze the concept of digital currencies, focusing on Bitcoin, the most prominent digital currency to date. It will start with a brief history and definition of the concept of money, followed by a deeper analysis of digital currencies in general. The last two chapters of the thesis will focus on Bitcoin, describing in detail the currency and making an analysis of its strengths, weaknesses, opportunities and threads.

Keywords: *Money, History of Money, Definition of Money, Digital Currency, Virtual Currency, Cryptocurrency, Bitcoin*

Contents

1. Money

"*Money is what Money does.*"

F. A. Walker

Introduction

Money and the history of money is a fascinating subject. It is easily recognizable that today, money and the financial system are an essential part of our society and our economy.

Nevertheless, what money is, varied substantially over time, and it had gone through a dynamic process in order to become what it is today.

In this chapter I will overview money's main historical stages of development, go over the definitions in the literature, and review different types of money and its functions.

Barter Exchanges

Before the existence of any kind of money, it is assumed that any exchange of goods and services was conducted in barter transactions.

Barter is a way of making an economic transaction without using any kind of medium of exchange, but rather directly exchanging goods for goods and/or services for services.

Using barter as a way of conducting economic transactions is regarded as inefficient, because it raises the problem of the double coincidence of wants. The problem of double coincidence of wants arises because for a barter transaction to work, each trader has to need what the other is offering. Therefore it is quite improbable that the wants, needs or events that cause or motivate a transaction, to be occurring at the same time and the same place (Mill, 1848).

For example, if Tom wants to sell apples and to buy oranges, he will be able to carry out the transaction only if he finds someone that wants to sell oranges and wants apples in return.

Other disadvantage of barter is the absence of a common measure of value. In the absence of money it is difficult to find a way to measure the value of a certain good or service. In our example, it would be rather difficult to come to a common understanding of the value of an apple in terms of an orange, and therefore the values of apples and oranges cannot be effectively measured against each other.

The indivisibility of certain goods can also be a difficulty when doing barter.

If a person want to buy a certain amount of another's goods, but can give in return only an indivisible unit of a good which has a greater value, the transaction cannot occur as the unit cannot be divided. For example, if Tom wants to buy ten oranges but can trade only a horse in exchange, he will not be able to divide the horse in smaller units so it can have an efficient barter transaction.

If a society would rely only on barter exchanges, storing wealth for the future may be a problem, as many of the barter transaction would be conducted with perishable goods. Therefore another impracticality regarding barter is the difficulty of storing wealth. For example if Tom, after exchanging his apples with oranges, would like to store some of his wealth for the next winter, he will not be able to store the oranges, as they would get bad and lose their value in a short period.

Therefore, in order to resolve the challenges that barter poses, people started to use other forms of payment, and they invented money.

First Monies

According to "Money: A History" by Jonathan Williams, the earliest records of money can be found dating from roughly the third millennium BC in Mesopotamia and Egypt. This is the first time when historians have found the first usages of precious metals as a primitive form of money, mainly in form of bullions, a term traditionally describing gold bars, silver bars, or other precious metals bars. But, precious metals were not the only money around.

Several inscriptions depicting laws and debts show that everyday items, common jewelry or even grain could be used as a form of payment.

Bullions were still making the transactions quite difficult and therefore, in parallel, the government standardized the money and casted metal (typically silver) ingots of a uniform weight and quality. As silver and other precious metals were hard to obtain by most of people, the ingots were acquired mainly by aristocracy and wealthy people, and therefore their use was restricted to the upper class. In time, different regions created different shaped ingots, from the bronze dolphins shape in the Black Sea area, to the bronze spade money and bronze knife money in ancient China (Williams, 2007).

Gold and Silver ingots found in Egypt and Bronze dolphin made at the Black see (Williams, 2007)

One important aspect to be noted is that the material used as a payment would have an intrinsic value, i.e. would be valuable itself. For example, in Mesopotamia, when silver would be paid from one party to another, the metal would be weighted according to an agreed upon amount, and exchanged as payment. Because precious metals were in themselves valuable and were not subject to decay, gold and silver have become an effective way to make payments or exchange against goods and services.

At this point, the main problem was the limited amount of precious metal, and the uneven distribution of the metals across lands and kingdoms. The solution to this problem was the introduction in ancient Lydia around 600 BC of electrum coins, made from a more available and natural occurring alloy of gold and silver (Taylor, 2010).

In time, electrum coins were replaced again by gold and silver coins, probably because the wide spread of silver coins in the near-east and some problems regarding the irregular amount of gold/silver in the alloy.

These silver coins would be very popular in the Mediterranean area mainly because of the Greek influence at the time.

The Greek coins were probably the first form of money to be used on such a large scale and are regarded as the first money used internationally for trading between different countries. Before that, every country had its own medium of exchange, but with the expansion of the Greek empire and the conquests of Alexander the Great, the Greek coinage spread and become accepted on large territories (Taylor, 2010).

Electrum coins found at Ephesus (Williams, 2007)

History of Money - The Roman Empire

The next empire that followed Greek dominance over the Mediterranean area was the Roman Empire.

Not surprisingly, the nations that have managed to conquer a lot of territory and came in a position of military dominance, were the nations that dictated the economic and the coin standards.

As it grew in power and dominance in the Mediterranean world, Rome gradually developed its money from bronze coinage, to silver coins based on the Greek model.

It introduced a single coinage system for all the regions under the Roman Empire, and created three main coins: the gold aureus, the silver denarius and the bronze as (Williams, 2007).

Every coin would bare the face of the emperor, will be produced in the name of the monetary magistrates, and will be regarded as the official money of the Roman Empire.

Gold aureus, silver denarius and bronze as from 210 BC (Williams, 2007)

Before the roman coins, many coins had a chisel cut in, so that the amount and purity of the silver content (or other precious metal) can be verified and tested. What the Romans did, was to make the amount of precious metal contained in the coin practically irrelevant, as the coin was accepted everywhere in the roman empire, regardless of its purity. This marked a turn in the empire destiny, as they created fiat money, whose value was based upon the government authority and not the precious metal it was made from (Taylor, 2010).

The creation of fiat money allowed the Romans to gradually decrease the silver content of their coins without reducing their value. In time, this lowered the amount of silver in the coin to the point that in the third century the coin was only dipped in silver (Taylor, 2010).

At its lowest point, in the time of the emperor Tetricus, the amount of silver in a coin was no more the 0,5 % (Williams, 2007).

In addition, because of the vast size of the empire, large amounts of coins had to be produced, and it is estimated that the imperial budget in the second century AD was around 230 million denarii a year (Williams, 2007).

As a consequence, too many coins were created and inevitably inflation resulted.

To illustrate the inflation of the roman money, the wage of a Roman legionary soldier in the time of Julius Caesar (46 BC) was around 225 denarii, and by the time of Maximinus (235 AD) was 1800 denarii. The difference is not a result of a higher pay to a soldier, but rather the value of a denarius has decreased considerably.

This pattern of devaluation and inflation in large empires can be observed also in other cases like in the Middle East, China or the late British Empire (Taylor, 2010).

History of Money - After the Roman Empire

As the Roman Empire declined, the monetary infrastructure of the Romans was practically destroyed, the taxation system broke down, and the coinage replaced with local, mainly gold, barbarian coins (Williams, 2007).

After the splitting up of the Roman Empire, no other political entity has succeeded to control the Mediterranean area, and despite several attempts, no political unity and stability has been achieved for many centuries.

This lack of political stability had as a consequence, the inability to achieve a monetary unity and therefore the evolution of money had little progress in this part of the world. As Europe had fallen in the so-called dark ages, a common currency was not achieved for many centuries to come.

The western European states used mainly high value gold and silver for taxes, paying armies and giving to church. This was accessible to the upper classes only, and the lower classes returned to mainly barter exchanges.

Until the issue of a gold coin in the Italian provinces in the thirteenth century, Europe used silver pennies for transactions, but as the value of the pennies was low, they were not suited for international use (Williams, 2007).

In the case of the eastern part of the fallen Roman Empire, the Byzantium, they succeeded to create and maintain their own gold currency, called tremessis (also known as the nomisma or solidus) for one thousand years until the fall of the empire in the fifteenth century (Taylor, 2010).

They successfully maintained their currency for many centuries, and it was used for taxation, to pay the army, civil servants, buildings and ceremonies. They also had lesser denominations, called *follis*, sometimes made out of silver, but mostly of copper, that were used for lower value transactions (Williams, 2007).

History of Money - Paper Currency

In parallel with the Roman Empire, we can observe another very different development in Asia, particularly in China.

Starting from the usage of animal products, ornaments and metals as exchange medium, China developed a unique and forward thinking monetary system. With the rise of several dynasties, particularly Han and Tang, China succeeded to create a stable political and economic environment, and therefore they could develop a complex monetary system.

Under the influence of the Tang Dynasty (618-907), Chinese culture had experienced a so-called "golden age" and it has spread its culture and influence through East Asia, including their own monetary system. Moreover, the Kao-tsung dynasty (650-683) introduced a primitive form of paper money, with many hundreds of years before any other part of the world would create such an innovation (Taylor, 2010). The roots of paper money can be found in the receipts of deposit that merchants used in order to avoid carrying heavy amounts of coinage in large commercial transactions.

The introduction of this kind of money had an important effect on the whole economic system, as paper started to become more and more used, and started to replace coins.

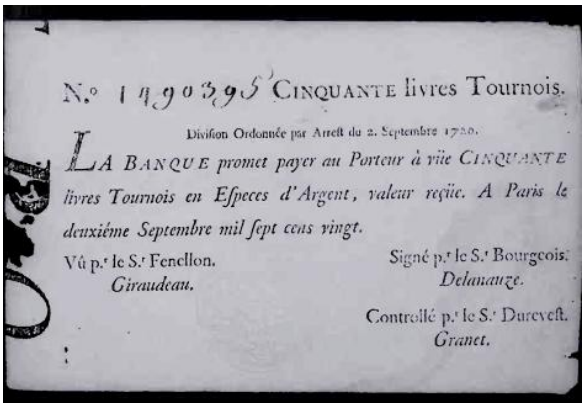
By the 13th century, under the influence of the Mongols, paper currency has become mandatory and coins were banned (Williams, 2007).

Similar to what happened to the Roman Empire, the problems of overissue and counterfeit destroyed the currency's value by inflation, and paper money lost eventually its dominance as a monetary system.

Coming back to Europe, as no political stability could be achieved, silver and gold bullion, rather than paper currency, became the standard currency.

There were a few attempts to introduce paper currency, like for example the Palmstruch's Banco of Stockholm in Sweden (1656) or John Law's Banque Generale in France (1716), but most of them ended up in inflation, and overall inhibited the introduction of paper currency in Europe (Williams, 2007).

There were nevertheless some local successes with introduction of paper currency without inflation, like for example in 1600s in Sweden and in colonial America in the 1700s (Taylor, 2010).


N.° 1790395 CINQUANTE livres Tournois.

Division Ordonnée par Arrest du 2. Septembre 1720.

LA BANQUE promet payer au Porteur à vûe CINQUANTE livres Tournois en Especes d'Argent, valeur reçûe. A Paris le deuxiéme Septembre mil sept cens vingt.

Vû p.r le S.r Fenellon. Giraudeau.

Signé p.r le S.r Bourgeois. Delanauze.

Controllé p.r le S.r Dureveſt. Granet.

Note for 50 Livres, issued by John Law's Banque Royale in France, 2 Sept. 1720 (Williams, 2007).

As money issued by banks was a new concept in the West, and there was no experience to draw upon, the first attempts were doomed to fail, but as time passed, paper money and different types of paper credit or bills of exchange became more circulated in society.

By the end of the 18th century, paper money produced by state and private banks was used in 20 countries around the world, and it would pave the way for a far more controlled and centralized financial system in the next two centuries (Williams, 2007).


Wiener-Stadt-Banco-Zettel,

Twenty five gulden note of the Wiener Stadt Banco, Austria 1762 (Williams, 2007).

History of Money - The Gold Standard

The gold standard means that a paper currency could be exchanged, on demand, with its value in gold. It was introduced in England in 1717, in America in 1792 and got to be generally accepted in Europe by the end of 1870s (Taylor, 2010).

As a result, a country could produce paper currency only if it were backed up by the appropriate amount of gold reserves. This was arguably the first primitive form of a universal currency, as gold fixed national money to each other and created a stable conversion rate between all major currencies of the world.

Before the First World War not every country was using the gold standard. Many countries, like South America and the Far East, used a less reliable silver standard, and tried to create a fixed gold/silver ratio.

By the end of the 18th century, Europe and North America were using the gold standard and the rest of the world the silver standard.

With the First World War, the gold standard was disrupted and would never fully recover. As countries needed money to pay for the war, they suspended the gold standard and started to print money that were not backed up by gold reserves. This led to high fluctuating rates and inflation, and was disastrous for countries like Germany and Austria, where hyperinflation reached unprecedented heights (Taylor, 2010).

After the Second World War, at the Bretton Woods Conference in 1944, a new initiative to stabilize world currencies began, in order to avoid the problems that followed the First World War.

Here the dollar was established as a replacement for the gold standard, and the world's currencies were fixed to it. To be more specific, under the Bretton Woods regime, the US dollar was pegged to gold and all other currencies were pegged to the US dollar. In addition, two institutions, the International Monetary Fund (IMF) and the World Bank, were created.

Nevertheless, because there was no centralized control over the interest rates, like the Bank of England in the case of the gold standard, and every country's currency was valued by international supply and demand, the system of fixed exchange rates established at Bretton Woods did not survive and in 1971 it collapsed (Taylor, 2010).

After the collapse of the Bretton Woods's system, the world currencies started to apply a flexible exchange rates.

History of Money – Modern Financial System

In the last 50 years, the financial world has gone through a rapid development. The relationship between credit and debit, double accounting systems, bond markets, insurance funds, futures and options, stock markets, and other financial instruments offered sophisticated tools for a fast growing and globalized economy.

At the same time, the communication technologies had gone through a huge evolutionary development, with the advent of long distance communication, electronic networks, and the World Wide Web.

Around the 1960s, as the paper-dependent commercial transactions posed problems in terms of speed, accuracy and costs, a group of railroad companies in USA started to develop a system to conduct financial transfers vie electronic data transmissions. Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) standards were developed and became standard protocols for electronic transmission of data and funds between financial institutions. Some examples of EFTs include electronic wire transfers, automatic teller machine (ATM) transactions, direct deposit of payroll, business-to-business payments, and tax payments (Patomäki and Heikki, 2007).

As the use of electronic devices (like computers and smartphones) started to be the norm in the developed countries, different financial instruments spread to the general population enabling them to access and manipulate money like never before. Services like eBanking or online bill payments created a new avenue for spending money and managing transactions.

This way, money migrated from physical paper in the hand of the consumer, to a digital representation in the electronic environment.

Today, only a small percentage of the money in circulation is still in a physical paper/metal form. Cash is used today only for relative small transactions, but the majority of money is in electronic form and part of the global electronic financial system.

The global electronic financial system refers to a worldwide framework between institutions and economic actors that facilitates the international transactions of funds (Patomäki and Heikki, 2007). It emerged as a part of the economic globalization movement with the development of international treaties, common standards, global regulation and the establishment of central banks (Lawrence et al, 2012).

As part of the economic globalization, in 1994 the World Trade Organization (WTO) was established, and took charge to promote and maintain international trade, and to smooth out restrictions on commercial financial services like banking services, securities trading and insurance services (http://www.wto.org, accessed 15.10.2104).

As a result of this movement, international financial integration grew substantially in the last 20 years, in terms of consolidating financial markets and banks, creating interdependent relations and abandoning strict regulation in favor of a more open economy.

Definition of Money

In order (to begin) to talk about money, we have to define the term and answer the question: **"**what is money?**"**

Money is a loosely used term, and can mean different things to different people. In this thesis I will use it from an economical point of view, in the sense economists use it.

The only way we will not refer to it is that of money being synonym for wealth. Money and wealth are not the same. A wealthy person could have a great deal of wealth but very limited amount of money, as he/she could diversify his/hers portfolio and invest money in assets.

There are many definitions of money, and none is regarded as a definitive one. Usually, economists generally define money by its functions.

We start by looking at the **"**Principles of Political Economy**"** by the famous British philosopher and political economist John Stuart Mill.

He describes money as following:

"money performs three distinct services, capable of being separated by the mind, and worthy of separate definition and explanation:

1. A Common Measure, or Common Denominator, of Value.

2. A Medium of Exchange.

3. A Standard of Value.**"** (Mill, 1848, p. 333)

We shall have a deeper look into this definition by analyzing the functions Mill proposed as the main services money should produce.

1. Common Measure

The function of a common measure, or a unit of account, means that money can be used to measure the value of goods and services. Mill puts it in perspective with an example: *"If a tailor had only coats, and wanted to buy bread or a horse, it would be very troublesome to ascertain how much bread he ought to obtain for a coat…as it is much easier to compare different lengths by expressing them in a common language of feet and inches, so it is much easier to compare values by means of a common language of dollars and cents***"** (Mill, 1848, p. 334).

In other words, the value of goods and services in the economy can be measured in terms of money, in the same way as one can measure distance in terms of meters.

2. A Medium of Exchange.

The second function refers to money as a medium of exchange. If the first function measures value, the second function transfers it.

Simply put, it means that money can be used to pay for goods and services. This is the function that resolves the big problem of barter, namely that if Tom wants to exchange his apples for oranges, he needs to find someone who searches for apples to exchange with oranges.

By using money as a unit of exchange, Tom can exchange apples for money, and then money for oranges, which increases considerably his chances for a successful economic exchange.

Other economists narrow the definition of Mill by limiting money only to the second function of a medium of exchange.
For example, economist F. A. Walker says:
"*Money is the medium of exchange. Whatever performs this function, does this work, is money, no matter what it is made of.... That which does the money-work is the money-thing*.**"** (Mill, 1848, p. 351)

3. A Standard of Value.
The third function of Mill's definition refers to money as a standard of value. That means that money can be stored and retrieved over time. Investopedia defines this function of storing value as **"**... *an underlying basis for any economic system, as some medium is necessary for a store of value in order for individuals to engage in the exchange of goods and services. As long as a currency is relatively stable in its value, money (such as a dollar bill) is the most common and efficient store of value found in an economy*.**"** (www.investopedia.com, accessed 3.07.2014)

Another good definition of money is the one of Geoffrey Crowther's, who sees money as **"***anything that is generally acceptable as a means of exchange and that at the same time acts as a measure and as a store of value* (Crowther, 1941, p. 35).
This definition includes all the three functions of money and adds the fact that money should be a commodity, which is generally acceptable by the community as payment. Although the main three functions described are agreed upon by the majority of economists, there are other possible additional functions.
Jan A. Bergstra summarizes additional functions that money can have. Adding to Mill, he lists the following functions of money. Money can be:

- a legal tender (means of payment of taxes and fines),
- a standard of deferred payment,
- a dimension used for expressions that occur in formal texts,
- an optimum of liquidity,
- a sign of political association or a means of communication.

(Bergstra, 2013).

Trying to think of money in terms of its functions can be a difficult task, and one can be inclined to be more specific.

What is money? Is one of its functions, all of them, or a combination of them?

In order to clarify these questions, I will analyze the problematic with regard to the two main theories about money in the literature.

There are different economic schools with different points of view and different definitions about what money is, but broadly we can differentiate between two basic theories that are at the root of all the others. These are the Orthodox or Metallism theory and the Chartalism theory.

Metallism theory

According to the metallism theory (also referred as the atomistic view), money naturally emerged as a solution to the issues that appeared with barter exchanges.

In the primitive economy, individuals wanted to exchange goods and services but were confronted with the obvious limitations of barter, mainly the double coincidence of wants. Over time, money appeared as a natural way of avoiding these problems and reducing transaction costs. Different societies chose precious metals as money in order for the currency to have intrinsic value, and later issued paper money only as long as it was backed by a representative amount of gold or silver.

From the metallism theory point of view, money is a medium of exchange and is seen as a commodity, or its value comes from the value of the backed commodity. As money are usually backed up by precious metal, hence the name metallism (Tcherneva, 2005).

Money is also seen as emerging from the private sector, not as a creation of the state, and its primary function is to facilitate market transactions.

To make sure that the weight and purity were standardized, the state produced stamped coinage certifying their correct value. Therefore the state is seen as supporting the will of the private sector by making sure the coins are trusted on their quality.

Chartalism theory

Chartalism stays in opposition with Metallism.

In simple terms, chartal money is the token for value, while metallist money is the thing of value itself.

The term Chartalism comes from the Latin Word "charta' meaning "token", and it describes money as representing a token for value, rather than having value in itself. More than that, the main point of the theory is that money cannot be correctly understood without considering the state as the main driver in their appearance. Money is seen as an abstract unit of account, which is then used as a means of payment and the settling a credit-debt relationship (Tcherneva, 2005).

Whatever is the nature of the money, being gold, silver of paper, its function is to be a medium of exchange created and backed by the state.

They argue that the age of "state money" was reached when the state monopolized the right to create money and to impose legal tender, i.e. taxes and debts must be paid in that currency.

Based on the chartalism theory, the Modern Monetary Theory (MMT) has emerged as a way to describe and analyze modern economies where the currency is fiat money created by the government.

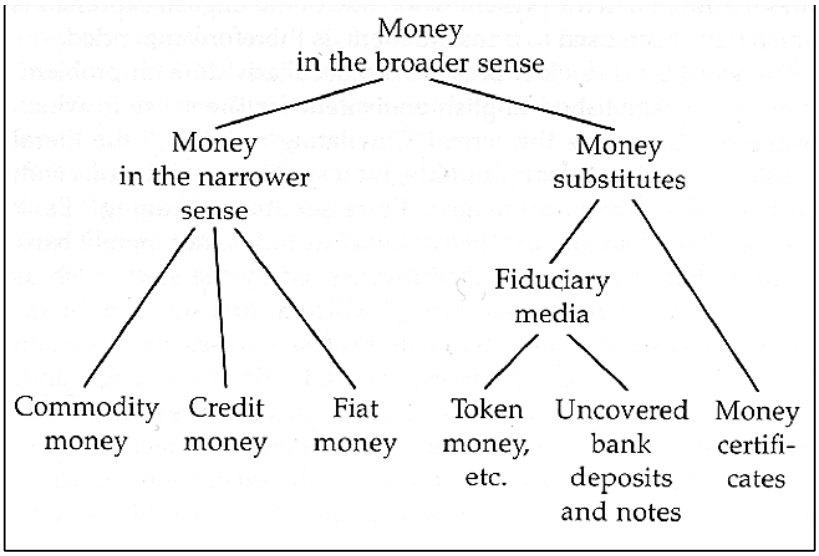
In MMT, money enters the economy through government spending, and is controlled by the power of the state to demand taxed and discharge debt. As the people have a constant tax obligation that has to be paid in the currency issued by the government, the state can maintain a constant demand for the currency, and coupled with private confidence and acceptance, the value of the currency can be maintained (Tymoigne and Wray, 2013).

To summarize, we can see money from two different points of view; first, as a medium of exchange evolved in the private market with the role of facilitating economic transactions and resolve the barter limitation; and from the second point of view, as a creation of the state, used as a means of payment and the settling a credit-debt relationship.

Classifications of Money

In **"***The Theory of Money and Credit***"** the Austrian economist Ludwig von Mises differentiates between (Mises, 1912):

1. Money in the narrower sense and,
2. Money substitutes



Mises's classification of money (Mises, 1912)

1. Money in the narrower sense is subdivided into:
   - **Commodity money**: money whose value comes from a commodity of which it is made. For example: precious metal coinage
   - **Credit money**: monetary claim against an individual that can be used to buy goods and services. For example: Bonds
   - **Fiat money**: derives its value from government regulation or law. For example: the Euro

2. Money substitutes is subdivided into:
   - **Money certificates**
   - **Fiduciary media**

They differ in the amount of the reserves backing them. The money certificates are 100% backed, whereas the fiduciary media are lesser backed.

Money can also be classified based on the basis of the material used to make it. Therefore we distinguish between (Vasudevachary, 2011):

1. Metallic Money and
2. Paper Money

1. The Metallic Money made from metal (Gold, Silver, Copper, Nickel etc.) and is under classified in different types:
   - **Standard Money**: is the principal coin of the country of issue, unlimited legal tender, and its face value is equal to its metallic or intrinsic value.
   - **Token Money**: is generally used for making smaller payments and serves as a subsidiary for standard money. The face value is higher than its intrinsic value and has limited legal tender power.
   - **Subsidiary Money**: similar to token money, they are used for smaller payments. Usually they are made of lighter metals.

2. The Paper Money is made from paper or other similar materials, and is classified in three types:
   - **Representative Money**: is fully backed up by precious metal reserves by the monetary authority.
   - **Convertible Money**: can be exchanged into its equivalent in gold and silver
   - **Inconvertible Money**: the monetary authority gives not guarantee that it can convert the money into its equivalent in gold and silver.

   (Vasudevachary, 2011)

Inside vs Outside Money

Another important way to classify money is by making the distinction between inside and outside money.

In order to understand the difference, we need to observe that the amount of physical fiat currency that is circulated today in a country's economy is quite small when compared with the amount of money that exist in other forms, like for example bank deposits and savings accounts. Added to that, even the small day to day payments tend to be made through some kind of electronic device,

like debit cards or credit cards, especially in developed countries.
Therefore we notice that the amount of physical money in form of bills or coins is only a small percentage of the total amount of money that is available. Money is, for the most part, no longer a physical thing, like a banknote or a gold bar. The common form we can find it today is in numbers in a computer system.
The majority of money today is distributed through a system of private banks, which primarily don't use physical money in their transactions, but rely on electronic transfers and accounting methods. This form of money is called inside money. To be considered inside money, these instruments must be convertible in the local fiat currency (like Euro or Dollar), accepted as payment for products, and transferable to others (Choi et al, 1997).
Inside money is the dominant form of money in the modern economy and, as the economy has become increasingly electronic, it has taken on an increasingly prominent role in the modern economy.
Although the electronic form is the most representative form of inside money, we can find under the umbrella of the term also other forms of inside money, like coupons, tokens, casino chips, stadium cards and prepaid telephone (Choi et al, 1997).
Another characteristic of inside money is the dimension of the territory in terms of transactional activities. Usually, inside money can be used only in the confinement where it is recognized and accepted as payment. As, for example, casino chips would be valuable only in the casino that issued them.

In contrast with inside money, the outside money is the fiat currency issued by the government that is used across the society, and has legal tender function. This includes cash notes, coins and bank reserves.
Although cash and coins have become more and more obsolete, they are still the most used type of money by the general population, especially in developing countries that don't have complex financial infrastructures.

Characteristics of Money

Money must have certain characteristics in order to be usable in everyday life. These characteristics depend on the complexity of the economy and the society.

Nevertheless, there are a few general characteristics that are important for a typical modern economy.

Therefore, the primary form of money in existence today resides in bank accounts as bank deposits

In order to function well, money should have the following characteristics:

- Durable. This simply refers to the physical quality of money. Being made of metal, paper, or other material, money has to be fairy durable when handled, and should not deteriorate when being used for a long period of time.
- Portable: Money has to be easy movable and easy transferable to other people.
- Divisible: Money should be easy to divide into smaller amounts. People should have the possibility to change it to smaller units in order to carry out small transactions.
- Uniform: All the bills and coins must have the same size and shape, and be recognizable as being the same currency. People should also be able to count and measure the currency.
- Limited supply. The more money that is in circulation the less it is valued by the economy. In order to maintain its value, money must have a limited supply.

To conclude, money represents one of the great human innovations. Starting from the limitations of barter exchanges, money rose as a way to enable humans to have better economic exchanges and to aid wellbeing. From its creation on, the concept and definition of money went through an evolutive process, from the primitive monies of Mesopotamia to the complex monetary system of the Roman Empire and the global financial system of today. Money played an important role throughout the history and is still very much part of the way the human society functions.

02. Digital Currencies

“There are 3 eras of currency: commodity based, politically based, and now, math based.”

Chris Dixon

Introduction

Money is a social institution created by man, and from its beginnings to the present day has demonstrated a capacity to adapt to the social and political environment. Depending on the circumstances, money existed in different forms and shapes, was made by different materials, and has been issued by different entities.

For a long time, money was issued by private actors, and governments did not have monopoly over the currencies. Around the nineteenth century, with the emergence of powerful nations in Europe, currency was standardized and legal tender status was controlled only by the government. Following into the twentieth century, practically every government would have its own currency that was issued and controlled by the state (Bal, 2013).

The government would publicly issue the money, give regulations to protect the currency, and develop fiscal policy to control and stabilize the economy. This was an important step forward to emerge from the fiscal chaos of the seventeenth and eighteenths century, and to create a reliable national economy. This centralization of money, among other circumstances, has helped to establish the modern framework that enabled the progress and prosperity that many people enjoy today.

However, with the development of technology and the emergence of the internet, the trend seems to have reversed, and private issued money started to have its comeback.

Although the centralization and the publicly issuing of money had brought much stability and growth, one could observe that it had also negative effects, like for example when a state starts to debase its own currency (Brodbeck, 2007).

In the last 50 years there have been a number of economists that studied the problems that arise when the state controls the issuing of money. They wrote articles and books about it, and offered different possible solutions to the problem.

In the 1970s, F. A. Hayek, an Austrian economist, wrote two influential papers: “Choice in Currency: A Way to Stop Inflation” (1976a) and “Denationalisation of Money” (1976b), where he argues against government’s dominate role in issuing money. In regard to currency, he proposes a move from centralized control of the government to a free market where every bank can create its own currency. In this way, by means of competition, only the strongest currency will maintain a strong purchase power and will become dominant (Hayek, 1976a).

Kevin Dowd, a British economist, in the book “The State and the Monetary System” (1988), makes the argument that if free competition works within the commodity market, it should work in regard to currency too. He also points out that the state, historically, has often debased their currencies and drove the economy down in order to follow political objectives (Dowd, 1988).

David Glasner, in his book “Free banking and monetary reform” (1989), argues with the classical economists about the concept that only a central monopolistic authority can supply money. He points out that in a free market competition, the private issuers will fight not to depreciate their currency and to maintain a high purchasing power. This would not necessary apply to the government, which main goal is to maintain the sovereignty, and not to sustain the currency (Glasner, 1989).

Lewis Solomon in the book “Rethinking our centralized monetary system” (1996) argues for a parallel independent private-issued currency that would exist along the state currency, as a way to make the system more flexible to the local needs, and less susceptible to system failures (Solomon, 1996).

All these works, among others, were a signal that the concept of private money was not a thing of the past, and it still was a viable option for the future of money.

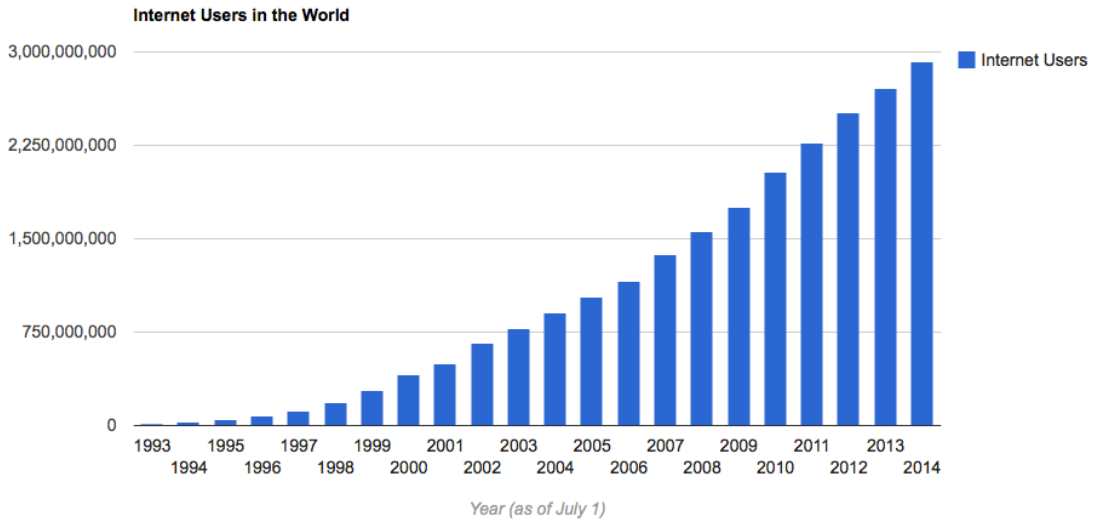
Technology

The development of the human race, in social and economic terms, can be influenced by many forces, but since the industrial revolution it seems that technology has had a unique role in pushing further the evolution of mankind.

In the development of technology lies one of the distinctive characteristic of humans, namely the capacity to innovate and create new structures, to find new ways of thinking, and new ways of acting.

Once a new technology appears and is embedded in the society, it can have a profound impact and can change old structures and patterns. On the other hand, it can be disruptive and destroy older technologies and older ways of doing things. One of the important innovation of the last 20 years is the rise of the internet and the World Wide Web.

The Internet is a world-wide computer network that can be accessed via a computer or a digital gadget with an internet connection. The growth and adoption of the internet had an exponential grow in the last 20 years, with less than 1% internet users of the world population in 1995, and reaching over 40% in 2014. The number of internet users is projected to will reach 3 billion users by the end of 2014 (www.internetlivestats.com, accessed 07.2014).



Growth of Internet Users (www.internetlivestats.com, accessed 07.2014)

The internet, as a technological innovation, has changed the way people interact, and opened new possibilities of communication.

This new way of communicating has reached deep in societies, and influenced several important aspects of our lives, including the way people interact, access information, and the way they make economic exchanges.

With the expanding reach of the internet, there has also been a proliferation of virtual communities of people with similar interests and goals. There are many types of virtual communities, ranging from social networks (Facebook, Instagram) to knowledge sharing communities (Wikipedia), virtual worlds (Second Life), forums (Reddit), to games and specialized information communities (WoW, Bitcointalk).

In these circumstances we can find the initial forms of virtual currencies, as different communities have created and circulated their own digital currency.

Definitions of Digital Currencies

The Financial Action Task Force (FATF) defines virtual currency as *"a digital representation of value that can be digitally traded, and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status in any jurisdiction."* (FATF Report, 2014, p.4)

In addition, FATF states that the fulfillment of the above mentioned functions is dependent of the agreement within the virtual community of users.

The European Central Bank (2012) proposes a different definition. In their view, a virtual currency: *"is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*" (European Central Bank Report, 2012, p.13)

The United States Government Accountability Office, in their report on virtual currency (May 2014), acknowledges that there is no statutory definition for digital currency yet, but still defines the term to refer to *"a digital representation of value that is not government-issued legal tender*."

(United States Government Accountability Office, 2014, p.4)

They follow to distinguish digital currency from U.S. dollars and other government-issued currencies, as ”*virtual currencies do not necessarily have a physical coin or bill associated with their circulation*”
(United States Government Accountability Office, 2014, p.4).
Lastly, they refer to the three main functions of money: *“while virtual currencies can function as a unit of account, store of value, and medium of exchange, they are not widely used or accepted*” (United States Government Accountability Office, 2014, p.4)

The latest published definition to be found comes from the European Banking Authority (July 2014). They define digital currency as "*a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*" (European Banking Authority, 2014, p.11).

Drawing on elements from all the definitions, we can say that a virtual currency is:

- a type of electronic money accepted by natural or legal persons;
- created by a private entity (private issued) and accepted by a community of users;
- can fulfill the three main functions that define a currency: medium of exchange, unit of account, store of value;
- is unregulated and does not have legal tender status in any jurisdiction;
- has no physical coin or bill associated with their circulation.

We should add that this definition is a temporary one, and may change with the development of the concept of virtual currency.

In the literature research, we noticed, there is not yet a defined common set of terms that reflects the different forms of digital currency. The most often used terms are *Electronic Money (e-Money), Digital Money, Digital Currency, Virtual Money* and *Virtual Currency*, but their meaning is still rather confusing.

I will categorize the several terms in two categories and define them as for their most common meaning in the literature.

The main difference between the terms is if we are talking about a publicly issued currency that is regulated and used as a legal tender, or a private issued currency, that is not regulated (or partially regulated) and is not used as a legal tender.

The following table defines the terms, as will be used in this paper:

Publicly Issued Currency	
Electronic Money (e-Money):	Represents traditional currency in a digital form. (for example Euros or US dollars)
Digital Money:	The term is used as a synonym for Electronic Money.
Private Issued Currency	
Virtual Currency:	Represents a privately issued currency that has no legal tender status.
Virtual Money:	The term is used as a synonym for Digital Currency
Digital Currency:	The term is used interchangeable for Electronic Money and Virtual Currency. In this paper, we will use the term to refer to Virtual Currency.

Electronic money (also e-Money or digital money) are traditional currency in a digital format. They are issued by the government, are regulated and legal tender in the country of issue. The supply of money is fixed and controlled by the state (European Central Bank Report, 2012). Example: Euro or US dollar used to make online payments.

According to ECB and the Electronic Money Directive (2009/110/EC), Electronic Money "*is monetary value as represented by a claim on the issuer which is:*

- *stored electronically;*
- *issued on receipt of funds of an amount not less in value than the monetary value issued;*
- *accepted as a means of payment by undertakings other than the issuer."* (European Central Bank Report, 2012, p.16)

Digital currency (also virtual currency or virtual money) is a digital form of currency, issued by a private issuer usually within a virtual community.
Although a digital currency could fulfill some of the criteria used for the electronic money, there is one crucial difference:
In the case of electronic money, the link between the digital representation and the traditional money is preserved by a legal foundation, and the unit of account is the same as in traditional money.
In the case of digital currency, the law does not preserve a link between the currency and any form of traditional money, the unit of account is purely virtual and does not have a counterpart in any traditional type of currency. Therefore they have no state backing and are mainly unregulated (European Central Bank Report, 2012). Example: Bitcoin or Litecoin

We can summarize the differences between electronic money and digital currency in the following table:

Criteria	**Electronic money**	**Digital currency**
Format	Digital	Digital
Unit of account	Traditional Currency	Virtual Currency
Legal Tender	Yes	No
Legal Status	Regulated	Unregulated
Issuer	Publicly Issued	Privat Issued
Supply of Money	Fixed by the Government	Fixed by the Developer / Not fixed
Control and Supervision	Controlled by the Government	No
Possibility of redeeming funds	Guaranteed by the Government	Not guaranteed

European Central Bank Report (2012)

Classification of Digital Currencies

According to the European Central Bank 2012's report on Virtual Currency Schemes, we can classify virtual currencies into three types (European Central Bank Report, 2012):

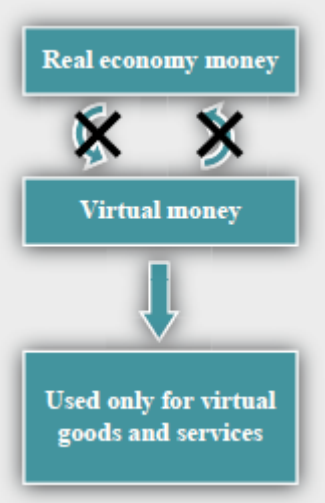
1. Closed virtual currency system
2. Unidirectional virtual currency system
3. Bidirectional virtual currency system

1. Closed virtual currency system

In the case of a closed virtual currency system, there is none or minimal link between the community that is using the virtual currency and the real economy. Another term used for this type is "in-game only" money (European Central Bank Report, 2012).

We can find this type of currency in virtual worlds or online games such as Massively Multiplayer Online Role-Playing Game (MMORPG). Usually users can earn, within the game, virtual money based on their performance, and then use them to buy specific items inside the game. The virtual currency can be used only inside the game and in theory it is not possible to trade it outside.

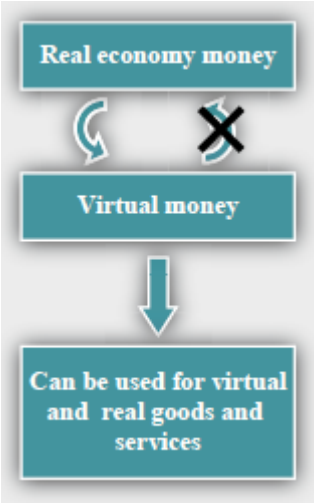
One example is World of Warcraft, an MMORPG that uses “WoW Gold” as its internal currency. World of Warcraft players can gain “WoW Gold” by playing the game, and then use the accumulated money to equip themselves for higher levels in the game.



Closed virtual currency system (European Central Bank Report, 2012)

2. Unidirectional virtual currency system

This type of system offers the possibility to purchase virtual money with real currency. Therefore a user could pay, for example, Euros via Paypal in order to get an amount of the virtual money. The particularity of the system is that, once you purchased the virtual money, you cannot convert them back into real money (European Central Bank Report, 2012).



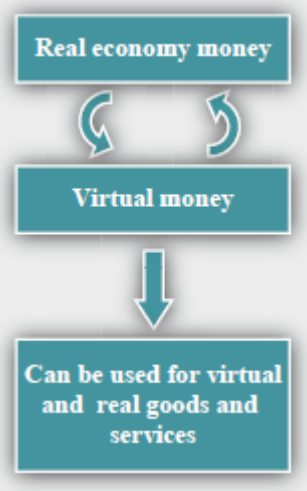
Unidirectional virtual currency system (European Central Bank Report, 2012)

This type of virtual money is usually used to purchase virtual goods and services, but may also be used to buy real goods and services. One example is the virtual currency introduced by Facebook in 2009, called Facebook Credits, that allowed its users to buy virtual goods on the platform.

3. Bidirectional virtual currency system

This systems offer the possibility to exchange from real currency to virtual currency just like any other convertible currency in the world.

A user can pay real money to buy virtual money, and vice versa, can pay virtual money to buy real money. The digital currency is used to buy both virtual goods and services, and real goods and services (European Central Bank Report, 2012).



Bidirectional virtual currency system (European Central Bank Report, 2012)

An example of this type of virtual currency is the “Linden Dollar” that is used in the virtual world Second Life. A Second Life user can buy Linden Dollars using real currency, use the currency on the platform, and then convert from Linden Dollars into a real currency, like the US Dollar.

Another example is the Bitcoin. One can use Bitcoin to buy virtual or real goods, and can exchange it against real currencies.

Centralized vs decentralized

Another way to classify digital currencies is by their degree of centralization.

Centralized digital currencies have an administrative authority that controls the systems. This entity establishes the rules of use and has the authority to withdraw the currency from circulation.

The exchange rate of these currencies can be either floating, i.e. determined by demand and supply in the market, or pegged, i.e. determined by the administrative authority (FATF Report, 2014).

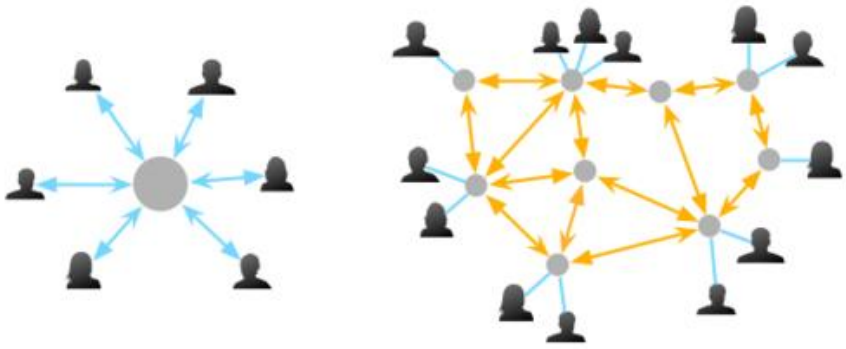
Most of the existing virtual currencies follow a centralized model, like for example: E-gold, Linden Dollars, WoW Gold.

Decentralized digital currencies, also known as cryptocurrencies, are based on different mathematical algorithms that have implemented a self-regulating mechanism.

They are usually open-sourced, distributed and have no central monitoring or supervision (FATF Report, 2014).

Validation and certification of transactions are performed by the network and do not require a third party to control the system as the algorithms are protected by cryptography that rely on public and private keys to transfer value.

Typical example of decentralized digital currencies are Bitcoin, Litecoin and Dogecoin.



Centralized vs Decentralized interactions (http://brucemacvarish.com/, accessed 12.10.2014)

Cryptocurrencies

The newest and arguably most advanced form of digital money is represented by a new class of currencies, called cryptocurrencies. As the name suggests, this type of currency relies heavily on cryptography and mathematical algorithms in order to function, but brings also other radical innovations to the protocol.

One could argue that the new wave of enthusiasm regarding digital currencies is based on the emergence of a wide range of new cryptocurrencies, and the front runner of all digital currencies: Bitcoin.

The concept of cryptocurrency emerged in January 2009, when an anonymous researcher or group of researchers going by the name of Satoshi Nakamoto published a paper detailing the new protocol. In this paper, he/she laid out the characteristics of the new currency and, as a proof-of-concept, created the first currency of this kind.

Although there are differences between different existing cryptocurrencies, they all share a few core principles. These include the fact that a cryptocurrency relies on cryptography to ensure the security of the protocol, is not controlled by any centralized regulatory institution, offers a high degree of privacy, the transactions are publicly available, the code is open source, and the creation of new coins is imbedded in the validation mechanism of the network (Nakamoto, 2009).

A more detailed analysis of cryptocurrencies in general, and of Bitcoin in particular, will be further discussed in chapter 3.

Characteristics of Cryptocurrencies

Decentralization

The nature of the open source protocol and the use of the network to validate the transaction are some of the most important characteristic of cryptocurrencies.

The system is self-regulated and does not require a third party, like an institution or a government. The transactions are processed by the network and the users are responsible for the security of their private keys.
The decentralization is to be seen as a way to protect against any use of the currency as a policy tool. This is important for the cryptocurrency community, and was one of the motivation behind the invention of Satoshi Nakamoto (Nakamoto, 2009).

No need for banks

As the users hold their coins on their private computers, the need to use a bank is bypassed. All the costs and limits related to the use of a bank are eliminated. Open hours, distance, waiting lines and fees can be skipped when using a cryptocurrency. One of Satoshi Nakamoto's argument for cryptocurrency was the protection against the fail of banks as we have seen with the financial crisis of 2008 (Nakamoto, 2009).

Lower Transaction Costs

The cost of transferring cryptocurrency is minimal. The transactions are easy, instant, and no more complex and costly as sending an email.
As everything is digital, there is no need for additional costs or fees related to the transfer of cryptocurrency. This makes it an ideal currency to be used for online transaction and e-commerce.

The ecosystem of digital currencies

The term "ecosystem" comes from biology and is relevant to gain knowledge of a phenomenon. In order to have a better understanding, instead of observing a single unit, it is better to analyze the environment and to see the interactions between the units.
In regard with the business world, James Moore coined the term "Business Ecosystem". He defines it as "*an economic community supported by a foundation of interacting organizations and individuals—the organisms of the*

business world. The economic community produces goods and services of value to customers, who are themselves members of the ecosystem.
The member organisms also include suppliers, lead producers, competitors, and other stakeholders" (Moore, p. 26).

The European Central Bank describes the market participants in regard with digital currencies as follows (European Banking Authority, 2014):

Users

A user has digital currency in order to purchase goods and services, to transfer value to another person, or as an investment.

Companies

A company receives digital currency as payment for providing goods or services.

Exchange

An exchange is an entity that takes digital currency in return for other forms of currency. Their role is to make sure that the digital currencies can be exchanged against fiat currencies or other digital currencies. Usually the exchange entity provides also information about the prices and volatility of the digital currencies.

Miners

In decentralized digital currencies, miners are people that use their computer processing power to validate transactions and create new blocks of currency. By validating the transactions in the network, they also increase the security of the system and bypass the need for a central authority.

Trade platforms

Trade platforms offer a market for buyers and sellers of digital currencies. Their role is to link together the buyers and sellers, and provide information about where the digital currencies can be used.

Wallet providers

A user can hold their digital currency on their local device, or can choose to use a wallet provider. A wallet provider offers the service of holding and administrating a digital currency wallet account. They provide an overview of the user transaction, ensure security and offer other additional services.

Inventors

Inventors are people that create the original concept of a particular digital currency. Usually, they promote and develop their invention by creating a service or a business around it.

Service Providers

Usually the service providers are in the technical area, and provide applications and software relevant to the use of digital currencies. There are also providers of hardware for mining purposes, or other related services.

Information Providers

Information providers use the internet to make available information related to digital currencies, and inform the general public about new developments.

Early Digital Currencies

At the time of this writing, there are approximate 420 different types of digital currencies that are operating in around 1300 markets (http://coinmarketcap.com, accessed 17.07.2014)

In the last 5 years, especially after the public success of Bitcoin, there has been an explosion of new digital currencies. Nevertheless, they were not as popular 10 years ago and did not even exist 20 years ago.

In the next pages I will present the early types of virtual money, and the precursors for today's digital currencies.

Digicash

Digicash was a company founded in 1990 by David Chaum, one of the founders of cryptocurrency. He was a mathematician and had worked for a number of years as the head of the cryptography department of the Centre of Mathematics and Information Science in Amsterdam. He has built a great reputation in his field, and is still regarded as one of the top scientist and developers of digital signatures, cryptography, online voting systems and anonymous communication. (http://money.usnews.com, accessed 21.07.2014)

In his work on Digicash, he created a cryptographic digital currency that allowed anonymous money transactions and put the base for the technology that is still used today. Digicash closed in 1998, and subsequently sold its assets to Ecash.

CyberCash

CyberCash was an internet payment service for electronic commerce founded 1994. The firm initially offered an electronic wallet software to consumers, and a software for credit card payments to merchants. Later "CyberCoin" was created, a digital currency used for micropayments. Although they had had a promising start, with a 79% rise in their stock on the first day of trading, the company was plagued by several technical problems, like hacking allegations and Y2K issues. The firm did not survive the dot-com bubble bust and ended their services in 2001. Its transactions business was sold to Verisign, the company that later was bought by Paypal (http://money.usnews.com, accessed 21.07.2014).

E-Gold

One of the earliest issuers of digital currency was e-gold, a firm that in 1996 created a digital currency that was backed up by gold. It was in use until 2007, and at its peak was processing more than 2 billion USD worth of precious metal transactions per year.

It is said to be the first wide spread digital currency, reaching 2 million accounts by 2002 and over 3 million by 2005. Nevertheless, it got a “bad reputation” as the company was haunted by allegation that the service was used for criminal activities (Samani et al, 2014).

The currency was in operation until 2007, when the US Department of Justice indicted the proprietors of e-gold on counts of violating money laundering laws (FATF Report, 2014). E-gold success inspired several imitators that created similar currencies like Goldmoney, e-Bullion, CrowneGold, Pecunix, and INTgold.

Webmoney

Webmoney was founded in Moscow in 1998, and had experienced a fast growth, first in Russia and then worldwide. According to their website, they reached more than 25 million users in 2014. (www.wmtransfer.com, accessed 17.07.2014)

Initially, the platform experienced the same allegations as e-gold, but following a change in practices in 2010 they avoided a similar "fate" and managed to remain in function (Samani et al, 2014).

At the time of this writing (2014), Webmoney offers users the possibility to conduct transactions using WebMoney units (WM-units) without needing a bank account or credit card. They also provide online financial services like P2P payment solutions, internet based trading platforms, merchant services and online billing systems (http://www.webmoney.ru/eng/about/, accessed 17.07.2014).

Beenz

Beenz started in 1998 a type of digital currency, where users would get virtual beenz points for performing different activities, like visiting websites or shopping online. Then, the user could use the currency to buy online to a number of partner online merchants.

The company managed to raise around 100 millions USD, but with the burst of the dot.com bubble it ended its activities in 2001. CNET counted Beenz among the greatest dot.com failures (http://money.usnews.com, accessed 21.07.2014).

Flooz

Similar to Beenz, Flooz.com was an internet venture started in 1999, which offered the possibility to purchase the online currency "Flooz" and use it to buy

products from partner online shops. The currency did not get enough adoption and was plagued by a series of credit card thefts and money laundering allegations. The company closed its business in 2001, and was perceived as one of the early indicator of the dot.com bubble bust (http://www.zdnet.com/flooz-com-collapse-linked-to-massive-credit-card-fraud-3002093922/, accessed 21.08.2014).

Internet Cash

InternetCash.com was a company started in 1999, which pioneered a secure internet payment system that was based on using PIN numbers to securely process a transaction without the use of a credit card. They also sold pre-paid cards with digital money that could be used to buy from partner websites.

Although the company managed to raise capital and developed a successful payment system, they could not survive the dot.com bubble bust and were forced to shut down in 2001.

Despite the failure, the business model of Internet Cash proved to be successful via other companies that used their concepts to build secure payment and credit card protection applications. (http://www.internetcash.com/, accessed 21.07.2014)

Liberty Reserved

Created in 2006 in Costa Rica, Liberty Reserved is famous because of its fall. It reached quickly more than 1 million users, but in 2013 was closed by an international investigation of the US federal prosecutors. It is alleged that Liberty Reserve was used to launder more than 6 billion US dollars for criminals, and the founders were sentenced for money laundering and operating an unlicensed financial transaction company (Samani et al, 2014).

Facebook Credits

Facebook is the largest social network in the world, with over 1.3 billion users and more than 600 million mobile users (http://www.statisticbrain.com/ accessed 25.07.2014).

In 2009 they introduced a new internal currency named Facebook Credits, which was supposed to be used by Facebook users to purchase items in games and non-gaming applications on the platform.

The value of a credit was equivalent to a 10th of a dollar and would be exchanged into 15 currencies. It was expected that Facebook will expend their currency to micropayment across the Facebook platform to be used in more than a million other application on the site, for access to certain features, music, videos or news articles.

In 2012, in an unexpected move, Facebook announced that they will not develop further their Facebook Credits system and that they favor the use of local currencies (http://www.nytimes.com/2010/09/23/technology/23facebook.html?_r=1&, accessed 25.07.2014).

Major Digital Currencies Today

Bitcoin

Bitcoin is the “superstar” among digital currencies.

Based on an innovative paper, written by pseudonymous researcher operating under the name of Satoshi Nakamoto, Bitcoin is the first widely successful digital currency based on peer-to-peer networking and cryptography. The supporters of Bitcoin argue that the cryptocurrency could make an ideal currency for mainstream consumers and merchants (Grinberg, 2011).

Bitcoin became famous in the world of financial news in late 2013 and early 2014 after its trading value rose from less than five US dollar cents in 2010 to 1.200 USD in 2013.

In February 2014, the biggest exchange platform for Bitcoin, Mt.Gox, failed to secure the bitcoins they deposited and filed for bankruptcy. This was followed by another wave of media coverage, and Bitcoin and digital currencies became a topic of intense debate on the internet and in the public media.

At the time of this writing (2014), Bitcoin is valued to over 600 USD and has a market capitalization of over 7.8 billion USD (http://coinmarketcap.com, accessed 24.06.2014).

Litecoin

Litecoin is seen as the successor of Bitcoin, as is based on the same peer-to-peer cryptocurrency protocols.

As Bitcoin, Litecoin creation and transfer is based on an open source protocol and is decentralized. It is seen as bringing some improvements over Bitcoin, like better and cheaper mining possibilities, faster generation of blocks, and the total amount of units is 4 times greater (https://litecoin.info, accessed 24.07.2014).

Among the digital currency communities, if Bitcoin could be seen as gold, then Litecoin would be silver in comparison, as it is easier to mine and there are larger quantities to be created. As of 2013, Litecoin had received extended coverage by mainstream media, and is presented as an alternative to Bitcoin.

At the time of this writing, Litecoin is the second-largest cryptocurrency by market capitalization with 247 million USD, and is valued at 8.12 USD (http://coinmarketcap.com, accessed 25.06.2014).

Ripple

Ripple is one of the few cryptocurrencies that does not use the mathematical cryptography used for Bitcoin and the majority of other cryptocurrencies.

Founded by Chris Larsen and Jed McCaleb in 2013, the Ripple currency uses XRP, a math-based algorithm powered by a network of global computers. Because no person or organization controls XRP, the currency cannot be created, falsified, or duplicated (https://ripple.com, accessed 25.07.2014).

In order to counter abusive users who attempt to spam the network, every Ripple transaction destroys a tiny amount of the currency. This XRP security cost is insignificant to any normal Ripple user, and it should be able to stop any abusive use of the network (https://ripple.com/currency/, accessed 25.07.2014).

Presently (2014), Ripple had a market capitalization of just under 50 million USD and a price of 0,006 USD (http://coinmarketcap.com, accessed 25.06.2014).

Peercoin

Peercoin was invented in 2012, and is a cryptocurrency similar to Bitcoin but with several key differences.

Peercoin's original innovation is the proof-of-stake/proof-of-work hybrid system. This should address a problem of Bitcoin, namely that in the future, Bitcoin mining will require greater computational strength and produce fewer coins, thus lowering the incentive to mine and increasing the likelihood of a monopoly. With Peercoin, new coins are generated based on what the user already holds, thus making a monopoly less likely. The proof-of-stake system it is said also to use less energy to mine coins than Bitcoin (http://www.peercoin.net/, accessed 25.07.2014). At this moment (2014), Peercoin values 1.19 USD, and has a market capitalization of over 25 million USD (http://coinmarketcap.com, accessed 25.06.2014).

Legal Status of Digital Currencies

Because of the quick rise of Bitcoin, a digital decentralized cryptocurrency, governments were confronted with the task of reacting and trying to figure out how to deal with digital currencies, how to tax and regulate them.

Presently (2014), most countries do not have an official policy or stance regarding digital currencies, though governments are beginning to take notice of the rapid development of digital currencies.

Generally, the governments have reacted in particular to Bitcoin, but the attitude can be extrapolated to all the decentralized digital currencies.

Now (2014) At the time of this writing, Bitcoin is legal in most countries, with the exception of Vietnam and Iceland. Although there have been mixed messages and a clear statement has not been given, China and Russia also gave signs signal that they would regard Bitcoin as illegal. China banned banks and financial institutions from processing Bitcoin transactions, and the top prosecutor in Russia referred to Bitcoin as illegal (http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world, accessed 24.07.2014).

The attitude of most industrialized countries is to observe the development of the digital currencies and find a way to tax it. A few countries, like UK, Germany and USA, started to develop and implement taxing rules.

UK

Initially, HM Revenue & Customs (HMRC) recognized Bitcoin and other decentralized digital currencies as a voucher that required a tax on the value of the coins. After UK-based traders have threatened to move abroad, as the regulation made their businesses unprofitable, HMRC reconsidered, and in March 2014 they re-classified virtual currencies as assets or private money.

In this case the creation (or 'mining') of Bitcoin, the activity will generally be outside the scope of VAT as it does not constitute an economic activity for VAT purposes. Therefore income received by miners for related activities, will not be taxed (http://www.hmrc.gov.uk, accessed 24.07.2014).

Added to that, when Bitcoin is exchanged for a real currency, no tax will be imposed on the value of the digital currency. For retailers that will receive Bitcoins or other digital currencies, normal tax rates will apply at the sterling value of the currency at the point the transaction takes place.

In relation to corporation tax, income tax and capital gains tax, the rules of taxation will apply depending on the activities and the parties involved (http://www.hmrc.gov.uk/briefs/vat/brief0914.htm, accessed 24.07.2014).

Germany

In August 2013 Germany has recognized Bitcoin as “unit of account” and “private money”, and stated that they should not be seen as electronic money.

Under the German tax law, the commercial sale of Bitcoin is a “miscellaneous service”, and thus, needs to be taxed under German law.

This has as consequence that the commercial sale and trading of digital currencies like Bitcoin are to be subject to capital gains tax, just like any other trading activity. Nevertheless, if the Bitcoins are held for a longer period than a year, tax gains won’t be applied (http://www.bundesverband-bitcoin.de, accessed 23.07.2014).

For retailers who accept Bitcoin as payment, this decision imposes a double taxing during transaction: first, on the sale of goods and, second, when they want to exchange the Bitcoin into other currency.

United States

The United States has generally offered support to Bitcoin, at least at federal level. The United States Congress even held a hearing on the currency where prominent financial experts and Bitcoin community members participated and shared their expertise.

The IRS has produced in 2014 a guideline regarding the taxation of digital currencies, describing the applicability of existing taxes to transaction using digital currencies.

Based on a report by The Financial Crimes Enforcement Network (FinCEN) issued March 2013, the IRS acknowledges that, although it has no legal tender status, a virtual currency operates like a “real” currency. They also refer to it as a “convertible” currency, i.e. acts as a substitute for real currency and can be exchanged for real currency (Internal Revenue Service, 2014).

For federal tax purposes, virtual currency is not treated as currency that could generate foreign currency gain or loss, but is treated as property or asset.

A US taxpayer who receives virtual currency for goods or services, has to declare the fair value of the virtual currency in US dollars at the date of receiving. The fair value is to be determined by the exchange rate of the currency into US Dollars. If the taxpayer uses the virtual currency mainly for sale to customers in a trade, then he realizes ordinary gain or loss on the exchange. The virtual currency can also be seen as a capital asset, similar to stocks and bonds, and in that case, one can realize capital gain or loss in the sale or exchange of the currency. Also, for a taxpayer that mines digital currencies, the fair market value at the date of receipt is seen as gross income (Internal Revenue Service, 2014).

Criminal Investigations of Digital Currencies

Since its appearance, the technology of digital currency, and in special cryptocurrency, has gained popularity through the general public as a way to transfer wealth and for electronic commerce purposes. As with any technology, digital currencies can be subject to both useful practices as well as malicious uses. Since the first tryouts of digital currencies, the phenomenon attracted actors seeking to exploit the experimental nature of the protocol, the vulnerabilities or the lack of clear rules of conduct (Heid, 2014).

Since the first digital currencies, like e-Gold and Webmoney, allegations and convictions of money laundering and other criminal activities has plagued the phenomenon and its development.

Criminals use the internet and other related technologies to distance themselves from any physical proximity to the illegal activities, and therefore profit from services like virtual banking, electronic money transfer, online purchasing and others. All this allows criminals to buy and sell without any direct contact, and using different methods they can make their activities hard or impossible to trace (Bryans, 2014).

With the emerging of cryptocurrency, the pseudoanonymity offered by the technology can be used as a shield for criminals under which illegal activities can be conducted.

Bitcoin, the major cryptocurrency today, allows every user to transfer money everywhere with minimal costs and maximum speed, while remaining practically anonymous and without leaving any paper trail behind.

Adding to that, the user of cryptocurrency can use pseudonyms and aliases, and if using secure channels like Tor, their presence is virtually impossible to backtrace (Bryans, 2014).

Therefore, the most valuable characteristics of the currency can be used also towards illegal activities, and financial regulators, government agents, and other fiscal enforcement agencies have become worried that financial crimes can be more easily engaged and much more difficult to combat (Ogunbadewa, 2013). For example, on 24 April, 2012, the Federal Bureau of Investigation (FBI) released a document expressing worries that the cryptocurrency Bitcoin will be exploited by criminals to launder money and other illegal activities (Federal Bureau of Investigation, 2012).

In March 2013, the United States Financial Crimes Enforcement Network (FinCEN) has issued a document to serve as a guidance against the damaging effects that can be caused by the operations using cryptocurrencies (Ogunbadewa, 2013).

The approach of FinCEN was to regulate the third-party services that play the role of money transmitters, i.e. which accept, transmit or exchange virtual currencies. Therefore, if a person wants to operate a business as an exchange between digital currency and real currency, it will have to register with FinCEN as a money transmitter. They will also be required to have special bookkeeping and reporting tools for transaction of more than 10.000 US dollars (Financial Crimes Enforcement Network, 2013).

In the last 10 years there have been a fairly large numbers of allegations and convictions related to money laundering and digital currencies. We will present a few examples of the most representative cases of criminal investigations (Federal Bureau of Investigation, 2012).

E-Gold

E-Gold was the first world-wide successful digital currency. Created in 1996, it offered a gold backed digital currency and came to process about 2 billion USD in 2008. After US regulations regarding currencies changed, the company was charged with illegal money transferring and money laundering. E-Gold accepted a plea bargain and all assets, all the gold and the digital currencies were seized by the US government, and later liquidated for around 90 million US dollars.

One of the e-Gold owner, after the shutdown of the company, started a new similar company called Liberty Reserve which encountered similar legal troubles(http://www.psmag.com/navigation/business-economics/digital-currencies-led-biggest-money-laundering-case-ever-bitcoin-74083/, accessed 31.07.2014).

Liberty Reserved

At the center of money laundering using digital money is Liberty Reserved, a company based in Costa Rica that was offering currency transfer and payment processing. The company allowed customers to easily open accounts, and

convert several national currencies into the digital currency called LR (Williamson at al, 2013).

In May 2013 Liberty Reserved was shut down, and according to US prosecutors, the enforcement action was the largest online money-laundering case in history. It is believed that in total there were conducted 55 million transaction with billions of dollars in volume and hundred thousand users around the world (http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=all&_r=0, accessed 30.07.2014).

E-Bullion

E-Bullion was a digital gold currency based in Panama. The company offered the possibility to open accounts with real money, convert them in digital currency, and then move them around the world while avoiding many banking reporting requirements.

In 2008 the company was seized by the US authorities and in August 2011 officials stated that the company was used for illegal money laundering activities (Williamson at al, 2013).

GoldAge

Created in 1999, Gold Age was a digital currency exchanger, working with digital currencies like e-Gold and e-Bullion.

In 2006, the owners of GoldAge have been indicted on charges of operating illegal money transmittal business by moving more than 30 million US dollars in digital currency around the world (Williamson at al, 2013).

Second Life

In 2012, the FBI assessed that criminal groups were using online gaming in order to launder money by purchasing virtual game money and transmitting them inside the game to other members of the criminal organization. One example is the Second Life's Linden Dollars that were seen as a source for criminals to perform various illegal activities, like money laundering or illegal gambling. Following an investigation in 2007, Second Life banned virtual

casinos in the game and upgraded the rules regarding potential uses of the virtual money for illegal activities (Williamson at al, 2013).

Silk Road

Silk Road was a sophisticated black market website offering a large palette of illegal goods and services, ranging from drugs, fake documents, computer hacking, guns to forgers and hit men contracts.

The Silk Road website was hosted in the so-called “cyber underworld”, also known as the "darknet." The particularity of the darknet is that it offers full anonymity and makes the transactions virtually impossible to backtrace.

This website was regarded by the FBI as "the most sophisticated and extensive criminal marketplace on the Internet today", and staked up to 1,2 billion US dollars in sales and about a million customers.

Silk Road was closed in October 2013 and the alleged founder was arrested. The FBI seized its assets, including 26,000 bitcoins worth about 4 million US dollars, and estimated that Silk Road's operator made $80 million in commissions (http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/, accessed 31.07.2014).

Although the website did not create a digital currency, nor was used for money laundering proposes, the transactions on the platform used Bitcoin in order to avoid leaving a papertrail, and therefore the case was connected in the media with the use of digital currencies for illegal purposes.

Related to the illegal platform, two individuals were arrested and accused of facilitating exchanging anonymously US dollars for Bitcoin in order to be used on Silk Road. They would advertise their services on Silk Road, receive the cash deposit in a bank and send Bitcoins to the customers in the same day.

Each of the two was charged on account of conspiracy to commit money laundering and of operating an unlicensed money transmitting business (http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR.php, accessed 31.07.2014).

To conclude, digital currencies represent the marriage between the concept of private money and the development of the electronic networks. Although it is a fairly new phenomenon, so far it has experienced a “bumpy road“, with many failed attempts to gain large adoption, many criminal activities allegation, and struggles with governmental regulation. Nevertheless, in the last 5 years, with the development of cryptocurrencies and Bitcoin, digital currencies have gained a new wave of interest, and a whole business ecosystem developed around them. In the next chapter we will focus on Bitcoin, the frontrunner of the digital currency phenomenon.

03. Bitcoin

"Bitcoin may be the TCP/IP of money."

Paul Buchheit

Introduction

The first proposal of anonymous digital currency dates from 1998 when Wei Dai, a member of the cyber punks electronic mailing list, published an article that sought to avoid the need for an intermediary between electronic payment transactions.

In his article, he proposed an architecture in which **"***untraceable pseudonymous entities [could] cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts***"** (Wei Dai, 1998, p.1). Therefore, he sought to create a currency that was free from government control or other third-party institutions.

Eleven years later, after the global financial crisis of 2008, a person, or a group of people, functioning under the pseudonym Satoshi Nakamoto, published a paper entitled **„**Bitcoin: A Peer-to-Peer Electronic Cash System**"**. Satoshi Nakamoto took further the idea of Wei Dai (further), and developed the theoretical framework for an anonymous online digital currency that relies on peer-to-peer technology for the management and distribution of payment transactions (Nakamoto, 2009).

Nakamoto presented the theoretical architecture of such a digital currency in a paper published in 2009, and as a proof of work (he) he/they applied the theory and created the first digital cryptocurrency: **Bitcoin**.

What is Bitcoin?

Bitcoin is *„a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution***„** (Nakamoto, 2009, p.1). It is also a pseudoanonymous digital currency that has no central control, is not backed by

any government or other legal entity, and is not redeemable for gold or other commodity. Because of its digital nature, a bitcoin can be very easily transferred to another computer by sending a packet of information, similar with sending an email.

The protocols used for transmitting bitcoins through the Internet use cryptography, therefore Bitcoin is proposed as a secure and efficient currency that takes advantages of the latest communication technologies.

The security of the transactions are accomplished through **"**cryptographic proof**"**, a tool that enables the network to guarantee the integrity and validity of the messages.

Furthermore, it is proposed that the structure of the network offers the possibility to have a perfect functioning digital currency without the need for any controlling authority or third-party institution. This feature of Bitcoin is fundamental to the philosophy behind the creation of cryptocurrencies, as one of the motives behind Satoshi Nakamoto**'**s paper was the banking system's failure to maintain a stable financial environment. He explicitly embarked on creating a currency that was not dependent on any government, bank, payment network, or clearinghouse (Nakamoto, 2009).

The lack of a central authority in coordinating transactions in the market has as consequence a dramatic decrease in transaction costs when comparing with other traditional currencies. Most of the transaction costs are arguably the fees paid to the coordinating authorities, and therefore it is proposed that Bitcoin can offer much lower transaction costs, as the coordination is managed by the network itself with minimal costs. The Bitcoin network offers *„an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party"* (Nakamoto, 2009, p.1).

Having no institutional authority to back it up, the currency doesn**'**t derive its value from regulation or state laws. The only value of a Bitcoin is based on supply and demand, i.e. what people are willing to pay for it.

The proponents of Bitcoin argue that the currency has valuable properties, like high liquidity, low transaction costs, micro-payment possibilities, and would be an ideal currency for the use in electronic commerce (Grinberg, 2011).

Terminology

As Bitcoin is a currency based on a new concept, there are some new words and terms that need to be defined in order to better understand of the phenomenon.

Bitcoin

Bitcoin - with capitalization, is used when describing the concept of Bitcoin, or the entire network itself; - without capitalization, is used to describe bitcoins as a unit of account. Bitcoin it is also often abbreviated BTC or XBT.

Bitcoin Address

A Bitcoin address is an identifier of 27-34 alphanumeric characters that consist of random digits and uppercase and lowercase letters.

The main purpose of a bitcoin address is to be used as a receiver of funds when sending bitcoins. We could compare it to an email address, and when Tom wants to send some bitcoins to Anna, he will use Anna's bitcoin address. Unlike emails, one bitcoin address should be used only for a transaction, and for the next transaction, a new address will be produced.

Addresses should not be confused with a wallet or an account. Its only function is to receive funds, as is the only information you need to provide for someone to pay you with bitcoins (https://bitcoin.org, accessed 11.08.2014).

Block

In the Bitcoin network, new data is recorded in blocks. A block is a record of the most recent transactions that have not yet been recorded in any prior blocks (https://en.bitcoin.it/wiki/Block, accessed 11.08.2014).

We could compare a block to a page in a notebook. On every page (a block) the last transactions are recorded and added to the notebook (the blockchain). Once a block has been written, it will never change nor be removed from the blockchain. Roughly every 10 minutes a new block is added to the blockchain through mining.

Block Chain

The blockchain is one of the main innovation of Bitcoin.

We can define it as a public record of Bitcoin transactions in chronological order. It is basically the collection of all the individual blocks, sorted by date.

The blockchain contains all the transactions and can be accessed at any time and by every user. In this way, one can find out how much value belonged to each address at any point in history. Therefore, the blockchain is used to verify transactions and to prevent double spending (https://bitcoin.org, accessed 11.08.2014).

Confirmation

Confirmation means that a transaction has been processed by the network. Transactions receive a confirmation when they are included in a block. Even a single confirmation from one node in the network can be considered secure, although for larger amounts people typically wait for 6 or more confirmations. Each confirmation exponentially decreases the risk of a reversed transaction (https://bitcoin.org, accessed 11.08.2014).

Hash Rate

The hash rate is used as (the) unit of measuring the processing power of the Bitcoin network. In order to mine new coins, the Bitcoin network has to process complex mathematical operations, and the hash rate represents the cumulative processing power of the entire network. For example 10 Th/s hash rate means that the network can make 10 trillion calculations per second (https://bitcoinwisdom.com/bitcoin/difficulty, accessed 12.08.2014)

Mining

Bitcoin mining is the process of using computational power to confirm transaction and increase security. Through mining transaction records are added to the blockchain in order to confirm them to the rest of the network. Each individual block must contain a proof of work to be valid, and in (the) case of Bitcoin, the network uses the hashcash proof-of-work function.

A secondary purpose of mining is to introduce new bitcoins into the system. For their computational power, miners receive a transaction fee, as well as newly created bitcoins (https://en.bitcoin.it/wiki/Mining, accessed 12.06.2014).

Wallet

The wallet is a secure and password protected software on a user's computer, used to transfer or receive bitcoins. It contains the user's private key which allows him/her to spend the bitcoins. The wallet also offers additional services, like showing the total balance of the coins in its possession, or exchanging coins for other currencies (https://en.bitcoin.it/wiki/Wallet, accessed 12.08.2014).

Peer to peer (P2P)

Peer-to-peer networking is an architecture that partitions tasks between peers. Peers make available a part of their resources, such as processing power, to the whole network without the need of a central coordination mechanism. Further, the system allows each individual to interact directly with the others. The Bitcoin network uses a peer-to-peer architecture so that each user is broadcasting the transaction of other users. Therefore no central control is required.

Cryptography

As Bitcoin relies to such a great degree on cryptography to secure the transactions, I will describe the main elements used in the system.

Henk van Tilborg in Encyclopedia of Cryptography defines cryptography as a discipline of writing a message in ciphertext with the aim of protecting a secret from malicious parties (Tilborg, 2005).

The general procedure to achieve this objective is to transform a normal text into a modified text, which is altered in such a way that it can be read only by using a "key" to unlock it.

Related to Bitcoin, there are three aspects of cryptography that are important (Piasecki, 2012):

1. Encryption and decryption
2. Hashing
3. Digital Signatures

1. Encryption and decryption

In cryptography, encryption is the process of encoding information from a so-called plain text into ciphertext in such a way that only authorized parties can read it. In such a scheme, the information, referred to as plain text, is encoded using encryption algorithms and generates ciphertext that can be decoding only by a special key. Decryption is the process of converting the ciphertext back into its original form, so it can be understood (Tilborg, 2005).

For Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the public record of the transaction.

2. Hashing algorithms

A hash function is used to map data of arbitrary size into short fixed length output strings. In cryptography, hash functions are used to verify that some input data matches a stored hash value in order to assure data integrity. If any part of the data is changed, then the hash function will not match the original generated hash, and therefore the changes would be revealed. A good cryptographic hash function will offer the certitude that the message wasn’t altered, as is impossible to have two different messages with the same hash, or to modify the message without changing the hash (Tilborg, 2005).

In the case of Bitcoin, in order to generate new bitcoins, the hashcash cost-function is used. Hashcash is a secure, efficiently verifiable cost-function or proof-of-work function. Using symmetric key cryptogaphy, typically either SHA1 or SHA-256, the hashcash function has no secret keys, does not require for a third party to manage it, and is fully distributed and infinitely scalable.

By using hash functions, Bitcoin blocks don’t have to contain serial numbers, as they can be identified by their hash, which serves the purpose of identification as well as integrity verification.

(https://en.bitcoin.it/wiki/How_bitcoin_works#Cryptography, accessed 11.08.2014).

3. Digital Signatures

Digital signature is a technique for demonstrating the authenticity of a digital message, by giving the receiver the assurance that a given entity has sent a certain message and that the message was not altered. Generally, the combination of a private key and the corresponding public key is used to authenticate the source and the integrity of the message (Tilborg , 2005).

The main cryptography scheme used by Bitcoin is the Elliptic Curve Digital Signature Algorithm (ECDSA), a variant of Digital Signature Algorithm (DSA) which uses Elliptic Curve Cryptography (ECC). The ECDSA works by creating a random private key that is used to sign messages and a corresponding public key used for checking the signature (Piasecki, 2012).

Each bitcoin is linked with the current owner of the ECDSA public key. When creating a new transaction, i.e. when you are sending someone bitcoins, you are attaching the coins to the new owner's public key, and then signing the message with the personal private key in order to authenticate the transaction. This way, when the transaction is published in the blockchain, everybody will know that the new owner of these coins is the owner of the new public key. The signature on the transaction verifies for everybody that the message is authentic.

This way, at any time, the transaction and the owner of the coins can be verified in the blockchain (https://en.bitcoin.it/wiki/How_bitcoin_works#Cryptography, accessed 11.08.2014).

How does Bitcoin work?

Satoshi Nakamoto defined an electronic coin as a chain of digital signatures involved in a transaction (Nakamoto, 2009). Therefore, a bitcoin should be understood only as part of a transaction, as it doesn't exist without being involved in a transaction. You cannot point to a physical or digital object (even

a digital file) and find a „thing" called bitcoin, as the coin is defined by the history of ownership transactions.

Therefore, in order to explain the way Bitcoin works, we have to refer to a transaction. In the context of Bitcoin, a transaction is a cryptographically signed record that reassigns ownership of a bitcoin to new addresses (https://en.bitcoin.it/wiki, accessed 06.10.2014).

Let's suppose Tom is the owner of a bitcoin and wants to transfer it to Anna.

As a typical transaction, he will send a message to Anna to transfer his ownership of the bitcoin to her. This kind of transaction poses a few challenges.

This digital transfer of ownership has two main problems that we need to overcome in order to have a successful transaction:

1) The problem of forgery

2) The problem of double spending

Bitcoin is digital money and therefore is data (i.e. a string of bits), and similar to other digital informations (like a digital picture) can be easily copied or multiplied.

How can we prevent Tom from using the same information over and over, and spend the same bitcoin multiple times? (the double spending problem)

Further, how can we prevent someone else to forge Tom's bitcoin? (the forgery problem)

In order to understand the solution of the Bitcoin protocol to these problems, we will to analyze further the architecture of a transaction.

1) The problem of forgery

In order to overcome the problem of forgery, we can introduce a digital signature that uses public and private keys for the authentication and verification of the integrity of the bitcoin.

Let's say Tom wants to send Anna the bitcoin. He will sent Anna the message: „*I, Tom, give Anna one bitcoin*".

Using his unique private key, Tom can create a digital signature that will authenticate him as the sender of the message. This way, Anna can be sure that the message is coming from Tom. This protocol establishes that Tom truly intends to give Anna one bitcoin, and in the same time protects the message

from forgery. Added to that, in the process of signing the message, Tom will link the current transaction with the old previous transactions of the bitcoin, and add it to the history of transactions involving that specific coin.

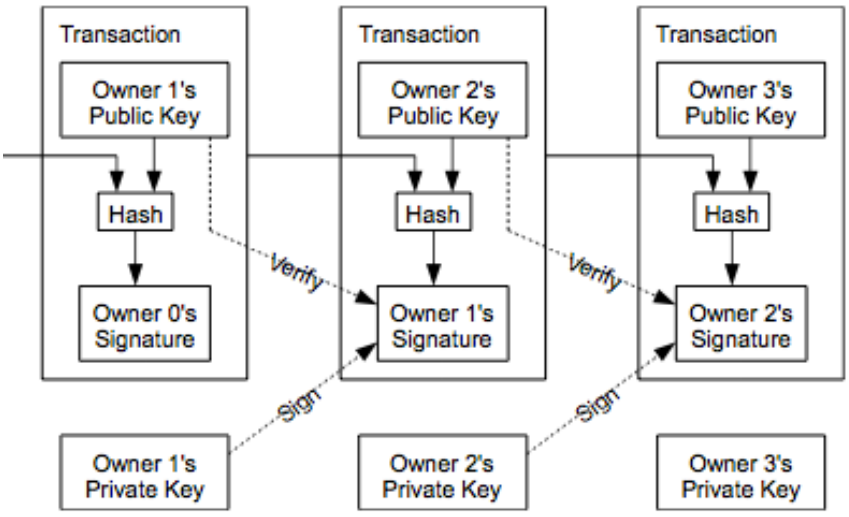
To generalize, each owner of a bitcoin can transfer the coin by digitally signing a hash of the previous transaction plus the public key of the next owner, and add these two informations at the end of the coin. Therefore the receiver of the bitcoin can verify the signature and the see the chain of ownership (Nakamoto, 2009).

For every bitcoin transaction we can distinguish two elements:

Inputs: records which refer to the information from other previous transactions and the current owner's signature. Every input must have a digital signature that unlocks the bitcoin to be spent. Only the person owning the bitcoin is able to create such a signature, and therefore it is ensured that funds can be spent only by their owner (https://en.bitcoin.it/wiki/, accessed 06.10.2014).

Outputs: records which determine the new owner of the transferred bitcoin. Each output must determine which Bitcoin address is the recipient and the new owner of the bitcoin.

For each new transaction of that bitcoin, the present output will be used to create the new input, and a new output will be created in order to assign the new ownership (https://en.bitcoin.it/wiki/, accessed 06.10.2014).



Overview of the transaction protocol of Bitcoin (Nakamoto, 2009).

2) The problem of double spending

In order to prevent Tom from sending the same Bitcoin several times (to double spend), we need to assign to each Bitcoin a unique label or a serial number. Then the message will be *„ I, Tom, give Anna one bitcoin with the serial number 123*".

Generally, this issue could be resolved by introducing a bank. The bank would provide serial numbers for the bitcoins, keep track of who has which bitcoin, and verify that transactions are legitimate. This would mean that Tom and Anna will both have to go through the bank in order to verify the authenticity of the bitcoin and transfer it.

The novelty of the Bitcoin system is that it eliminates the bank entirely from the protocol. This new concept is to make the whole network to overtake the role of the bank. If before the bank would keep the records of all the existing bitcoins and their owners, now this role is assumed by the whole Bitcoin network. The solution introduced by Satoshi Nakamoto was to make all the previous transaction available for the public. This way the participants in the network can agree on a single history of all the old transactions and add every new one to the list.

Each member of the Bitcoin network has access to the complete record of all the bitcoins and all the transactions. One can think of this as a shared public ledger showing all bitcoin transactions, which in our case is called the blockchain.

When Tom sends his bitcoin to Anna, this can be verified by asking the network to confirm the authenticity and validity of the transaction. For Tom and Anna's case, the users in the network will search the records and will verify if Tom is the owner of the bitcoin, and if the transaction can be carried out. The verification of the transaction in the network would be similar to Anna going to the bank and verifying if the bitcoin is owned by Tom and can be transferred to her.

Therefore, by receiving the validation from the network's nodes, Anna can be sure of the validity of the transaction, and accept to receive the bitcoin. Once the transaction is complete, then it is automatically added, as part of a new

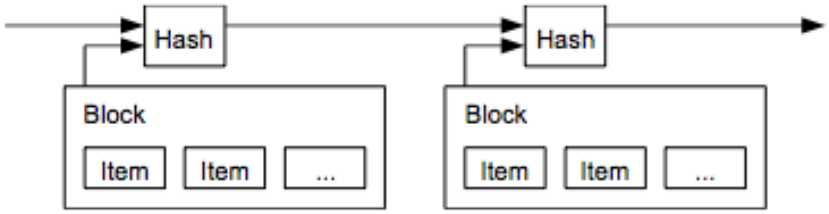
block to the blockchain, and becomes part of the public record of bitcoin transactions, at which point it is irreversible.

In order to maintain the integrity of the history of all the transactions, Bitcoin uses a timestamp server. This works by taking the hash from the previous transactions, add the current transaction, and create a new hash containing both the old and the new transactions (Nakamoto, 2009).

In regard to creating a unique number to assign to each bitcoin, the role of the serial numbers is resolved by using transaction hashes.

A transaction hash is like a digital fingerprint that is extracted from each transaction. Each bitcoin is then identified by a transaction, and exists only as a part of it. Therefore, we could say that there is no separate bitcoin at all, just a long series of transaction in the blockchain.

By using transaction hashes, the need for any central authority issuing serial numbers is removed, as they can be self-generated from each transaction.



Hash creation (Nakamoto, 2009)

The hashing functions in such a way, that each hash number is linked to the previous one, similarly to each block in the blockchain that is linked to the previous blocks. Therefore, it is possible to follow the chain of transactions back in the history until you reach the first Bitcoin transaction, also called the Genesis Block (https://en.bitcoin.it, accessed 11.08.2014).

Usually, SHA-256 hashes are used, and in order to increase the encryption they are computed twice (https://en.bitcoin.it, accessed 11.08,2014).

Example of double-SHA-256 encoding of string "hello":

```
hello
2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
9595c9df90075148eb06860365df33584b75bff782a510c6cd4883a419833d50
```

(https://en.bitcoin.it, accessed 11.08.2014)

Bitcoin: Proof-of-Work

In order to avoid certain schemes to manipulate the network and cheat the system, Nakamoto used the concept known as *proof-of-work*.

Based on a paper by Dwork and Naor, a proof-of-work protocol is used to deter the abuse of a certain service on a network by requiring the service requester to invest some work, usually meaning a computational process by a computer. It is important to be relatively costly and time-consuming to produce it, and trivial to check whether the invested work is valid (Dwork and Naor, 1993).

The concept used in the Bitcoin protocol is to make it computationally costly for the nodes in the network to validate the transactions, and in the same time to give a reward for processing them.

Making it computationally costly protects against manipulating the network, as validation cannot be influenced by the number of network identities someone controls, but only by the total computational power (CPU power) they can bring to bear on validation. With the growth of the network, the difficulty for a cheater rises as he/she would need enormous computational resources to cheat, making it impractical to try.

The computational power is used to solve a mathematical puzzle that is part of the validation protocol, and is necessary for the rest of the network to accept a transaction. For the Bitcoin, the proof-of-work involves computing for a value that when hashed, the hash will begin with a number of zero bits (Nakamoto, 2009).

Solving the puzzle is the target of every node in the network, but as the network is large and has a lot of computational power, the chances that a user will solve the puzzle and create a new block are proportional with the computational power invested.

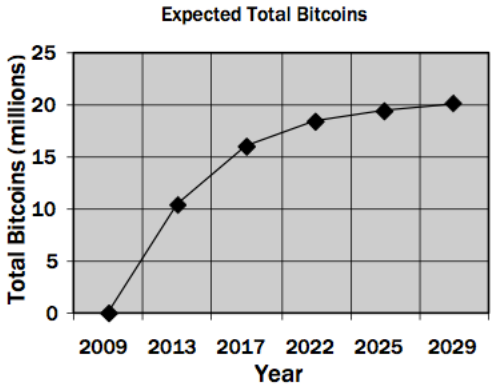
For example, if Tom invests 1% of the networks total computational power, his chances to resolve the puzzle are roughly one in one hundred.

Giving rewards keeps the users active in processing transactions and creating new blocks to be added in the blockchain.

For each block of transactions validated (called mining), the successful user (called a miner) receives a reward. The reward is given by creating new bitcoins and assigning them to the miner that solved the puzzle. This is also the way new bitcoins come in the system.

In 2009, for each block created the reward was set to be 50 bitcoins. For every 210,000 validated blocks (roughly once every four years) the reward is cut in half. This has happened just once until now, and to date the reward for mining a block is 25 bitcoins.

This process will continue every four years until 21 million bitcoins will be in circulation, and no more coins will be created (https://en.bitcoin.it, accessed 11.08.2014).



Supply of bitcoins curve (Grinberg, 2011).

Therefore, the proof-of-work protocol has three main roles:

- guards the network from being manipulated
- offers rewards as an incentive for the users to validate transactions
- inserts new bitcoins into the system.

To conclude, the Bitcoin system functions by using different concepts to resolve the challenges imposed by the nature of digital transfers.

A bitcoin is understood as a chain of digital signatures involved in a transaction. The nature of digital transaction poses two main problems: the problem of forgery and the problem of double spending.

In order to avoid forgery and maintain the security of transaction, Bitcoin relies on cryptography and digital signatures.

To avoid double spending without relying on a central authority, Bitcoin uses the network as a validation mechanism.

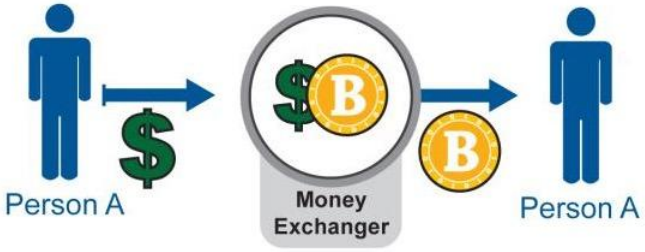
In order to guard against manipulation of the network and to create new coins, Bitcoin uses a proof-of-work concept to validate transactions, rewarding miners for taking part of the validation process, and in the same time supplying new bitcoins to the system.

Obtaining bitcoins

In order to obtain the Bitcoin, one can choose from three avenues (Plassaras (2013).

The first way is to use fiat currency, such as USD or Euro, to buy bitcoins. Like exchanging any other traditional currency, one can exchange real money to bitcoin by going to an exchange house that offers this service.

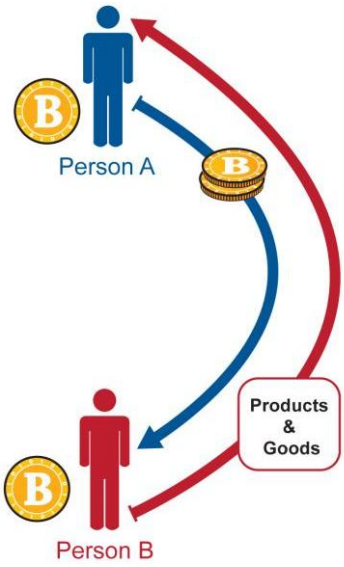
Like the traditional exchange markets, the price of Bitcoin relative to the other currencies is set by supply and demand.



Obtaining bitcoins through exchange

The second avenue to obtain bitcoins is to sell goods or services and accept Bitcoin as payment, or to receive a bitcoin from another user without giving anything in return.

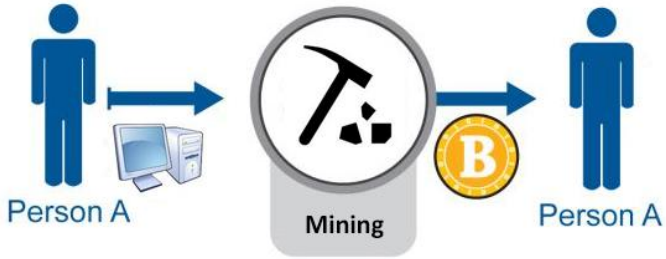
Such a transfer is simple and rapid, like sending an email. One important aspect of the transaction is the absence of any central authority to overview the deal. Doing that, one can take advantage of the low transaction costs and the speed of the payment process.



Obtaining bitcoins through transaction.

The third way to obtain bitcoins is to participate in the transaction network and use your computer computational power to verify transactions and create new blocks. As a reward, one receives transaction fees, and the newly created bitcoins that are distributed among the network.

The system is conceived in such a way that in order to create new bitcoins, the network has to be active in validating the transactions, and as a reward the miners receive the newly created currency. Essentially, the users are volunteering their machines to the Bitcoin network in order to receive a part of the new bitcoins, and the network is using the miners to validate the transactions.



Obtaining bitcoins through mining.

The system is conceived so that the difficulty of creating new coins rises with the number of miners. Usually miners are grouping themselves in mining pools

and collectively use their computational power to create new blocks and receives the rewards.

Valuation of Bitcoin

Bitcoin has no intrinsic value as it not backed by a commodity, nor has the backing of a central authority. Despite that fact, a growing group of people believe that the underlying Bitcoin technology has value, and therefore are willing to pay money for it. Therefore, we can say that Bitcoin has value because people think it has value.

In the future, the Bitcoin technology may be used for a different types of financial services like different forms of electronic payments, contracts, or distributed exchanges. Since Bitcoin is perceived as having this potential, it makes it valuable in the eyes of the investor.

Although the currency is not backed by any central authority and is not legal tender to any government, its value is supported by the individuals and merchants who use Bitcoin for transactions and payment for goods and services.

Therefore, if we can come to the conclusion that Bitcoin has a positive expected value in the future because of its potential to be a "revolutionary" technology, then we can understand why it is valuated.

The value of a bitcoin is generally driven by two groups of people: the people that use it for transaction, i.e. buying and selling goods and services, and the people that use it for speculative purposes in order to capitalize on the price chance. Combined, they both comprise Bitcoin's total monetary base. Based on the analysis of market transactions, it seems that the speculative investors have shown a particular interest to buy bitcoins for long term purposes, leading to a rise in the value and a larger monetary base.

Anonymity

One of the characteristics of Bitcoin is that it needs only a private and public key to transfer coins, and therefore offers a degree of anonymity to the user. As the public key is a string of letters and numbers, the identity of the user is not directly visible in the transaction.

But, in order to achieve a decentralized system, the whole history of the transactions has to be made public.

Although the identity of the persons making or receiving the payments is not directly linked with the transaction, the question arises of the degree of anonymity that a Bitcoin transaction can offer.

Reid and Harrigan analyze in their paper various possibilities to use different tools and approaches in order to associate public keys with external identifying information. Using passive analysis approaches like Integrating Off Network Information, TCP/IP Layer Information, Egocentric Analysis, Context Discovery, and Flow and Temporal Analyses, they conclude that the activity of users can be observed in detail.

Furthermore, active approaches can be successfully used to active deploy „marked" bitcoins to discover the identity of a certain user. Other relevant sources of information regarding the identities of the users can be extracted from centralized services such as wallet software and currency exchanges, which store data on the user's activity (Reid and Harrigan, 2013).

To conclude, for the user it is important to be aware that although Bitcoin provides no direct link between the transaction and its identity, the degree of anonymity is limited and, using different techniques, private information can be acquired.

The Ecosystem of Bitcoin

As defined earlier in this paper, an economic ecosystem is a community of interacting organizations and individuals that form relationships and create value for the whole community (Moore, 1996).

One important aspect to point out, is the fact that the network increases in value with the number of people using it. Similar with other networks on the Internet,

for example Facebook, the more people take part in the network, the more attractive it is for merchants to join, which attracts further users.
This is known as a positive network effect. With the number of users and merchants rising, the whole Bitcoin system benefits in several ways:

- more bitcoins are transacted
- more services are built around the currency
- more liquidity and circulation velocity is achieved
- the price becomes more stable, thus increasing customer confidence

Looking at the system we can distinguish different players that have different roles in the market.

Users

A user is a person or a company that uses bitcoins to purchase goods and services or to transfer value to another person.
Based on Holdgaard (2014), there are three main categories of users:

Normal users. These are the people that use the currency for transactions or storage, or just for the love of the technology.

Ideological users. These users have a strong political or ideological point of view in regards to the financial system and the government, and use the currency as a way to promote their views. We can name libertarians or anarcho-capitalists as an example for this type of user.

Gray users. These are the users that have taken advantage of certain features of the technology, in order to buy or sell illegal products or services. As an example we can name the Silkroad users or other similar services.

Holdgaard makes the argument that the early adopters of Bitcoin were represented in a bigger percentage by the gray users and the libertarians. The argument stands on the assumption that, as the Bitcoin system wasn't yet big

enough up to be used as a normal means of payment, the majority of users had different motivation for using bitcoins, like the anonymity for the lack of centralized control. As the currency matures and grows in size and adoption, it is fair to assume that the user base will switch from gray users and libertarians towards normal and regular users (Holdgaard, 2014).

According to an online survey from 2013, the "average" user of the Bitcoin system is:

- male (96%),
- 32.7 years old, libertarian / anarcho-capitalist (37%),
- non-religious (61%),
- with a full time job (43%),
- and has annual income of 50,000 USD and above.

They are usually interested in technology and have as top motivators curiosity, profit, and politics (http://simulacrum.cc/2013/03/04/the-demographics-of-bitcoin-part-1-updated/, accessed 21.08.2014).

Companies

In the context of Bitcoin, a company receives digital currency as payment for providing goods or services. There are different types of companies that are populating the ecosystem, and they offer different types of services or goods.

Wallet providers

Once a person has obtained bitcoins, he/she can store them on a personal computer or use an online wallet service. A wallet is a software used to store bitcoins. Using an online wallet to store bitcoins has advantages and disadvantages, but the main reason is that you can outsource the security of your coins to a professional. There are several wallet providers that offer a variety of additional services to the users, like offering the possibility to exchange bitcoins for other currencies, or guaranteeing different degrees of security.

Blockchain.info

Blockchain.info is one of the earliest wallet provider on the web and is known for its user-friendly website and its straightforward services. Unlike other web

wallets, the company lets the user get full control of the secret key for the Blockchain wallet, thus protecting against fraudulent activities (https://blockchain.info/, accessed 21.08.2014).

Coinbase

Coinbase is one of the most popular online web wallets. One distinguishing feature of the service is that you get a range of extra features. You can connect, for example, your wallet to your bank account and easily buy and sell bitcoins for your national fiat currency. They also integrate a range of different merchants, making it very easy to use the coins for different purchases (https://coinbase.com/, accessed 21.08.2014).

BitcoinWallet.com

BitcoinWallet gives the possibility to send or receive bitcoins as easily as sending an email. They bypass the problem of the long list of random characters that compose a wallet address, and offer the possibility to send/receive by using an easily recognizable address.

Payment Processors

The role of the payment processors is to make it easy for companies to accept payments in Bitcoin. They offer services like converting bitcoins into fiat currency or implementing software and web applications.

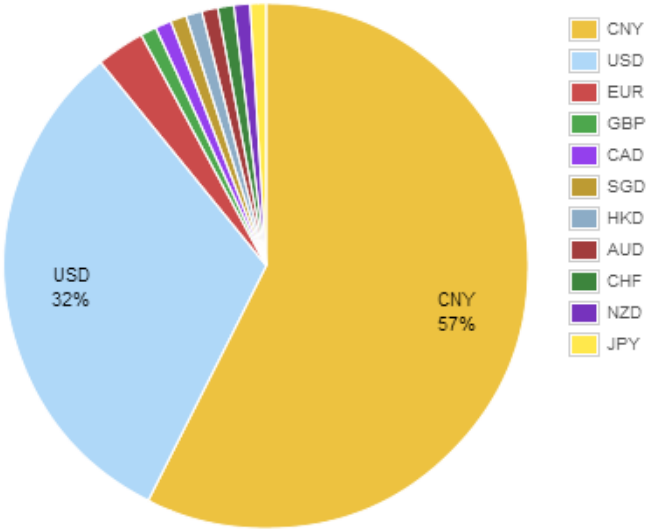
BitPay

Bitpay is one of the biggest payment processor in the Bitcoin ecosystem. They offer unlimited transactions, instant conversion to USD, daily bank deposits, retail POS solutions, eCommerce integrations, email support, no transaction fees, and access to all of BitPay's plugins, APIs, and apps (https://bitpay.com/pricing, accessed 12.08.2014).

Exchanges and Trade Platforms

An exchange platform is a firm that gives the possibility to trade bitcoins into other forms of currency. By using the exchange companies, one can buy or sell bitcoins against different local fiat currencies and vice versa. Increasingly, they

are offering a greater number of services, including a wider range of both fiat and alternative currencies, and various trading tools (http://bitcoincharts.com/, accessed 22.08.2014).



Distribution of currencies exchanged for bitcoins in August 2014 (http://bitcoincharts.com/, accessed 22.08.2014)

Until the end of 2013, Bitcoin exchanges were dominated by Mt.Gox, an exchange firm based in Tokyo that was handling 70% of all Bitcoin transactions worldwide. They suspended their services in February 2014 after announcing that around 850.000 bitcoins belonging to customers were missing from their accounts.

This opened the market for other companies to take over the exchange volume of bitcoins, and a new range of exchange firms rose to fill the void left by the Mt.Gox failure.

Bitstamp

Bitstamp is an exchange firm with a trading volume of 15.000 to 20.000 bitcoins per day. After the fall of Mt.Gox, they took the position of market leader in Europe where by using SEPA-transfers one can move money at low costs (https://www.bitstamp.net/, accessed 22.08.2014).

BtcChina

BtcChina started as China's first Bitcoin exchange with a small trading volume, but in time grew to be one of the largest exchange firms in the Chinese market. After Mt.Gox, they became the world's largest Bitcoin exchange by volume. They advertise themselves as the secure exchange platform that offers high liquidity, nonstop availability, and professional customer service (https://vip.btcchina.com/, accessed 22.08.2014).

Cryptsy

Cryptsy is a relatively new ”player” in the exchange market, and has seen in the last year a rapid growth in both customers and sales volume. They handle over 100 cryptocurrencies and offer a platform that is simple and easy to use. Although the firm plans to offer USD deposits and withdrawals soon, at the present time it is designed to act specifically as an exchange between cryptocurrencies (https://www.cryptsy.com, accessed 22.08.2014).

Bitfinex

Bitfinex is a trading platform, which offers high 'leverage' with margin trading and liquidity in return for a set interest fee. This kind of margin trading increases potential rewards, but also the risks. They offer different financial instruments like classical short/long orders or TR Swaps and Leverage Trading (https://www.bitfinex.com, accessed 22.08.2014).

Kraken

Kraken is a professional trading platform with all the finance features offered in the normal trading world. They offer one of widest ranges of advanced options for trading Bitcoin, Litecoin, Dogecoin, Ripples, and other digital currencies, which can all be traded against each other, or against USD or Euros. Kraken also features a sliding scale of fees, meaning that regular users who trade enough to hit the targets will get to reduce fees (https://www.kraken.com/, accessed 22.08.2014).

Winklevoss ETF

In order to make Bitcoin accessible for investors and people that buy stocks and bonds, there is a strong incentive to create exchange traded funds, or ETF's, so to make it safer and easier for the casual investor. At the time of this writing, the Winklevoss brothers are applying to create such a service, and if successful, would be a major step forward for the expansion of Bitcoin.

Hardware providers

Because mining is a demanding computational process, new specialized hardware has emerged in order to meet the high requirements. At first, the mining process used the CPU (computer processor) in order solve the block equations. After a short period of time it was realized that computer GPU's (graphic card processor) could be used to improve the mining process and work more efficiently. Further, a new mining hardware called FPGA came to the market, but after a short period of time it was replaced by ASIC technology, which is the leading hardware used today (http://www.topbitcoinmininghardware.com/ accessed 22.08.2014).

Butterfly Labs

Butterfly Labs was the first company to successfully provide mining equipment. They are specialized in FPGA & ASIC technologies, and provide different mining equipment like mining cards, mining racks, and even clouds mining solutions. They also offer consulting services in the fields of semiconductor design as applied to encryption, routing, security and digital signal processing (http://www.butterflylabs.com/, accessed 22.08.2014).

Spondoolies Tech

Founded in 2013 by a group of Israeli high-tech veterans, Spondoolies-Tech is a company specializing in cryptocurrency mining equipment. Their goal is to provide an infrastructure on which cryptocurrency will flourish, by creating mining rigs from the bottom up, and producing machines that are designed for efficiency and performance (http://www.spondoolies-tech.com/ accessed 22.08.2014).

KNC Miner

KNC Miner is a hardware company that offers complete upgradable modular ASIC mining devices specialized on Bitcoin and Litecoin. Their modular design adds several benefits to the standard services, like making management and upgrades easier, enhancing cooling efficiency, and making each cube very quiet (https://www.kncminer.com/, accessed 19.10.2014).

Mining Guilds

As mentioned before, miners are an essential component of the Bitcoin system, as they are necessary to confirm new blocks and to create new coins. As the computational power needed to create a proof-of-work increases with time in difficulty, the miners get together in communities, also known as mining pools, and work together to increase their chances of getting the rewards.

In time, two big "players" emerged in these communities: BTC Guild and GHash.IO.

BTC Guild

Being one of the oldest remaining Bitcoin pools, BTC Guild offers a very easy way to start mining. By simply joining the community, the user creates a profile, then selects a pool and start mining.

BTC Guild is a mining pool that uses PPLNS (Pay per Last N Shares) with a 2% fee. This simplicity makes a lot of people use the guild, and therefore has become very popular (https://www.btcguild.com/, accessed 22.08.2014).

GHash.IO.

GHash.IO. is at the moment the largest mining community with more than 180,000 users, and controlling 29% of the hashrate by the time of this writing. They offer instant mining payouts, stable hashrate, and live statistics, as well as trading possibility (https://ghash.io/, accessed 22.08.2014).

Communities

One crucial part of the Bitcoin phenomenon is the community that was created around the currency.

Composed of coders, developers, high tech enthusiasts, entrepreneurs, mathematicians, financial experts and economists, the community created around Bitcoin has played, and still plays, a very important role in maintaining and developing the currency. The community crystallized around a few Internet websites where the most important discussions and debates are taking place.

BitcoinTalk

BitcoinTalk was the first Bitcoin forum, started by Satoshi Nakamoto himself. The forum has more than 4 million posts, and is the most active Bitcoin community. One can find general discussions about the Bitcoin ecosystem, development and technical discussions, mining and hardware threads, economics and finance, as well as project developments and advertising campaigns (https://bitcointalk.org, accessed 22.08.2014).

Reddit's Bitcoin Community

The Bitcoin Subreddit is a highly active forum, with discussions on Bitcoin and related topics that are shared and then voted according to popularity. (www.reddit.com/r/Bitcoin/, accessed 22.08.2014).

Additional to the online forums and communities, several conferences and seminars have emerged around the world. The leading countries in organizing such events are the United States of America, Europe, and China (https://bitcoin.org/en/events, accessed 22.08.2014).

Foundations

Internationally there are several foundations that promote awareness on digital currencies and Bitcoin, and support the regulation of the new digital currencies.

Bitcoin Foundation

Bitcoin Foundation is the biggest international foundation that is dedicated to the development and promotion of Bitcoin. They try to reach out to the specialists in different areas that would help them to promote the expansion of Bitcoin, and to build a stable economic landscape. Their mission is to

standardize, protect, and promote Bitcoin (https://bitcoinfoundation.org/, accessed 22.08.2014).

Beside Bitcoin Foundation there are many local foundation created around Bitcoin that help to promote local awareness. For example, in Austria, there is the Bitcoin Austria Foundation that has regulatory meetings in Vienna and Graz and helps to promote and expand Bitcoin locally (http://bitcoin-austria.at/, accessed 22.08.2014).

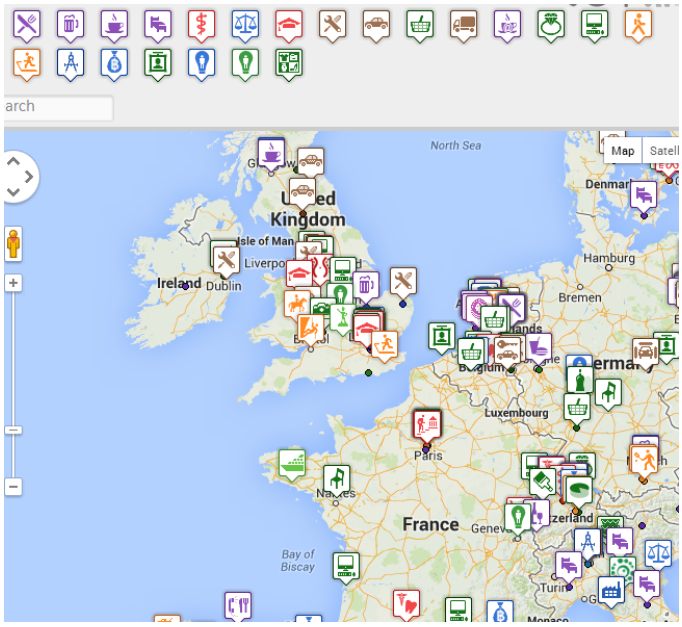
Marketplaces

For Bitcoin to become more than an investment or speculation currency, it has to work as a payment system that is practical and people can use it to buy everyday things. This area has seen a large growth in 2014 with a number of merchants, some of them retail „giants", deciding to accept bitcoins in exchange for goods and services (http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/, accessed 22.08.2014).

One of the easiest way to find merchants that accept bitcoins is via marketplaces and aggregator sites that gather large numbers of shops and companies that accept payment in bitcoins.

For example, *usebitcoins.info* offers the possibility to see stores and businesses that accept bitcoins, by showing them pinpointed on a digital map. Also *www.coinmap.org* offers similar applications that make it easy for everyone that wants to spend bitcoins. Other sites that display maps with real world shops are *Airbitz.com*, *Bitcoin.travel*, or *BitcoinMaps.org*.

Most of the firms that accept bitcoins are online e-commerce sites, but there is also an increasing number of off-line stores that accept payments in digital currencies.



Map with firms that accept Bitcoin in Europe.
(http://usebitcoins.info/, accessed 22.08.2014)

Regarding e-commerce sites, there are several major firms where bitcoins are accepted. For example Dell, Overstick, Newegg, CeX, CheapAir.com and Expedia. Adding to that, some popular e-commerce platforms, like Shopify and Digital River, have joined in providing digital currency as a payment option. There is also a wide range of physical stores that accept bitcoins, like retail stores, hotels, bars and restaurants. Bitcoins can be also used to buy services, especially web and technical services, on gambling sites, or on online auctions. Another use of Bitcoin that is increasingly popular, is to tip or donate to a cause, or to reward an interesting comment on the Internet.
Different campaigns and funding projects use Bitcoin and other digital currencies for their money raising efforts (http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/, accessed 22.08.2014).

Geographical Distribution

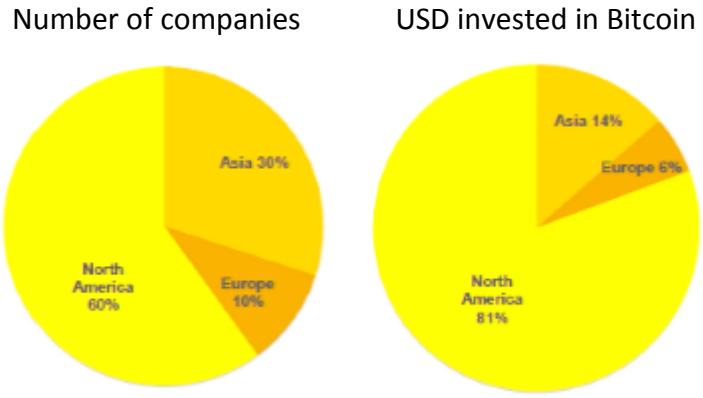
In order to have an overview on the geographical distribution of Bitcoin, we will analyze different aspects of the ecosystem created around Bitcoin and its geographical spread.

One of the key aspect maintaining Bitcoin's momentum in 2014 was the financial investment made by the venture capital community in Bitcoin and its surrounding ecosystem.

Based on the „State of Bitcoin 2014" report issued by Coindesk, Bitcoin features a relatively decentralized geographic investment footprint, with 60% of all Bitcoin Venture Capital companies based in USA, followed by Asia with 30% and Europe with 10% (State of Bitcoin Report, 2014).

Interesting to see is that although USA has around 60% of all the Bitcoin companies, over 80% of all new investment go to North America. Further, over 50% of all the money invested in Bitcoin goes in the Silicon Valley area, although only 27% of Bitcoin companies are located there (State of Bitcoin Report, 2014).

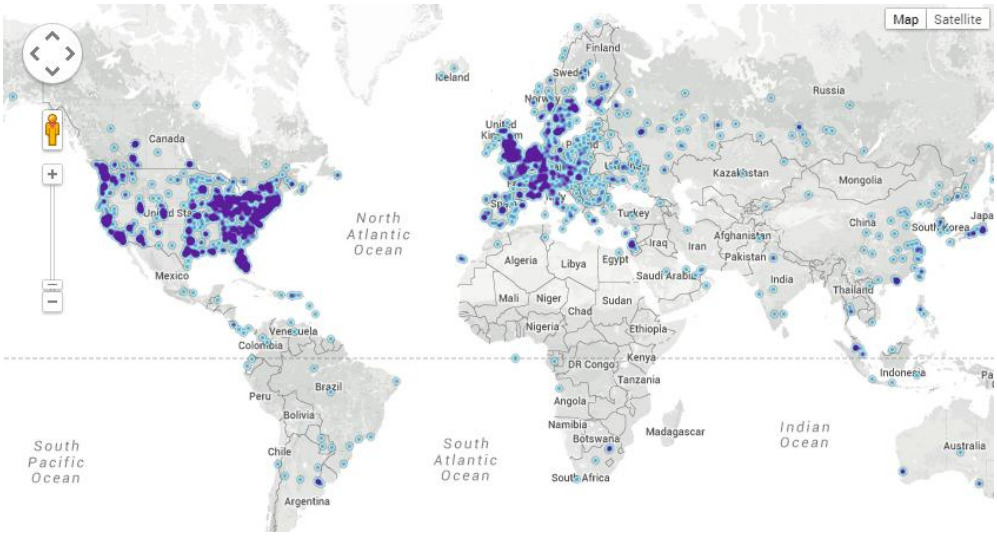
These statistics suggest that the biggest Bitcoin hub in regard to venture capital investment to date is Silicon Valley area in the USA, followed by Asia and Europe.



Number of Bitcoin companies and percent in 2014 Bitcoin investments by continent (State of Bitcoin Report, 2014).

Regarding to the Bitcoin network and the distribution of the nodes, by analyzing the statistics developed by Bitnodes, we can see that the main focal points of nodes are in the USA followed by different countries from Europe. The greatest number of available nodes are to be found in USA (2648 nodes) followed by Germany (545 nodes) and UK (455 nodes) (https://getaddr.bitnodes.io/, accessed 7.10.2014).

The data suggests that in terms of Bitcoin nodes, USA and Europe are the strongest hubs, followed by Canada and Russia (https://getaddr.bitnodes.io/, accessed 7.10.2014).



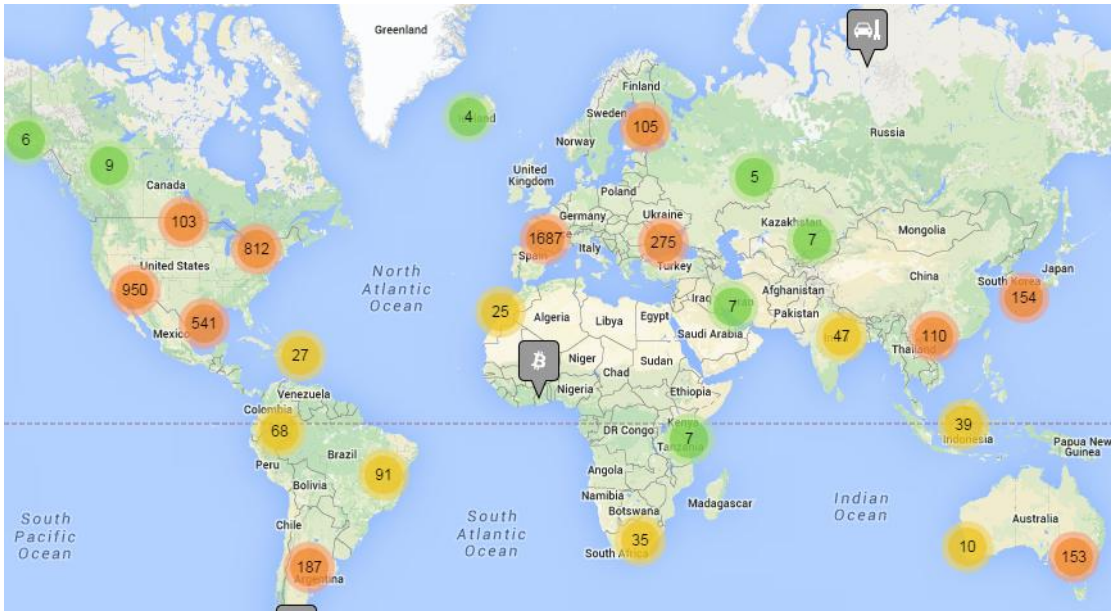
Geographical distribution of nodes (https://getaddr.bitnodes.io/, accessed 7.10.2014).

Top 10 countries with their respective number of reachable nodes are as follow.

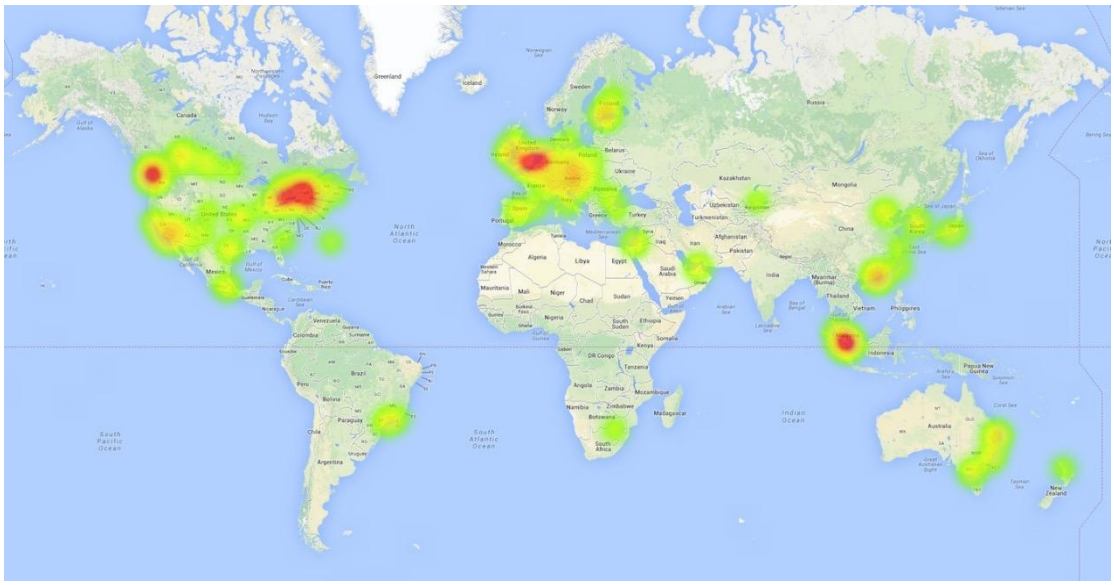
RANK	COUNTRY	NODES
1	United States	2648 (37.84%)
2	Germany	545 (7.79%)
3	United Kingdom	455 (6.50%)
4	Canada	396 (5.66%)
5	France	392 (5.60%)
6	Netherlands	318 (4.54%)
7	Russian Federation	270 (3.86%)
8	China	207 (2.96%)
9	Sweden	147 (2.10%)
10	Australia	139 (1.99%)

Top 10 countries in regard with reachable nodes
(https://getaddr.bitnodes.io/, accessed 7.10.2014).

Regarding the geographical distribution of the firms accepting Bitcoin as payment, we can see that the most concentrated zones are USA, Europe and Asia (http://coinmap.org, accessed 7.10.2014). Confirming the same pattern is the distribution of ATMs around the globe.

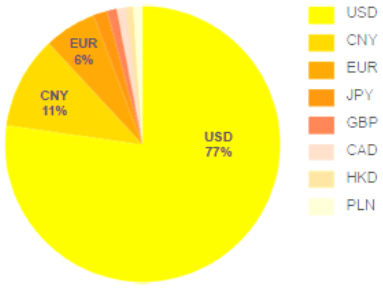


Distribution of firms accepting Bitcoin as payment (http://coinmap.org, accessed 7.10.2014)



Distribution of ATMs around the globe (http://coindesk.com, accessed 7.10.2014)

If we analyze the exchange volume distribution by currency value we see that over 75% of the exchanged Bitcoin were changed into US Dollar, followed by 11% Chinese Yuan and 6% Euro (State of Bitcoin Report, 2014).



Exchange distribution by currency (State of Bitcoin Report, 2014)

To conclude, we can say that the geographical distribution of Bitcoin is concentrated around United States of America, which leads in the number of firms accepting Bitcoin as well in number of nodes and ATMs, followed by Europe and Asia. The same pattern can be found also in regard to the most new venture capital investments in Bitcoin.

To conclude, Bitcoin is the biggest cryptocurrency to date. It is based on the theoretical framework developed by Satoshi Nakamoto, and has attracted a large community of adopters and developers around it. In order to function as a currency, it relies on a decentralized peer to peer networking, using cryptography to make it secure. To bypass the problems of forgery and double spending, Bitcoin makes the record of all transactions public, and relies on the network to confirm new transactions. The maximum number of bitcoins available is set to 21 million, which are created by a process named mining. Around the currency, a network of users, firms, exchanges platforms and mining equipment providers has grown providing many adjacent services and functions. The geographical distribution of the currency is distributed between United States, with the most firms accepting Bitcoin, followed by Europe and China.

In the next chapter we will analyze the advantages and disadvantages of Bitcoin, and try to find possible threads and opportunities for the future.

04. Analysis

Strengths. Weaknesses. Opportunities. Threats

Introduction

Digital currency is not a new phenomenon, but it has known a revival in the last years with the invention and development of cryptocurrencies in general, and Bitcoin in particular. We can say that nowadays cryptocurrencies are the most recent and innovative type of digital money, representing the front runner in the digital currencies world. From them, the biggest and well known cryptocurrency is Bitcoin.

In the previous chapters we went into detail regarding the concept of digital currency in general, and in particular Bitcoin, as the perfect example of the most established cryptocurrency to date. In this final chapter we will analyze the strengths, weaknesses, opportunities and threats of Bitcoin, as a representant for the whole digital currency phenomenon.

I will carry out a SWOT analysis for Bitcoin, and point out the characteristics regarded as the main strengths, the most controversial weaknesses, the positive scenarios that could be exploited in the future, and the elements that could harm or destroy Bitcoin.

Strengths

Payment freedom

Bitcoin offers the possibility to receive and send any amount of money anywhere in the world regardless of geographical borders, time zone, language, regulation or other limitations. The only requirements are access to the World Wide Web, and the skills to work with the Bitcoin software. This features are the main practical advantages of Bitcoin, as they offer new opportunities of transactions for people that in the traditional payment model could not fully make use of the system.

Transaction Costs

When it comes to cryptocurrencies, the low transaction costs is one of the most argued advantage. Usually, payments of Bitcoin have very low or inexistent fees. This is very attractive for merchants, who by having small fees to pay, can lower their prices and achieve competitive advantage. The absence of intermediaries and regulatory requirements are the main reasons why such low fees can be achieved (European Banking Authority, 2014).

For example, paying in Bitcoins has an average transaction fee around 1%, with the possibility to have it reduced to zero in exchange for a longer processing time. As the transaction is processed by the network, the higher the fee, the more priority it gets in the network and the faster is processed.

This could be the way the fees will be determined in the future, namely if you want to have a fast transaction you will have to pay a premium, if not, very low fees will apply. (http://www.coindesk.com/pros-cons-bitcoin-merchants-view/, accessed 31.07.2014)

To put it in perspective, at the time of this writing, transaction costs of PayPal range from 3% to 4% plus a fix fee of 0.30 US dollars, which in the case of small amounts (micropayments) can sum a fee up to 27%.

Other money transferring services like international bank transfer or Western Union have much higher rates.

The European Banking Authority makes the argument that the fees will increase overtime, as the number of virtual currency issued via mining will decrease and the network will migrate towards recuperating their investment of processing power from fees rather than from new issued currency.

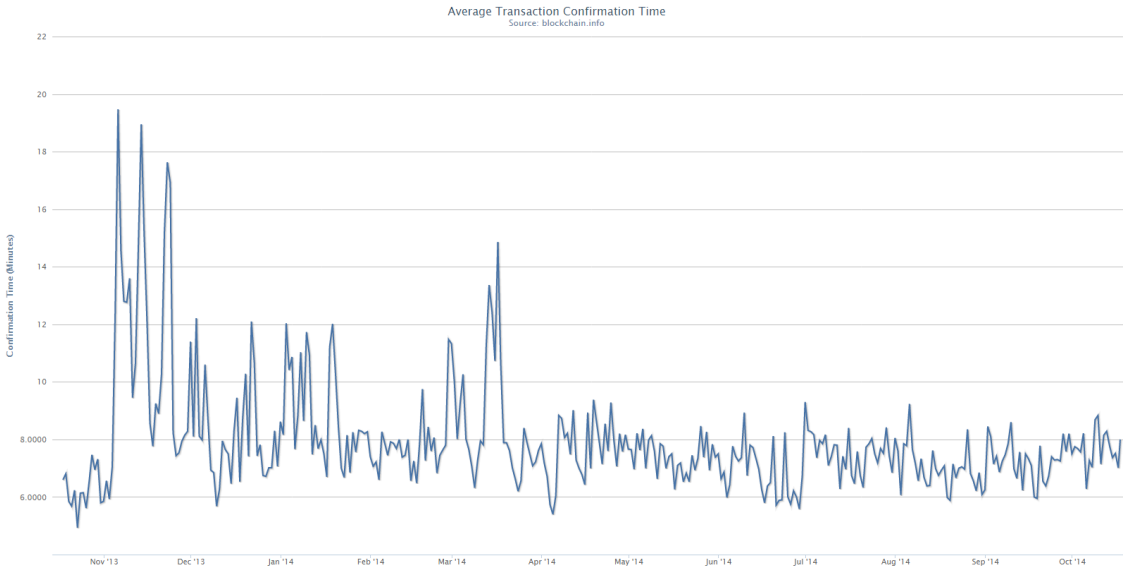
Adding to that, one should think also about the costs that will incur when changing the virtual currency into real currency.

Lastly, it is also projected that with time, new regulations and security measures will be imposed on the digital currencies and therefore the transaction fees will inevitably rise (European Banking Authority, 2014).

Transaction processing time

Using p2p networking, transacting virtual currency is clearly much faster than with traditional money. In comparison with credit card and bank transfers, the processing time of virtual currencies is much faster, with, for example,

between 10 and 60 minutes for Bitcoin. Bank wires in the same country take between one and three days, and between different countries could take up to weeks. This difference can be a great advantage for merchants and customers both, making the whole process much faster (http://www.servicecycle.com/advantages-of-using-digital-currencies/, accessed 31.07.2014).



Transaction time (2014) averaging at 8 minutes per transaction (https://blockchain.info/charts/avg-confirmation-time, accessed 17.10.2014)

Safeness and transparency

Credit card and bank transfer fraud has become a prevalent occurrence in day to day life on the internet. It is promoted that using Bitcoin, the risk of fraud can be bypassed. With no personal information being attached to the transfers, the risk of identity theft can be dramatically reduced, as the merchants will not store any sensitive information's (like credit card numbers) on their servers.

For example, Bitcoin transactions are publicly stored in the blockchain, and anyone can verify the transaction. However, no personal information is tied to the blockchain, offering protection for the customers.

Also, no hidden or extra fees can be charged without being noticed. (https://coinreport.net, accessed 31.07.2014).

Because of the way cryptocurrencies are constructed, all information concerning the transfer is transparent for everyone to verify and no individual or organization can control or manipulate it. This allows for the currency to be arguably neutral, transparent and secure (http://bitcoinembassy.ca/about/what-is-bitcoin/advantages-disadvantages, accessed 31.07.2014).

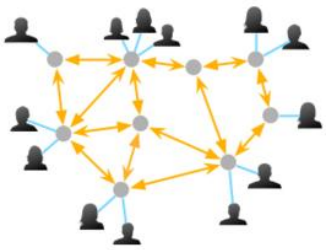
Anonymity

Bitcoin offers a degree of anonymity to the users involved in a transaction, as the identity of the user is not directly visible in the transaction. This means that unless users willingly link their identity with their public address, nobody can directly acquire it from the transaction. This increases the degree of privacy that a Bitcoin user has in comparison to traditional currency systems, where third parties have access to personal financial data.

As explained earlier in this paper, one should be aware that Bitcoin is not totally anonymous, as there are methods of analysis that can potentially discovery the identity of a user without his/her consent.

Decentralized architecture

Bitcoin it's a decentralized and open source digital currency that is managed by a network of computers on the internet, as opposed to traditional currencies that are controled by a central authority. The functioning of the currency is maintained by the network of nodes and the blockchain, a distributed public ledger that logs every bitcoin transaction. Some people see a similarity between the architecture of Bitcoin and the decentralized architecture of the internet. Based on that, they argue that such an architecture is superior to a centralized one, and therefore Bitcoin has the possibility of becoming the transactional protocol for the internet and global commerce.



Decentralized network (http://brucemacvarish.com/, accessed 12.10.2104)

Weaknesses

New and developing technology

Generally, a currency is more powerful with the number of people using it. Digital currencies, especially cryptocurrencies, are in their infancy and still new to most of the people. This has an influence on the general adoption and also affects the price volatility on the market.

Also, in order to understand the mechanisms, one needs to have some basic knowledge about computers and networks, and for many people this is still a challenge. If people don't understand the basics behind the technology, it will be difficult to recognize the advantages that a digital currency brings to the financial market. In general, people tend to resist change, prefer to stick to the old ways, and are reticent to risk adopting new technologies, especially when it comes to their finances.

Another issue is that the technology is still in active development, with updates and improvement coming to the market in form of new coins every month or two. One should keep in mind that new ideas are being explored that have never been attempted before, and therefore the future of any digital currency cannot be predicted.

This makes some people to feel insecure about purchasing bitcoins now, and prefer to wait for the "final" currency to hit the market (European Banking Authority, 2014).

Because it is relatively new in the financial world, it is important to acknowledge the fact that at this point neither Bitcoin nor other digital currency is an official currency, and therefore most of jurisdictions will require to pay income or capital gains taxes. This can rise the costs of using the currencies and is also an unknown risk factor, as in general no definitive regulation has been issued by governments. The lack of definitive regulation can negatively impact other actors in the financial ecosystem of the currency, as legal uncertainty remains over contractual relationships, and in time may be even rendered illegal.

Volatility

One of the biggest problems with digital currencies, especially cryptocurrencies, is their volatile nature relative to the major fiat currencies like

USD or Euro. As there is no centralized control and no manipulation of money supply, the price of a Bitcoin is given by the market.
Added to that, even the most popular cryptocurrency today, Bitcoin, is used by a relative small amount of business and companies, and therefore even small events or business activities can influence the price on the market. Therefore, the price can experience big swings over short periods of time, which is seen by many as a big risk factor (http://bitcoinembassy.ca/about/what-is-bitcoin/advantages-disadvantages, accessed 31.07.2014).
However, in theory, it is expected that the volatility will decrease in time, as more business start to use the digital currency and the market matures. The more people use a currency, the more stable its price gets, and the volatility risk decreases (European Banking Authority, 2014).

Bitcoin price chart in the last 12 months (http://bitcoincharts.com/, accessed 12.10.2104)

Some exchange centers provide a solution for the merchants using cryptocurrency, namely they can instantly convert the currency received into a fiat currency like USD or Euro, therefore minimizing the risk of losing from price movements. As a result, the merchant receives in the moment of payment the exact amount of digital currency exchanged in a real currency, and eliminates the risk or volatility.

Irreversibility

Transactions of cryptocurrencies are irreversible. Once a payment has been made, the only person that can refund is the receiver. Because there is no

central authority that can regulate the transaction, the only actors in the process are the sender and the receiver of the money. This has the positive effect that the transaction fees are kept at a minimum, but in the same time there is no safety net that can protect the sender from paying the wrong address or if the receiver acts in bad faith. This can pose problems in case of mistaken transaction or conflicts between sender and receiver.

The irreversibility factor shifts the responsibility of the transaction in the hands of the sender and receiver, which is a key feature of decentralized payment systems. This lack of protection can increase the risk in certain situations and therefore can be seen as a disadvantage.

Weaknesses as a Currency

David Yermack in his paper **"**Is bitcoin a real currency?**"** builds a case in which he argues the weaknesses of Bitcoin in relation to its functions as a currency. He argues that a currency functions as a medium of exchange, a store of value, and a unit of account, and Bitcoin fails to satisfy these criteria (Yermack, 2014).

As a medium of exchange, the usefulness as a currency in the consumer economy must be analyzed. It is argued that Bitcoin**'**s use in real economy is still very limited, with more anecdotal and media stories than real hard data. The number of retailers and merchants that accept Bitcoin is still limited, and the top merchants are in the computer industry, many of them offering niche hardware and software.

It is also argued that most of the transactions in Bitcoin, ranging around 70.000 BTC per day, are for speculative reasons, and less used to buy or sell products and services (https://blockchain.info/charts/n-transactions, accessed 15.10.2014).

As to the size of the world economy, it seems that Bitcoin has a negligible market presence, with a relative small volume of transactions and small number of merchants that accept the currency (Yermack, 2014).

Regarding the function of a unit of account, Yermack argues that for a currency to have this function, it must be treated as a numeraire when comparing the prices of alternative retail goods. Bitcoins faces a few issues in this regard.

On one hand, the high volatility varies greatly on a daily basis, which makes it confusing when trying to express prices in bitcoins. Added to that, it seems that there is a diversity of **"**current market prices**"** that can be obtained for Bitcoin from different exchange websites (Yermack, 2014).
Yermack argues that the disparity in market prices can go up to 7% between low and high quotes, which makes it very hard to offer a stable framework to express prices of goods and services. The last argument against using Bitcoin as a unit of account refers to the number of decimals needed when quoting prices in Bitcoin. As one bitcoin can be broken down in smaller units, called satoshi, the prices of trivial goods, like a Coca Cola bottle, must be expressed in numbers up to 5-6 decimals. This fact could make it difficult for customer to take Bitcoin as a reference price.

Coca Cola bottle expressed in Bitcoin (http://pizzaforcoins.com/, accessed 15.10.2014)

The last function of a currency is storing value, i.e. the owner obtains the currency at a point in time and exchanges it for goods and services at some future time of his choice, with the expectation that the currency still has the value as when acquired. In the case of Bitcoin, the challenge is posed by the fact that Bitcoin require a certain amount of security in order to store the coins securely, and even more important, one must take into consideration the risk imposed by the high volatility of the currency. Yermack puts the volatility range in perspective by comparing the exchange rate volatility of 142% for Bitcoin (in 2013) with the exchange rate volatilities of the traditional currencies (Euro, Yen, British Pound, and Swiss Franc), which fall between 7% and 12% (Yermack, 2014).

In conclusion, it is argued that Bitcoin is not yet a bona fide currency, lacking in every aspect of the main functions that need to be satisfied by an established currency. In order to progress towards becoming one, several issues has to be addressed, especially the daily value will need to become more stable so that it can reliably serve as a store of value and as a unit of account (Yermack, 2014).

Reliance on an electronic infrastructure

Bitcoin is a digital currency with no presence in the physical world. The only way to access bitcoins, use them for transactions, or store them, is through a computer or an electronic gadget.

This has obvious advantages, but also makes a currency totally reliant on an electronic infrastructure, which in the case of a world-wide power shut down or other type of interruption of the electronic infrastructure, can leave the currency system totally paralyzed. This holds true also for the traditional currencies that rely on an electronic infrastructure, but in the case of Bitcoin the dependence is 100%, and the consequences could be far-reaching.

Opportunities

Online Currency

The most straightforward opportunity for Bitcoin is to become the main currency for online transactions. Currently, the online payment market is dominated by credit card companies and Paypal, which typically charge high commissions and are prone to fraud. Bitcoin is seen by the supporting community as a superior online currency, offering very low fees, much faster transfers and a higher degree of anonymity.

Alternative Currency

Bitcoin have been used as an alternative currency to the national currency. For example when Argentina and Cyprus had currency problems, with legal restriction to prevent money from leaving the country and very high surcharge for credit cards, Bitcoin had gained a lot of attention and popularity as a viable

alternative to store value and to conduct transactions (http://www.economist.com/blogs/schumpeter/2014/06/bitcoin-argentina, accessed 14.10.2014)
Therefore it has been argued that Bitcoin represents a viable alternative option for countries where the financial system is not providing a stable environment and temporary alternative solutions are needed.

Offline Payments

Another opportunity for Bitcoin is to gain adoption for offline payments, as for example in restaurants and shops. There are already a number of shops receiving bitcoins, but the percent is relative small in comparison with the use of physical money. Although using Bitcoin for offline payment does not take full advantage of the main features of the protocol in comparison with physical money (like anonymity or low transaction fees), there are certain advantages in using it. For example, by using Bitcoin one must not carry large sums of money with him, which makes it more secure and less risky. Added to that, in some countries there are cash limits that can be carried or used in cash transactions. That would also be bypassed using Bitcoin as one can carry unlimited amounts of bitcoins on a digital wallet device.
With that being said, the prospect of Bitcoin or other digital currency to overtake the use of national currencies seems limited due to competition from very deep established customs and practices of using traditional currencies.

Micropayments

Another strongly argued opportunity for Bitcoin is to enable large scale micropayments. Micropayments are transactions of very small amounts of money via Internet. In the traditional online payment, using credit card or Paypal, micropayments tend to be unpopular because of the high transaction fees. If a merchants operates with low margins, micropayment using traditional online payment is most of the time unprofitable, as the transaction fees lower the margin profit considerably.
Bitcoin's advantages can offer a much better alternative, as the transaction costs are very low and the speed very fast, therefore is proposed as the perfect currency for micropayments

An example of such service using Bitcoin is BitcoinTip, which allows users from different forums to send small amounts of Bitcoin (or other digital currencies) to other users as a reward for a comment.

Challenges

Loss of confidence

Most of the currencies existing are backed by a legal entity (like a government) or a commodity (like gold). In the case of most digital currencies, especially cryptocurrencies like Bitcoin, there is neither support from a central authority nor backing by a commodity. Therefore the basis for an invested trust in a cryptocurrency is questioned. Why would someone have the necessary confidence in such a currency when there is no legal authority nor commodity behind it?

Even in this situation, apparently Bitcoin is trusted by enough people to keep it at a competitive level with other traditional currencies. This should not come as a surprise, as there have been other cases of currencies that were not backed by any government and still remained in use. One such example is the Iraqi Swiss Dinar, which for a period of ten years continued to circulate in north of Iraq with a stable trading value, after it was disendorsed by the Iraqi's government (http://www.cbi.iq/index.php?pid=History, accessed 13.10.2014). Although Bitcoin enjoys a wave a confidence from an even larger community, there are always realistic scenarios in which the confidence people have in the currency could drop drastically.

Economic Bubbles

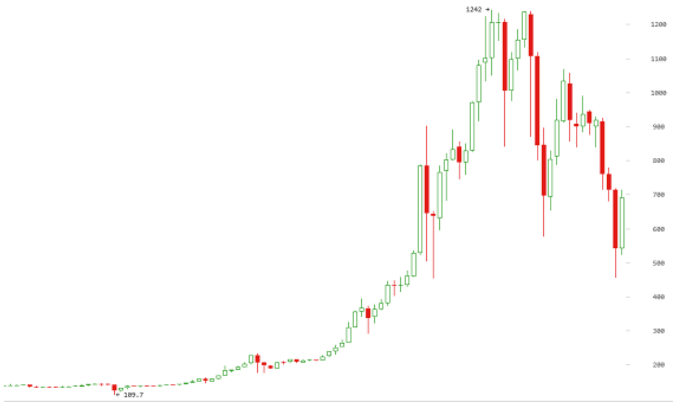
Like everything that is extracting its value from people's investment, Bitcoin and other similar cryptocurrencies are susceptible to investment bubbles and artificial value inflation. The sharp rise in value of Bitcoin at the end of 2013 and the subsequent fall has been recognized by many as a classic example of an investment bubble.

An investment bubble or economic bubble is defined by investopedia.com as "*a surge in equity prices, often more than warranted by the fundamentals and*

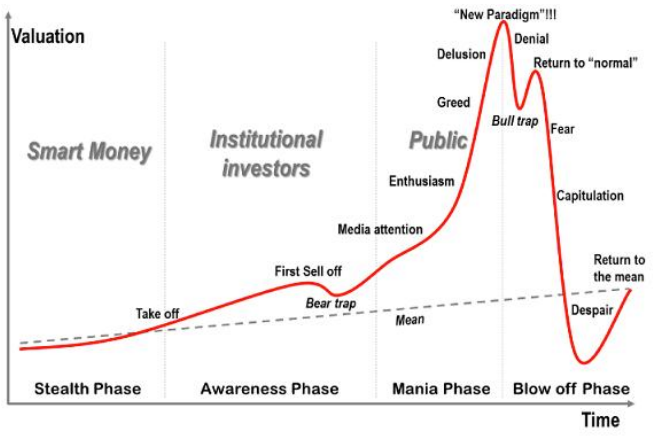
usually in a particular sector, followed by a drastic drop in prices as a massive selloff occurs **”** (http://www.investopedia.com/terms/b/bubble.asp, accessed 13.10.2014)

Jesse Colombo, an economic analyst for Forbes, has compared the price movement patterns of Bitcoin with the archetypal bubble stages created by Jean-Paul Rodrigue. He argues that at least for 2013, Bitcoin is following the classical pattern of an investment bubble, which should make people more careful in making hard predictions about future price movements. (http://www.forbes.com/sites/jessecolombo/2013/12/19/bitcoin-may-be-following-this-classic-bubble-stages-chart/, accessed 13.10.2014)

The following graphs are meant to point out the similarities between price movements of Bitcoin in the second half of 2013 and the typical bubble stages of Jean-Paul Rodrigue:



Bitcoin price chart of the second part of 2013 (bitcoinwisdom.com, accessed 12.10.2104)



Rodrigue’s bubble stages (forbes.com, accessed 12.10.2104)

Others have analyzed the price movement of Bitcoin and have reached the conclusion that there were several bubbles in the last 4 years, and that is a normal developmental path for such a currency. They identify the first bubbles in 2010 when the price went from 0.01 to 1,00 US dollars (a 100 times increase) and then from 1,00 to 30 US dollars (a 30 times increase). The last two bubbles happened in 2012 and 2013 with smaller increases up to 9 times. It is argued that the size of the bubbles decreases in time and they will come to a halt as time goes by and the currency gets more stability. Therefore, economic bubbles for Bitcoin are still to be expected, as it is normal to go through this kind of price changes. Added to that, if we look at the price movements of Bitcoin and the public interest in the currency as express in Google trends, one can see correlation that would suggest that the price will continue to be affected by media coverage and public awareness, which are by nature unpredictable (https://www.cryptocoinsnews.com/bitcoin-price-analysis-bubbles-past-future/, accessed 13.10.2014).

Further Development

Bitcoin has no central authority and the rules of the protocol were set by Satoshi Nakamoto in 2009. With that being said, in reality there is still a core team of developers that continue to work on developing and maintaining Bitcoin. They deal with issues like fixing bugs, make small changes and issue new releases (https://bitcoin.org/en/development, accessed 14.10.2014).

It is not inconceivable that the development team, or another group of interest with sufficient influence on the team, would make changes to the core assumptions of the protocol, like for example changing the limit of bitcoins or the inflation rate. Others have proposed the scenario when a competitor of Bitcoin, like a government or central bank, could impact the further development of the protocol by lobbying and influencing the community and the developers. As there is no central authority to protect against such prospects, there is always the possibility of a change in direction in regard with the further development of the protocol (Grinberg, 2011).

Such events could make the general population to lose confidence in the currency and, as a result, migrate to other forms of digital money or going back to fiat currency.
Another issue in regard to the further development of the protocol is the fact that the work on cryptocurrencies is ground breaking work, with no precedent, and therefore there is a risk factor always present. It could be conceivable that even with the best intention in mind, the development of Bitcoin could take a wrong turn and morph into something different from the present protocol.
All these risk factors could lower the confidence for certain investors or adopters, and if it is to succeed, the community must take counter measure to prevent such scenarios and build trust among the general population.

Legal Issues

A certain amount of people are cautious to adopt Bitcoin, as they are concerned that governments and financial authorities will hinder or even shut down its use. Added to that, it is a known fact that Bitcoin and other digital currencies are associated with criminal activities, and some people would not want to be associated or sustain such a currency. Even if we remove the association with criminal activities, there is no guarantee that governments will accept a currency which they cannot control. Therefore such governments could prohibit the use in their countries and therefore could affect the price and stability of the currency.
To avoid such long term risks, the community should build a positive image of the currency in the eyes of the public, and lobby the politicians and governments to integrate it in an international financial framework. Also an effort should be made to hinder the use of Bitcoin (or other digital currency) in criminal activities, like money laundering, tax evasion or illegal purchase of goods and services.

Deflationary Spiral

Bitcoin has a fixed amount of possible coins to be created. This means that the protocol has an in-built deflation mechanism. In the long run, when the maximum amount of bitcoins will be reached, and in the case of a widespread

use of the currency, the demand for bitcoins will outstrip the supply, causing the value of Bitcoin to increase.
As a consequence, the prices denominated in bitcoins will fall which may make the manufactures to lower production, leading to lower wages, lower demand, underemployment of human capital, and even to destruction of wealth (Grinberg, 2011). Such a process is known as a deflationary spiral. Faced with such a scenario, there is a strong incentive for investors to hoard bitcoins and not spend them, causing also the current level of transactions to fall, which will affect negatively the spread and adoption of the currency.
It is argued that a currency must be elastic, i.e. the supply can be increased or decreased in order to adapt to the needs of the economy, and that a central authority (like the central bank) must be in place to implement fiscal policy. As an example we can refer to the period when the US functioned under the gold standard (1880-1914), which was an inelastic supply, and the deflationary character of the supply led to high real interest rates, caused banking panics, and produced increased instability of output (Elwell et al, 2014).
The fact that Bitcoin does not rely on any central authority means that in case of a deflationary spiral, there will be no authority able to make the necessary adjustments. As being run only by the community and voluntary developers, the reach of a consensus regarding needed action could be difficult and even impossible. This could be a major threat for Bitcoin, as the inability to adapt to new economic environments could hinder or even destroy the currency.

Security concerns

The Bitcoin protocol is based on proven cryptography and digital signatures, and therefore basically safe against fundamental attacks. Nevertheless there have been numerous attacks on Bitcoin clients and platforms, raising the issue of security in the public eye.
The most mediatized, and with the greatest loss, was the attack against popular Bitcoin exchange, Mt.Gox, in 2013, when over 450 million US dollar worth of bitcoins were stolen, which drove the company into bankruptcy (http://www.wired.com/2014/03/bitcoin-exchange/, accessed 14.10.2014). Several other such attacks were carried in the last years, especially against wallet providers and exchange firms.

The main security problem is the theft of bitcoins. Like cash, bitcoins can be lost or stolen. If a user loses his wallet, it has the effect of removing money out of circulation. Lost bitcoins still remain in the blockchain just like any other bitcoin, but will remain dormant forever because there is no way for anybody to find the private key(s) that would allow them to be spent again (https://bitcoin.org, accessed 15.10.2014).
The attacks focus on large storage of bitcoins, like a wallet provider, or on personal computer where bitcoins may be stored. A large-scale theft of bitcoins could lead the user to lose confidence in the currency. Also, the scenario where one could lose all their bitcoins if a hard disk crashed or if the computer is stolen, could be a major barrier for certain users.
It is also possible, although arguably unlikely, that new bugs and security vulnerability in the standard client could lead to tempering the blockchain and even causing a total shut down of the network. A specific type of attack against the blockchain, called "Sybil attack", is the attempt of an attacker to fill the network with clients controlled by him, so that it can manipulate the creation of new blocks. This could give the attacker the possibility to isolate a node from the rest of the network making transactions open to double-spending attacks (https://en.bitcoin.it/wiki/Weaknesses, accessed 15.10.2014).
Although SHA-256 and ECDSA cryptography are considered very strong protocols, there is also the possibility that in the future they could be broken. In this case, a shift to a new algorithm will be necessary.
Other security concerns relate to other types of cyber-attacks on the protocol, like Denial of Service attacks or Packet sniffing, that could disrupt normal transactional activities or compromise the network.

Competition

Bitcoin is the first cryptocurrency, as it was based on the original paper written by Satoshi Nakamoto. In this regard, Bitcoin is the first mover in cryptocurrency market.
As for many first movers in a market with low entry barrier, it could happen that a revised and updated new cryptocurrency will gain better market adoption and overtake Bitcoin. This phenomenon would not be unusual in the

electronic marketplace, as we saw in the case of AltaVista being overtaken by Google, Myspace by Facebook or Hotmail by Gmail (Elwell at al, 2014). Currently, Bitcoin is the uncontested market leader in comparison to other digital currencies, but in time, as better protocols come to light and improvements are developed, there would not be a surprise to see the rise of other powerful and superior digital currencies.

Strengths	Weaknesses
• Payment freedom • Transaction Costs • Transaction processing time • Safeness and transparency • Anonymity • Decentralized architecture	• New and developing technology • Volatility • Irreversibility • Weaknesses as a Currency • Electronic infrastructure
Opportunities	**Threats**
• Online Currency • Alternative Currency • Offline Payments • Micropayments	• Loss of confidence • Economic Bubbles • Further Development • Legal Issues • Deflationary Spiral • Security concerns • Competition

Bitcoin SWOT analysis

Conclusion

To summarize, Bitcoin has clear advantages as a new and innovative digital currency that offers payment freedom regardless of geographic boundaries, low transaction fees and fast processing speed. The currency is also built on a decentralized architecture, with no central authority in control, which has certain advantages but could also pose some challenges in the future if the economic environment will change.

Because it is still a young and partially experimental currency, Bitcoin is still very volatile in value and lacks in fulfilling the functions of a currency in practical terms. As the transactions are irreversible and cannot be mediated by a third party, certain risks in case of conflicts could arise. Also, the total dependence on an electronic infrastructure could be seen as a weakness, as certain scenarios where disruptions to the world electronic network could be conceivable.

Bitcoin is experiencing now a wave of enthusiasm, and certain opportunities can be identified. As traditional currencies still lack as currencies used for online transaction, the biggest opportunity for Bitcoin seems to be becoming the main currency used on the internet. Also for countries where the national currency fails to offer a stable economic environment, digital currencies like Bitcoin could be seen as a viable alternative. Because of the low transaction costs and high speed, Bitcoin it is also seen as the best candidate for micropayments.

The main threats regarding Bitcoin are due to the fact that it is a young currency yet, and certain challenges are still to be overcome. The price volatility and the forming of economic bubbles have to be managed and the general population's confidence must be maintained.

The internal processes of maintenance and development of Bitcoin have to be managed is such a way that no interest group would compromise the basic assumptions of the protocol. Also the relationship with different governments should be improved, as to avoid certain conflicts with regulation and further development of the legal framework.

Lastly, the security around cyber-attacks on wallets providers and other Bitcoin related company must be maximized as they play a big role in the media exposure, and subsequently in the perceived image of the currency.

To conclude, Bitcoin is a new concept, but it is in the process of being understood and adopted by a growing number of consumers, merchants, and investors around the world.
Like every other young innovation, there are certain challenges and uncertainties about its future. Bitcoin has made significant progress in its adoption and usage since it was introduced in 2009, and its evolution over the next few years will determine whether this leading cryptocurrency will become an integral part of the global financial system, or whether it is destined to remain a niche player. Regardless of its success or failure, Bitcoin represents a new way of thinking about currency and financial transactions.

Literature

Ajibola Adetilewa Ogunbadewa (2013), The 'Bitcoin' virtual currency: a safe haven for money launderers? Cardiff University, Available at SSRN: http://ssrn.com/abstract=2402632

Aleksandra Bal (2013), Stateless Virtual Money in the Tax System, Bulletin for International Taxation, Available at SSRN: http://ssrn.com/abstract=2298537

Alex Heid (2014), Analysis of the Cryptocurrency Marketplace, http://www.hackmiami.org/whitepapers/HackMiami-Analysis_of_the_ Cryptocurrency_Marketplace.pdf (accessed 10.09.2014)

Andrew B. Whinston, Dale O. Stahl, Soon-Yong Choi (1997), The Economics of Electronic Commerce Textbook Binding, Macmillan Technical Publishing ISBN:1578700140

Appan Kandala Vasudevachary (2011), Money- Meaning, Functions, Classification and Gresham's Law, Dept of Economics, Koti Osmania University, Published by Appan Kandala Vasudevachary

Bastiaan Quasty (2014), Bitcoin and Cryptocurrencies - How Inftion Will Come About in Cybermoney, Centre for Finance and Development, Geneva; http://rpubs.com/bquast/CryptocurrencyInflation

Bryan Taylor (2010), A History of Universal Currencies, https://www.globalfinancialdata.com/news/Articles/A_History_Of_Universal_Currencies.pdf (accessed 10.09.2014)

Cindy Williamson, Jason Vazquez, Jason Thomas,Katherine Sagona-Stophel (2013), Technology in the fight against money laundering in the new digital currency age, http://accelus.thomsonreuters.com/sites/default/files/GRC00403_0.pdf (accessed 08.09.2014)

Craig K. Elwell, M. Maureen Murphy, Michael V. Seitzinger (2014), Bitcoin: Questions, Answers, and Analysis of Legal Issues, CRS Report for the Congressional Research Service, http://fas.org/sgp/crs/misc/R43339.pdf (accessed 07.08.2014)

Danton Bryans (2014), Bitcoin and Money Laundering: Mining for an Effective Solution. 89 Ind.L.J.441, Available at SSRN: http://ssrn.com/abstract=2317990

David Yermack (2014), Is bitcoin a real currency? An economic appraisal, New York University Stern School of Business, http://online.wsj.com/public/resources/documents/NBER.pdf (accessed 07.07.2014)

Dowd Kevin (1988), Private money: the path to monetary stability, Institute of Economic_Affairs,http://www.iea.org.uk/sites/default/files/publications/files/PRIVATE%20MONEY.pdf (accessed 12.10.2014)

Dwork, Cynthia; Naor, Moni (1993), "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". CRYPTO'92: Lecture Notes in Computer Science No. 740 (Springer): 139–147.

Éric Tymoigne and L. Randall Wray (2013), Modern Money Theory 101: A Reply to Critics, Levy Economics Institute of Bard College, Working Papers Series No. 778. Available at SSRN: http://ssrn.com/abstract=2348704

European Banking Authority (2014), EBA Opinion on 'virtual currencies, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (accessed 12.10.2014)

European Central Bank Report (2012), Virtual Currencies Schemes, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (accessed 12.08.2014)

FATF Report (2014), Virtual Currencies-Key definitions and potential AML/CFT Risks, The Financial Action Task Force, http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 10.08.2014)

Federal Bureau of Investigation (2012), Bitcoin Virtual Currency: Unique Features Present, Distinct Challenges for Deterring Illicit Activity, http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf (accessed 15.07.2014)

Fergal Reid and Martin Harrigan (2013), An Analysis of Anonymity in the Bitcoin System, Springer

Financial Crimes Enforcement Network (2013), Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (accessed 03.08.2014)

F.A. Hayek (1976a), Choice in Currency: A Way to Stop Inflation, Ludwig von Mises Institute

F.A. Hayek (1976b), Denationalisation of Money: The Argument Refined, Ludwig von Mises Institute

Geoffrey Crowther (1941), Outline of Money, Thomas Nelson And Sons Limited, http://www.jstor.org/stable/2226268 (accessed 12.10.2014)

Glasner, David (1989),Free banking and monetary reform: Cambridge University Press.

Henk C.A. van Tilborg (2005), Encyclopedia of Cryptography, Springer Science+Business Media, Inc.

Internal Revenue Service (2014), IRS Notice 2014-21, http://www.irs.gov/pub/irs-drop/n-14-21.pdf (accessed 18.08.2014)

Jan A. Bergstra (2013), Formaleuros, Formalbitcoins, and Virtual Monies, Informatics Institute, Faculty of Science, University of Amsterdam, http://arxiv.org/pdf/1008.0616.pdf (accessed 12. 09.2014)

John Stuart Mill (1848), Principles of Political Economy, London; Longmans, Green and Co.

Jonathan Williams (2007), Money: A History, British Museum Press; 2nd Revised edition

Lars Holdgaard (2014), An exploration of the Bitcoin ecosystem, Bitcoin Project, http://bitcoin-expert.net/master-thesis/, accessed 10.05.2014)

Lawrence, Robert Z.; Hanouz, Margareta Drzeniek; Doherty, Sean (2012), The Global Enabling Trade Report 2012: Reducing Supply Chain Barriers (Report). World Economic Forum

Ludwig von Mises (1912), The Theory of Money and Credit, Indianapolis, IN: Liberty Fund, Inc

Moore, James (1996), The Death of Competition: Leadership & Strategy in the Age of Business Ecosystems. New York: Harper Business.

Nicholas A. Plassaras (2013), Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF, Chicago Journal of International Law, 14 Chi J Intl L (2013) Forthcoming. Available at SSRN: http://ssrn.com/abstract=2248419

Patomäki, Heikki (2007), Globalization and Economy, Vol. 2: Globalizing Finance and the New Economy. London, UK: Sage Publications

Pavlina Tcherneva (2005), The Nature, Origins, and Role of Money, Center for Full

Employment and Price Stability, University of Missouri-Kansas City, http://www.cfeps.org/pubs/wp-pdf/WP46-Tcherneva.pdf

Piotr Piasecki (2012), Design and security analysis of Bitcoin infrastructure using application deployed on Google Apps Engine, Master Thesis Wydział Fizyki Technicznej

Raj Samani, François Paget and Matthew Hart (2013), Digital Laundry
An analysis of online currencies, and their use in cybercrime, Mcafee, http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf (accessed 08.07.2014)

Reuben Grinberg (2011), Bitcoin: An Innovative Alternative Digital Currency, Yale Law School, Hastings Science & Technology Law Journal, Vol. 4, p.160

Satoshi Nakamoto (2009), Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (accessed 01.06.2014)

Simon Brodbeck (2007), Virtual Money: A new form of privately issued money in the money market, European School of Management, Available at SSRN: http://ssrn.com/abstract=999022

Solomon Lewis (1996), Rethinking our centralized monetary system: the case for a system of local currencies, Westport, Conn: Praeger,

State of Bitcoin Report - Q2 (2014), http://media.coindesk.com/report/CoinDesk-State-of-Bitcoin-Q2-2014.pdf (accessed 06.09.2014)

United States Government Accountability Office (2014), VIRTUAL CURRENCIES - Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges, Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, http://www.gao.gov/assets/670/663678.pdf

Wei Dai (1998), B-Money, http://weidai.com/bmoney.txt (accessed 08.09.2014)

Zusammenfassung

Die Entwicklungen des Internets als globale Kommunikationsplattform eröffnen neue Möglichkeiten der Kommunikation, und verändern grundlegend diese die Art wie Menschen kommunizieren. Eine der interessantesten Entwicklungen ist die Entstehung der Digitalen Währung, ein recht neues Phänomen, welches die Art wie wir über Finanzen denken zu revolutionieren verspricht.

Diese Dissertation wird das Konzept der Digitalen Währung analysieren, insbesondere das vom Bitcoin, eine der prominentesten digitalen Währung zurzeit.
Es wird mit einer kurzen Geschichte und Definition des Begriffs "Geld" starten, gefolgt von einer tieferen Analyse der Digitalen Währung im Allgemeinen.
Die letzten zwei Kapitel der Arbeit werden sich mit Bitcoin befassen. Das Bitcoin-Protokoll wird im Detail beschrieben, die verschiedenen Akteure in der Branche aufgelistet, und die Stärken, Schwächen, Chancen und Gefahren untersucht.

Lebenslauf

Name: Peicu Rares Codrin
Adresse: 1160 Wien, Österreich
Tel: +43 6505356530
Email: rares.peicu@selfxp.com

Ausbildung

2012 –
Masterstudium Internationale Betriebswirtschaft - Hauptuniversität Wien (Wien)
2012
International Management (Erasmus) - Universitat de Valencia (Valencia)
2007 - 2012
Bachelorstudium International Betriebswirtschaft - Hauptuniversität Wien (Wien)
2000 – 2004
Bundesrealgymnasium (Matura) - Gheorghe Lazar (Bukarest)

Berufserfahrung

2014
Assistant Project Manager (Praktikum) - United Nations - INCB (Wien)

Tätigkeiten: Research, Project Design, Project Development, Team Management
Wirtschaftssektor: Communications & Intergovernmental Relations

2013

Assistant Project Manager - StreamKIT (Wien, San Francisco)
Tätigkeiten: Marketing, Project Development, Project Management
Wirtschaftssektor: Internet Broadcasting

2011-2013

Project Manager - Spotzer Media, Herold.at (Wien)
Tätigkeiten: Creative Director, Account Management, Product Development
Wirtschaftssektor: Video Advertising

Hauptfächer/berufliche Fähigkeiten

- Marketing
- Management
- Information Technology
- Product Development
- Research and Development
- Personal Management

Organisatorische Fähigkeiten

- Erfahrung in Koordinierung von Projekten
- Geschicklichkeit zu analysieren, planen, verwalten und motivieren
- Exzellente Kenntnisse zwischenmenschlicher Beziehungen

Soziale Fähigkeiten

- Selbsbewust
- Teamgeist
- Verantwortungsvoll
- Bellastbar
- Kommunicativ

Fremdsprachen:

- Rumänisch Muttersprache
- Englisch schriftlich und mündlich sehr gut
- Deutsch schriftlich und mündlich sehr gut
- Spanisch schriftlich und mündlich gut