AN ANALYSIS OF PRIVACY AND ANONYMITY IN THE CRYPTOCURRENCY FIELD

Cristina CARATA (GURĂU)[*]

Motto:

"The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A. The way I can take a $20 bill hand it over to you and then there's no record of where it came from. You may get that without knowing who I am. That kind of thing will develop on the Internet and that will make it even easier for people using the Internet. Of course, it has its negative side.

It means the gangsters, the people who are engaged in illegal transactions, will also have an easier way to carry on their business." (Milton Friedman, 1999)[1]

Abstract

In the society we live in today, financial confidentiality and privacy has become an important topic on the agenda, due to the fact that it is a concept embracing both data security and private life data security. Crypto-currency has brought forth new concepts, some of them even innovative - unknown to this date in the currency field - that can fundamentally change the way we look at payment systems.

Virtual coins are based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as security methods. Thereby, "digital wallets" and digital currency transactions are safe, irreversible and do not contain personal information from the user. In addition to this feature, virtual money payments can be made without personal information being linked to the transaction. Thus, since the emergence of the first virtual coin – bitcoin, in 2008 - cryptocurrencies quickly developed as a popular digital payment system, largely due to these fundamental features.

The present paper is intended to analyse why cryptocurrencies are becoming more and more popular due to the notions of "privacy" and "anonymity", the innovative technology used and the effects of such anonymous transactions: on one hand, the protection of personal data and fluency of financial transactions and, on the other hand, the use of this technology in illegal activities.

Keywords: *cryptocurrency; privacy; anonymity; technology; data security.*

---

[*] PhD student at „Mihai Viteazul" National Intelligence Academy, Bucharest, cristina.carata@yahoo.com

[1] Milton Friedman (July 31, 1912 – November 16, 2006) was an American economist who received the 1976 Nobel Memorial Prize in Economic Sciences for his research on consumption analysis, monetary history and theory, and the complexity of stabilization policy.

Introduction

The first monetary system known in history appeared in Mesopotamia, around 3000 BC, when the inhabitants of those territories began to use silver as a medium of exchange and as a unit of value. The moment coincided with the emergence of Hamurabi's code-a code that contained a set of rules for monetary exchanges through silver. Since then, the monetary system has experienced drastic and constant changes, including paradigm shifts.

Without aiming to analyse the changes the monetary system has gone through since its emergence until present days, of interest for the present article, in today's society, are the modern banking services, especially online banking. Remote Banking services through electronic means (shortly e-banking system) began to develop since 1995, the year in which the US Presidential Bank of Mariland launched its first online banking services (through internet). E-banking services use computer and electronic technologies as a support for payments and other document transfers. Because of the rapid changes in the IT domain, banks face specific risks regarding electronic banking and electronic money, especially in terms of customer data security (Georgescu-Goloşoiu, 2006).

As we speak, one of the issues that is appearing more and more often is the one of financial confidentiality and privacy, in the light of cyber threats increasingly more present in our everyday life. This topic has become an important one on the agenda, due to the fact that it is a concept embracing both data security and private life data security.

Over the past few years, data breaches have increased in frequency and size, making the need to protect sensitive information a top priority for businesses worldwide. According to a 2015 report, there have been more than a thousand worldwide data breaches that compromised nearly 563 million data records of customers' personal and financial information. Big names targeted and exposed in the last 12 months not only include Ebay, Adobe, Tesco and Morrisons, but also reputable financial institutions such as the European Central Bank, JP Morgan Chase and HSBC (*Hampton, 2015*).

Given that in recent years, especially because of the exponential technological progress, companies – including here banks as part of the monetary system - are gathering an increasingly bigger number of consumer data, more and more of them are concerned about maintaining confidentiality, in terms of their personal behaviours and information. Studies conducted mainly following the events of September 11, 2001 in the United States of America – a moment that marked an increase in the control of personal data, on a global scale, in order to combat the growing phenomenon of terrorism - show that people are more concerned about the security of their personal data

and are more aware of the fact that more and more data is being collected. The vast majority of people consider that they have lost control over their personal data, which has generated considerable concern. The biggest crackdown is the fact that companies - by default, banks - which collect all this information and personal data will not be able to store them safely.

An increasingly common problem is the trade-off between security needs and personal privacy. In other words, the question that emerges is at what point security will undermine the open society that we are trying to protect and how much personal freedom should we give up to be safe, both we and our data?

In the light of these growing concerns over the last two decades, one of the most important services that the banking system can do is to ensure the privacy of its client's data and personal information. Assuring data protection in the age of the Internet can be a relatively complicated issue, especially with regard to online transactions, but without forgetting the basic issues of pure personal data previously presented.

Because of all these concerns - on one hand, cyber-attacks that are more common in the online banking system and the threat regarding both personal data and patrimonial assets held in accounts and, on the other hand, personal intrusion - a growing number of people are turning their attention towards alternative financial solutions, one of which is the use of digital coins or *crypto-currencies*, such as *bitcoin* (the first and most popular currency of its kind, a benchmark in the field)

Why are *crypto-currencies* an alternative to the classic banking system?

Crypto-currencies are gaining more ground, in parallel with the decline of the public confidence in the classical banking system and other traditional financial institutions and as a response to personal data security issues. At the same time, *crypto-currency* has brought forth new concepts, some of which are even innovative - unknown to this date in the currency field - that can fundamentally change the way we look at payment systems. In technical terms, *crypto-currency* or virtual currency is a non-banking and decentralized method (supported by its users) to exchange value between individuals, peer-to-peer (bidirectional, without intermediary) and based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as securing methods (Carata, 2017, pp. 192-198).

Since the emergence of the first digital coin in 2008 - *bitcoin*, which has remained the most popular virtual currency so far - the scale of the phenomenon

led to the appearance, as we speak, of over 700 types of digital coins, or *crypto-currencies*, called altcoins. And the prospects for increasing the number of virtual coins are developing due to their popularity and media coverage.

The features of *bitcoin* - and at the same time, the features of the large majority of *crypto-currencies* - are strong arguments for their users regarding the decision to use them at the expense of classical banking systems. "Firstly, *crypto-coins* do not exist in physical form (they are digital coins without a classical representation in physical form) and, most importantly, they are a decentralized payment form. So, they are not created or controlled by any governmental institution, nor regulated. Secondly, virtual coins are based on cryptographic protocols and proof-of-work protocols (based on hashing algorithms) as security methods. Thereby, digital currency transactions are safe, irreversible and do not contain personal information from the user. In addition to this feature, virtual money payments can be made without personal information being linked to the transaction - or, at least, apparently, as we'll see below. Thirdly, international virtual money transfers have features that are not applicable to classical payment systems: they are almost instantaneous, there are no commissions in the classical sense of the term for the transfer of the virtual currency, there are no "third parties" involved- which eliminates the so-called "danger" of others having access to sensitive personal data, the transfer is peer-to-peer, without intermediaries and there is no maximum transfer limit or a limit over which transfers are controlled or examined by various institutions (Carata, 2017, pp. 192-198).

Due to this characteristics, for many of its users, *crypto-currency* can provide greater security, privacy, anonymity and flexibility compared to the conventional centralized financial system and, as a result, a much better way to conduct financial transactions while protecting their personal data.

A short analysis of privacy and anonymity in the *crypto-currency* field

One of the most controversial aspects regarding *crypto-currencies* is security, privacy and anonymity. The three notions, albeit similar, are not identical, especially with regard to the online domain. In short, privacy is the control over one's personal information or actions, security represents the freedom from risk or danger, and anonymity can be defined as being unidentifiable in one's actions (Romanosky, 2011).

First of all, *crypto-currencies* are a decentralized payment form and are not created or controlled by any governmental institution, nor regulated, as we speak. To put it in simple terms, instead of a government that prints money for economical purposes via central banks, in the *crypto-currency*

system, every user can "create" its money by *mining* (the mining process implies that users use a specific mining program that solves different algorithms in order to release blocks of coins into the network-in circulation). Furthermore, instead of putting trust in governments and the banking systems to back a currency and maintain its value, the value of the *crypto-currencies* comes from the network of people using it. As a result of all this, no private data are exposed to third parties in transactions – in the classical banking transactions, the third parties are represented by banks, that have access to all the information regarding it and the users involved.

As we have seen before, *bitcoin* – and largely all *crypto-currencies* – are based on a "peer-to-peer (P2P) architecture, which means *crypto-currency* users are able to issue transactions carrying payments in *bitcoins*. To provide some form of anonymity, direct personally identifiable information are omitted from any transaction; instead, source and destination are encoded in the form of public keys, which serve as pseudonyms. Every party can generate as many public keys as he wishes; the corresponding private keys are used to authenticate (sign) transactions and are stored in private wallets either locally on a user's computer or in cloud-storage providers (Ober, Katzenbeisser and Hamacher, 2013).

Furthermore, the block chain technology used by the virtual coins requires that the transactions be exposed in a public register. So, due to the fact that all transactions are stored publicly in the block chain, the anonymity of a user relies on the pseudonym not being linked to his true identity (Möser, 2013).

So, at a first glance, *bitcoin,* as well as all the others *crypto-currency*, is not really anonymous but just hides the true identity of the users behind some pseudonyms. For example, user A transfers to user B a sum of 10 *bitcoins.* Even though the identities of the two are not known, the transaction is still public, for an infinite term.

Last but not least, an aspect of particular interest in terms of "privacy" and "anonymity" in the *crypto-currency* is that related to the transfers of such digital coins. Thus, virtual currency transfers have a feature that is not applicable to classical banking systems: there is no maximum transfer limit or over which transfers are verified by different institutions. In simple words, regardless of the amount transferred between different users or the amounts withdrawn from user accounts, no additional personal data is required. Once transferred, electronic coins can be exchanged in the "classical" currency, such as the euro or dollar, anywhere in the world, through *crypto-currency* "exchanges". No additional verification or validation should be necessary to execute any transaction.

As a first conclusion, based on the arguments previously exposed, *bitcoin* - and the vast majority of digital coins - is built to allow its users to send and receive payments without exposing as much personal data as with classical money transfers and with increased security against hacker threats. However, *bitcoin* – as well as other *crypto-currencies* - cannot be considered anonymous. They only ensure a much higher level of privacy regarding personal data than the classic banking system. As we have seen before, the use of bitcoin leaves traces in the public ledger: all transactions are indefinitely public, even if the real identity of the users is unknown.

A special case in the privacy and anonymity domain of *crypto-currencies*, compared to the features outlined above, is represented by *Zcash* and *Monero* coins.

Due to the fact that *bitcoin* and altcoins in general are not really "anonymous" virtual coins but only offer a higher degree of privacy compared to the classical banking transactions and due to the fact that the need for anonymity remains a topic of high interest among users of this type of coins, *Zcash* appeared on the market.

Zcash is another *crypto-currency* like *bitcoin*, created in 2016 (based on an earlier 2014 protocol) through a collaboration between the researchers at Johns Hopkins University and a group of cryptographers at the Massachusetts Institute of Technology, the Technion – Israel Institute of Technology and Tel Aviv University. Although structurally similar to *bitcoin* and other altcoins, *Zcash* uses innovative cryptography techniques that allow increased privacy and anonymity for its users. In the case of *Bitcoin* and the so-called "traditional" *crypto-currencies*, a transaction consists of an origin address, destination address and the amount transferred. All these transactions are available on a decentralized ledger: the block chain. Because the block chain is public, the history of all transactions can be viewed by anyone. While addresses are not explicitly tied to users' real identities, recent studies have shown that the block chain can be mined to learn information about users' spending habits. *Zcash* extends *Bitcoin*'s protocol by adding new types of transactions that provide a separate privacy-preserving currency, in which transactions reveal neither the payment's origin, destination, or amount (ZeroCash Official Website).

In addition, according to its developers: "*Zcas*h enhances privacy for users by encrypting sender, amount and recipient data within single-signature transactions published to its public block chain ledger". Also "*Zcash* has a distinct advantage in terms of transaction privacy and as a result, anonymity" (ZeroCash Official Website).

So, at a first glance, *Zcash* takes the cryptographic technology of *crypto-currencies* at an innovative level that allows truly anonymous transactions between its users.

In the other case, of *Monero* virtual coin, its creators are unknown to this date (the only available information is a pseudonym of "thankful_for_today"). Just like *Zcash*, although structurally similar to *bitcoin* and other altcoins, *Monero* uses different innovative technologies to enhance the privacy and anonymity of its users.

Unlike most of the digital coins, *Monero* uses a special technology called "ring signatures" which shuffles users' public keys in order to eliminate the possibility to identify a particular user. Untreaceability doesn't protect a receiver from defining his or her balance through inspecting ingoing messages to the user's public address. Therefore, *Monero* employs a specific protocol which generates multiple unique one-time addresses that can only be linked by the payment receiver and are unfeasible to be revealed through block chain analysis. Like any other digital currency, *Monero* is cryptographically secured. Though, the peculiarity of algorithm consists in tremendous computational and electric capabilities that a hacker would need to try to obtain private information regarding the identity or the transactions.

Enhancing privacy and anonymity: TOR

Undoubtedly, *crypto-currencies* - whether we're talking about *bitcoin* or *Zcash* - have a degree of privacy and, sometimes, even anonymity that determine a growing number of people - worried about the security of their personal data and of financial transactions facing hacking threats – to choose them as an alternative financial instruments to the classic financial system.

An additional argument for choosing these alternative financial instruments is to use them together with other innovative technologies, such as anonymous communication technologies, like Tor, to further enhance data protection.

In the case of any communication and transaction system - including financial ones - the issue is to ensure anonymity and security between the information flowing through the network, between senders and recipients, against unwanted attacks outside the network. One of the technologies that ensure this is Tor - a technology that can be used successfully along with *crypto-currency* transactions.

Tor was originally a project created by the American Navy Research Laboratories to protect the online communications of United States of America governmental organizations. As we speak, it is a software that is used globally by users who value the anonymity of their online activity and is represented

by a non-profit organization whose primary purpose is the research and development of tools that offer privacy online.

From a technical point of view, Tor hides the real identity of the user who accesses different sites or carries out various transactions, "strolling" the information through different Tor servers, encrypting the traffic so that the user cannot be traced. The difference between Tor and conventional internet addresses is that Tor uses encrypted addresses with hidden content. Virtually Tor comes to replace classic browsers used in Internet browsing - like Chrome or Firefox. Any communication conducted through the Tor browser is safe, with the main application of being safe in the face of hacker attacks. The data is grouped in encrypted packets before entering the Tor network. After this moment, Tor removes part of the header of this package, which includes information such as the source, size, destination, and timing, all of which can be used to find out about the sender. Next, Tor encrypts the rest of the information, which a normal internet connection cannot do. Finally, encrypted data is sent through many randomly assigned servers, each of which decodes and then re-encrypts enough data to know just where it came from and where it goes.

Even if the two technologies, Tor and *crypto-currencies*, apparently do not have much in common, yet used together considerably increase the degree of privacy and anonymity in the case of financial transactions conducted through alternative financial instruments. Because almost all *crypto-currency* transactions – except the case of *Zcash and Monero* - are stored on the block chain, the data stored includes an amount transferred and the addresses of the sender and the recipient. So every payment has a traceable history that can be viewed by anyone. However, as we have seen before, these addresses are not themselves linked to a person or entity, however a person's identity can be associated with an address through other means. This is the point where Tor software can help protect identity and data. When a *crypto-currency* transaction is run through Tor, the chances of attacks by hackers on the transaction itself or personal data drop dramatically due to the cryptography of the previously presented data.

Conclusions

Throughout the world, technology has reached almost all domains: we are witnessing a spectacular technological advance that has revolutionized all areas, from medicine, education and the aerospace industry to the financial one. And evolution does not stop here. Although in the vast majority of cases the spread of state-of-the-art technologies in all fields offers visible benefits, as a side-effect, we can also discuss about the emergence of potential threats.

This is also the case for personal data protection and the security of financial transactions that are increasingly targeted by hacker attacks and beyond.

The desire to protect data and to secure security leads an increasing number of people to turn to alternative financial services, such as *crypto-currencies*, which, at least apparently, offer a higher degree of protection than the classic alternatives provided by banks. *Crypto-currencies* have become a reality of our days that can no longer be ignored. More and more institutions are turning their attention to this alternative method of payment. For example, the European Union has begun amending its legislation (Directive 849 of 2005), the Japanese government is taking the first steps for the official recognition of *crypto-currencies* and Norway's largest online-only bank, Skandiabanken, recently announced plans to offer customers the ability to link bank accounts to *crypto-currency* holdings. A clear benefit for *crypto-currency* users is the privacy and personal data security. Problems like internal fraud by bank employees that sell the customer data, spammers or scammers are removed in this way. As we have previously shown, the data of *crypto-currencies* users are harder to track.

But there are also controversies about the use of *crypto-currencies* in illegal activities. A recent example is the "WannaCry" malware attack from mid-May 2017, when data on thousands of computers, both individuals and institutions, were encrypted and the required reward was in *bitcoin*. Undoubtedly, the characteristics of virtual coins to represent a decentralized payment form (therefore not created or controlled by any governmental institution, their issuance is not supervised by any central authority nor regulated), the anonymity of its users and their transactions make it more attractive for those who engage in illegal activities and have begun to raise numerous alarm signals for institutions and countries around the world lately. For example, Thailand was the first state in the world to ban the sale and purchase of bitcoin coins or products using this payment system. The decision was motivated by the fact that there are very few laws and capital controls in this area. Soon, in 2014, Russia also followed, which motivated its decision by the fact that the Russian legislation provides for the rouble as the only official currency and the introduction of any other currency or substitute is strictly forbidden.

The antithesis of using *crypto-currencies* for illegal purposes is their use for charitable purposes. Recent news reveal the fact that The United Nations World Food Programme (WFP) uses the Ethereum Blockchain[2] to transfer vouchers based on *crypto-currencies* to refugees in Syria. Completed

[2] Just like Bitcoin, Ethereum is a descentralized cryptocurrency. According to its official website (www.ethereum.org), Ethereum is a decentralized platform that runs smart contracts

on 31st May, the project run by the WFP was designed to direct resources to thousands of Syrian refugees by giving them *crypto-currency*-based vouchers that could be redeemed in participating markets (De Castillo, 2017).

***

Virtual currencies will ultimately be subject to existing regulations in the financial domain and other supplementary systems (as is the case with EU Directive 849/2005). In addition, virtual coins cannot be more "anonymous" than cash and cannot hinder official authority investigations. Also, the whole *crypto-currency* system is built to prevent a wide range of financial irregularities.

References:

1. Carata (Gurău), Cristina, (2017), „Modern methods of financing terrorism in a global and intercultural society: *crypto-currency", Redefining community in intercultural context*, Vol. 6, No.1, pp. 192-198, accessed 1 September at http://www.afahc.ro/ro/rcic/2017/RCIC'17/rcic'17_volume.PDF.

2. De Castillo, Michael, (2017), *United Nations Sends Aid to 10,000 Syrian Refugees Using Ethereum Blockchain*, June 13, accessed on 11 September 2017 at https://www.coindesk.com/united-nations-sends-aid-to-10000-syrian-refugees-using-ethereum-blockchain/.

3. Georgescu-Goloşoiu, Ligia, (2006), *Electronic Banking/E-Banking, Editura Economică*, Bucureşti, 2006 accessed 7 September 2017 at http://ligiagolosoiu.ro/content/Servicii_bancare_electronice.pdf.

4. *Hampton, Paul, (2015), Why banks need a different approach to data security, January 9, accesed 11 September 2017 at* https://www.globalbankingandfinance.com/why-banks-need-a-different-approach-to-data-security/**.**

5. Möser, Malte, (2013), *Anonymity of Bitcoin Transactions An Analysis of Mixing Services*, Münster Bitcoin Conference (MBC), 17–18 July, Münster, Germany, accessed 2 September 2017 at https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf.

6. Romanosky, Sasha, (2011), *Privacy vs. Security vs. Anonymity*, January 4, accessed 3 September 2017 at https://concurringopinions.com/archives/2011/01/privacy-vs-security-vs-anonymity.html.

7. Ober, Micha, Katzenbeisser, Stefan and Hamacher, Kay, (2013), *Structure and Anonymity of the Bitcoin Transaction Graph*, Future Internet, no. 5, pp. 237-250, accessed 2 September 2017 at http://www.mdpi.com/1999-5903/5/2/237/htm.

8. ZeroCash Official Website, accessed on 8 September 2017 at http://zerocash-project.org/.