

ABSTRACT

1 THE BITCOIN

The Bitcoin (BTC) is a peer to peer virtual payment scheme, created by Satoshi Nakamoto in 2008 and introduced in the market in 2009. Satoshi Nakamoto is no longer an active developer (Aron, 2011) and it is not even clear what his true identity is. The Bitcoin has been designed to make online payments quick and simple, solving the double spending problem and eliminating the need for financial intermediaries, protecting at the same time the anonymity of the users. Any user can save his Bitcoins into a digital wallet which can be installed on his computer or outsourced to a third party service, and can transfer funds to any other user who has a "public address" to receive BTCs. An user can obtain Bitcoin by purchasing them from other users, buying them on online trading platforms, selling goods and services in exchange for Bitcoin, or obtaining them through a process called mining.

The paper written by Satoshi Nakamoto in 2008 is generally regarded as the founding act of Bitcoin. It should be noted, however, that such a digital currency could not have seen birth without some underlying technological innovations - more specifically in the field of cryptography - and without the impulse of the Austrian School of economics. The historical events surrounding the birth of Bitcoin are important too, and the financial crisis of 2008 has played a primary role in expanding the cultural impact of Bitcoin.

The Bitcoin has quickly risen in popularity, spawning other cryptocurrencies. The developers of Bitcoin have deliberately made its source code available to anyone for any use: the competition between cryptocurrencies is clearly encouraged by the developers themselves.

The total market capitalization of Bitcoin has rapidly exceeded the value of 14 billion dollars in December 2013 (Bitcoin - Market Capitalization, Coindesk). From an initial value of circa €0.0005 in 2009 (Karlstrom, 2014), BTC began to grow in 2013, reaching the value of \$120 in September 2013 and eventually touching the peak of \$1,147 in the first days of December 2013. After a severe downturn during the first half of 2014, the Bitcoin has begun to appreciate again and now - in mid-June 2014 - it is worth about \$ 590. (Bitcoin Price Index Chart, Coindesk), while the total market capitalization is estimated at 7 and a half billion dollars.

In the words of Karlstrøm (2014), we can say that Bitcoin is a combination of three existing phenomena. As a matter of fact, this currency combines the features of a "traditional" electronic currency with a security protocol for managing anonymous

trading, and is able to achieve through a software that replaces the modern central banks in the issuance of money (Karlstrøm, 2014).

In short, payments are allowed without the need of going through financial intermediaries, and there is no central authority controlling the issuance of money. New Bitcoins are created only through a process called mining. Some users called miners compete with each other in order to validate transactions by solving complex mathematical problems, and are rewarded with new Bitcoins in exchange for their service. Not only is this the only way in which new Bitcoins are created, but the amount of this payout is going to decline over time too.

2. ECONOMIC PROFILES

The emission cap of Bitcoin has been locked by its developers at the amount of 21 millions of BTCs. Every ten minutes, a new block is generated: new Bitcoin are issued every time a user solves a new block, and the number of Bitcoin generated per block decreases by 50% every 4 years. *This algorithm was chosen because it approximates the rate at which commodities like gold are mined* (Controlled Supply Currency, Bitcoin wiki). It has been calculated that the emission cap will be reached in 2040 (ECB, 2012): from that date on, no new Bitcoin will be issued, and the money given to miners as a reward is going to be obtained by placing a small fee on transactions.

The lack of a central authority makes any attempt to balance the money supply in accordance with the demand result in a failure. This leads to a constant appreciation of Bitcoin, which helps miners keep the incentives to sustain the growing costs of mining.

As we know, Bitcoin has appreciated until the end of December. The ones who feared the dangers of speculation, however, expected a sudden collapse in value. A collapse was actually triggered after People's Bank of China took harsh measures against Bitcoin, but this collapse did not lead to the demise of Bitcoin, which has recently started to appreciate again. Speculation seems to have provided the raw material for the spread of Bitcoin, fueling the demand of Bitcoin and spreading the currency among new users.

But is Bitcoin a currency? Money has four functions: it must satisfy the criteria of being a medium of exchange, unit of account, reference for deferred payments and store of value. *Bitcoin does its best as a medium of exchange* (Money from Nothing, 2014). Users can transfer money anywhere in the world while being guaranteed with reduced transaction costs and high levels of anonymity. However, the volatility of

the currency makes the Bitcoin inadequate as a store of value and as a standard of deferred payments, preventing the Bitcoin from becoming an unit of account, and keeping it from displacing traditional currencies (Bitcoin's deflation problem, 2014).

Interestingly, Hayek (1976) finds that monetary instability jeopardizes the last three uses of money, making a deflationary currency undesirable as well. Moreover, he argues that a free market of competing private currencies can automatically converge towards monetary stability. If the State monopoly on the issuance of currency is abolished, unstable, inflationary or deflationary currencies would end up being discarded by the general public since they would not be able to ensure all four function of money.

In addition, the Bitcoin has some other limitations:

- A Bitcoin can only be stored inside a digital wallet. However, keeping a Bitcoin in a digital wallet is more like hiding money under the mattress rather than depositing it in the bank. But a banking system and credit cannot coexist with Bitcoin. The abolition of the banking system, rather than a step forward, it only looks like an involuntary step back to the Middle Ages (Hanley, 2013).

- The majority of BTC's does not circulate within the system and the wealth is concentrated in a few entities. If we sum up the amounts accumulated at the 609,270 addresses which only receive and never send any BTC's, we see that they contain 7,019,100 BTC's, which are almost 78% of all existing BTC's (Dorit & Shamir, 2013). The same study showed that there were only 78 entities with a current budget of more than 10,000 BTC's, while the balance of 97% of the entities in the system consisted in less than 10 BTC's.

- If the Bitcoin loses significant value due to a sharp decrease of demand, the miners would have little incentive to continue to invest in more powerful hardware or to bear higher energy costs. The only incentive for miners to validate new blocks and keep their BTC's would be the belief of a further appreciation of Bitcoin.

- The Bitcoin can not take the place of a fiat currency without dramatically appreciating. Because of the controlled currency supply, Bitcoin can not be issued on demand, making the replacement of a legal tender almost impossible. Not only such a rise in value would not be credible, but, as a consequence, it would lead to the breakdown of Bitcoin itself: *no rational player would use Bitcoins for spending purposes* anymore (Hanley, 2013)

3. LEGAL ASPECTS

This digital currency has been used for illicit purposes. More precisely, the Bitcoin was often used to evade taxes, launder money and buy goods illegally. Although identical problems may occur with the use of traditional cash (ECB, 2012), the total lack of legal framework make the Bitcoin ideal for this kind of activities.

Meanwhile, others demanded trading platforms to be regulated: these Bitcoin Exchanges are deemed unsafe and operate at the limits of legality. These services provide few guarantees to their customers and it is not unusual to witness security breaches which often lead to the disappearance of thousands of BTC.

These trading platforms are the weak spot of the Bitcoin. A successful attempt in regulating the Bitcoin should probably aim to regulate these exchanges. Disciplining these trading platforms should not only protect consumers from excessive risks but should also reduce money laundering and tax evasion with Bitcoin. In order to evade taxes or launder money, it is necessary to convert real money in exchange for Bitcoin: by requiring trading platforms to adapt to the anti-money laundering regulations, these illicit activities can be put under control.

Updating the european anti-money laundering provisions (Directive 2005/60/EC) in order to include Bitcoin and the other cryptocurrrencies would be an adequate measure. Furthermore, a system of registration and licensing of the trading platforms could be introduced and these exercises can easily be incorporated into the existing anti-money laundering legislation (Stokes, 2012). Although similar measures can not trace transfers between users, they would allow the value of Bitcoin, once converted, to be traced into the financial system of the real world (Stokes, 2012).

Draconian measures are possible too: Marian (2012) suggests that, being the money supply of BTC's limited, central banks could buy most of Bitcoins in circulation, or governments could deploy a considerable amount of computing power - more than 51% of the total power of the network would be enough - to dismantle the system from the inside.

Any attempt to regulate Bitcoin, however, has to be made at the european level. As a matter of fact, local measures would not take account of the disruptive potential of Bitcoin and could be easily circumvented. An european Regulation or Directive would without doubt be the most appropriate act to deal with this problems related to technological progress.

The existing provisions, however, are not applicable. The regulation of Bitcoin and trading platforms does not fall within the European anti-money laundering directive (2005/60/EC). The Directive does not apply because Bitcoin does not fall into the definition of electronic money contained in the Electronic Money Directive (EMD) (2009/110/EC) . Therefore, it is necessary for the EU to produce a new legislative act on the subject.

4. THE FUTURE OF BITCOIN AND OF CRYPTOCURRENCIES

The Bitcoin alone has not the potential to replace a legal tender or to disrupt the central banking system.

The controlled emission of BTCs does not guarantee the stability of the currency: if an increase of the demand occurs, the Bitcoin cannot help but appreciate. The creators of this digital currency wanted to fight inflation and take power away from central banks, but thought that planning the emission of money and impeding further expansions of the monetary base was the only way to achieve these ends. This idea, however, was strongly criticized by Hayek (1976) in his work "The denationalization of money".

In his work, Hayek advocated the idea that private financial institution should issue their own money. These so-called *issue banks* would issue currency in total freedom, and the effect of competition between these private currencies would result in the emergence of stable currencies whose value would be based on the prices of different baskets of goods. The public would eventually learn to discard every other currency which is not able to ensure its own stability. It is evident that the Bitcoin has failed to implement these guidelines but, if we look at the dynamics of the whole cryptocurrencies market, we would notice that Hayek's project is now more relevant than ever. The current scenario is similar to the one envisioned by Hayek, and the competition between crypcurrencies could correct the flaws of Bitcoin and generate an offspring of less volatile and more secure digital currencies, able to compete with fiat currencies.

At this point, we can expect Bitcoin to suffer from the *Myspace effect*, and disappear in the wake of other cryptocurrencies who have perfected a winning formula or, at best, continue to exist as a part of a wider pool of successful cryptocurrencies.

But why did these alternative cryptocurrencies have not replaced Bitcoin yet? Maybe because they are still relatively obscure and a few merchants and trading

platforms accept them. We could add that their value is still too low, that the legal framework is unclear, and non-expert users refrain from using them because they do not even know how to use digital wallets. Last but not least, we can argue that many cryptocurrencies, living in the shadow of the success of Bitcoin, are still try to imitate its misleading economic foundations.

The real revolution, however, comes from the ideology of Bitcoin. Bitcoin was developed by a motivated group of technologists who dreamed of creating a new currency that would cause fiat currencies to wither away. [...] They wanted to do this because they believe that fiat currencies are the root of financial evil. They wanted to apply the Silicon Valley idea of disruptive technology to the world economy (Hanley, 2014).

In a globalized world where internet plays a increasingly pervasive role, new technologies have seen their influence grow dramatically. The decision making process has moved from the States to Silicon Valley. The IT industry now forces its standards to the rest of the world, regardless of our lifes, our economies and even our democracies.