The Way of Cryptocurrency

Mircea Constantin ȘCHEAU[1], Pop Ștefan ZAHARIE[2]
[1]"Alexandru Ioan Cuza" Police Academy of Bucharest, Romania
[2]"Dimitrie Cantemir" Christian University, Bucharest, Romania
mirceascheau@hotmail.com, popstefan2000@yahoo.com

Cryptocurrency market is estimated at several hundred billion dollars. The number of digital coins has exceeded the threshold of one thousand, each day appearing or disappearing some of them. Volatility, the difficulty in practical operation, high cost, associated risk and particular complexity make it quite difficult to choose one of the products without adequate counseling. Proponents of new technologies presents relevant arguments, while the appellants their call attention to the potential hazards/dangers to which expose themselves the investors. Reality offers us a spectrum that combines measures to limit the phenomenon development with the recognition and support from national and international organisms from which, however, is expected to adopt a joint position on the approach. Born at the end of the first decade of the second millennium, cryptocurrency has begun and continues to raise the interest of financial markets in general and specialized institutions in particular.
Keywords: *Financial Transfers, Cyber-Crime, Money Laundering, Technology, Globalization*

1 Introduction

The The Satoshi Nakamoto alias was used for the first time in 2008, when it was launched on the financial markets a new concept of issuing cryptocurrency based on digital signatures and peer-to-peer trading without having to disclose the identity of the parties and without the transaction to takes place through the involvement of a banking financial institution [27]. The block containing a verified transaction set is added to a chain that contains a history of all transactions and broadcast on the network so that the entire chain of nodes can be updated. Blockchain is a digital register that contains the history of payments made with each unit in circulation. Anonymity incurs operational risk and security risks requiring the adoption of special measures to prevent cyber-attacks or illicit operations. Botnet networks used among others to mine virtual currencies can quite easily create fake traffic on multiple websites. Governance must include in this case restrictive measures to ensure and enforce the legal framework and the regulatory environment. The resilience of a network can be strengthened by increasing the number of nodes, but that the secondary effect is making the data processing process more difficult as a result of the increase in the number of checks.

The blockchain new technology has quickly found applications in the industry, developing in almost ten years after its launch multiple platforms scheduled to store, transfer and manage digital information. In the financial sector, including clearing and settlement operations, reconciliation processes have been streamlined and the degree of security and scalability has been incremented [8]. However, derived currents questioned the consistency of the concept, which experienced a "split" at the end of July 2017. It can show on the bitcoincash.org website that the new "Bitcoin Cash" was officially launched and has experienced rapid growth starting from an initial quote of US $219, and US $ 422 value reached at the beginning of August 2017. Entrepreneurs have managed to create a second version of the cryptocurrency, but as expected, the official bifurcation has spawned conflicts between supporters of the two currents [42]. The way in which Distributed Ledger Technology (DLT), also known under the name of blockchain, works for bitcoin and altcoins (alternatives to bitcoin) is presented in figure 1 [21].

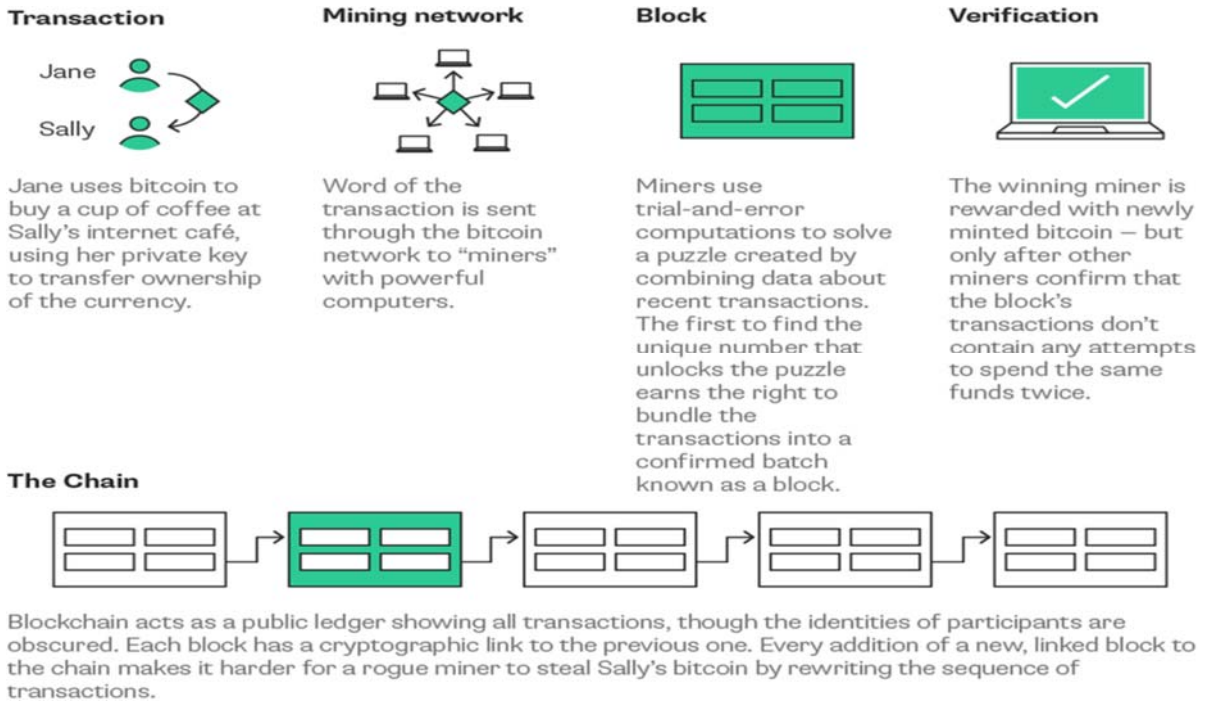

Fig. 1. How Blockchain works for Bitcoin [21]

DLT refers to protocols and infrastructure that allow computing systems in different locations to validate transactions and update synchronized records on a network. A feature of bitcoin and other cryptocurrencies in circulation is the absence of any central institution to govern / support the currency. From here it can maybe born very difficult problem to solve, whose subject is the lack of confidence of the financial markets concerning the widespread adoption of these currencies [1].

2 Arguments for cryptocurrencies and against

Virtual coins can be said that there are items stored in electronic form that can serve transactions as physical currency and does not have any intrinsic value, being supported only by the idea that they can be exchanged for real goods, services or real coins [7]. The launching of a cryptocurrencies by a central bank may have the side effect of a wear and tear of the currency printed on paper [3]. In line with the specifications in a Bank for International Settlements (BIS) report 2017, central banks should however consider introducing their own cryptocurrencies to counter the risks generated by the explosive growth of virtual unit transactions and their value. According to some analysts, the central bank can process payments by debiting the payer's account and crediting the payee's account, the cryptocurrency issued may be complementary to other payment methods used by the central bank [36]. A system based on distributed registry raises access challenges for Real Time Gross Settlement (RTGS) systems but a review for the test environment can provide unexpected solutions [37].

Anonymity is one of the reasons for challenging virtual currencies but is presented and as supporting argument in the context of the need for efficient exploitation by the institutions. Analysis carried out and reviewed by the consortium of major central banks, based in Basel, Switzerland, draws attention to the constant increase in the price of digital currencies. Since the official launch, the bitcoin value has raised over than four hundred times, the average of fluctuations being able to transpose itself into a long-term exponential curve. Derivatives contracts in virtual currencies can be operated on cryptocurrencies trading platforms under regulated conditions, in this way some central banks conferring recognition in 2017 of the new financial concept:

- Swiss Financial Market Supervisory Authority (FINMA) has granted Falcon Private Bank from Zurich permission to manage assets based on the blockchain technology needed for the operation of multiple digital currencies - with the potential for global remodeling, the financial system is based on this technology used to verify and record transactions;
- The United States authorities have accepted an operator, Ledger X, that attracts investors in the desire to diversify their portfolio;
- With help of Chain.com, which is a blockchain infrastructure, Nasdaq Inc. trades for private companies some of the securities;
- With the help of the products offered on the cash market by Digital Asset Holdings, LLC (digitalasset.com), headquartered in New York, the Australian Stock Exchange accelerates its clearing and settlement services;
- In Japan, economic stimulating strategy includes starting from 2017, the legal use of new technologies in the group of official payment instruments.

There are powerful voices such as that of the Austrian Central Bank Governor Ewald Nowotny, who believes that the whole spectrum of cryptocurrencies is exposed to speculative attacks, their vulnerability giving them a degree of instability rather large. In the same vein comes the declaration of the President of the European Central Bank, Mario Draghi, who stated in mid-October 2017 that digital currencies, including bitcoin, are not sufficiently "mature" to be regulated and that innovation must be "appreciated for its potential benefits" but must be also be "critically evaluated" for the risks it causes [5]. That is precisely why some states intend to adopt radical measures to block transactions in a market which was estimated at about $ 184 billion [18] at the beginning of November 2017, while more than one hundred banks and major financial institutions (ex: JPMorgan Chase & Co, Barclays Bank Plc, Banco de la República Colombia, HSBC, etc) have created an international consortium for the purpose monitoring financial transactions and transfers with digital currencies, R3 that builds for the financial markets a new operating system that will exploit the distributed Corda platform (r3.com) being an eloquent example in this case. The total value of cryptocurrency market increased significantly at the end of December of the same year, especially as Bitcoin exceeded the $ 18.000 threshold. On a median line the French Finance Minister was placed [28] when he said he would ask his counterparts in the 20-nation Group to take in consideration the common settlement/regulation of cryptocurrencies (bitcoins), statement taken over by novinite.com.

China, concerned, among other things, by possible actions about the influencing of the financial market or leakage of funds with the purpose of decapitalization, is one of the examples where a state has taken radical measures to prohibit all stock transactions with cryptocurrencies. At the beginning of September 2017, have been outlawed investment funds based on virtual money, which led to a reorientation of subject enthusiasts into a clandestine area. Immediately after the announcement of Chinese-officials was released in public space, the bitcoin dropped to below than $ 4,000, and in mid-October 2017 when the first rumors surfaced that the authorities would review their position, the bitcoin value has exceeded the $ 5,000. At the end of October 2017 bitcoin has exceeded the trading value of $ 6,000 on the BitStamp trading platform and pushed its market capitalization at about $ 100 billion [6] and on November 2 of the same year there was recorded a peak value of 7351, 46 USD / Unit, as can be seen on the coindesk.com website. Growth continued after two major derivatives markets announced in the second half of December 2017 that they received approval from the US Derivatives Authority to list bitcoin futures contracts, settled in cash based on the Bitcoin benchmark, more details being available on cmegroup.com website. Participants at a Conference at the end of September 2017 in Hong Kong on the subject of continued transactions in the light of the new Chinese announced

constraints, noted that it would be rather difficult to impose government control over offline operations as long as there is a consistent demand in this regard. On the other hand, offers are very tempting if we think that credit cards that operate with crypto moneys can also be issued, one of the examples being available on the platinumbitcoincard.com website. It is true that there is an imbalance in the risk / transaction balance and it is believed that will resist only consumers who are well informed and those suppliers who want to provide quality products. Huobi and OKCoin, two of China's largest operators, said it would take some time to update systems in line with the new guidelines PBOC [2]. Cryptocurrencies are not free of phishing or hackers attack [33] and some investment offers were simple cheats what had been implemented only for the purpose of obtaining undue benefits, but some of them were unveiled in a timely manner to limit the losses incurred by investors. The optical problem relating to criminal declared groups or those who try to "transfer" currency abroad to protect their investments or to launder money, is the choice of each of the players. With the hope of obtaining rapid very high incomes, many individuals and / or legal entities assume any unusual risks in a speculative area, and it not surprising at all that pyramid schemes also make their presence felt in this sector too [45]. In the same sense, one of the people quite controversial when we referring to "financial engineering" which caused huge damage, said that the cryptocurrencies promoters they actually set out "the biggest swindle of all time, a huge, gigantic scam that will explode in the end" [41].

On the other hand, the group of banks consisting of Société Générale, Unicredit, HSBC, Deutsche Bank, Natixis, Rabobank and KBC want to use a platform developed on an architecture of blocks Hyperledger Fabric of Linux Foundation, which will be hosted by IBM and will run on IBM Cloud. Blythe Masters, the Digital Asset Holdings CEO, has argued that a rise in the number of transactions via cryptocurrencies may be a solution to the financial crisis because it facilitates direct transfers, recognizing, however, the need for supervision through centralized institutions in order to prevent money laundering and financing terrorism [24]. The IMF Director Christine Lagarde, also believes that by the year 2022 more financial institutions it is possible to adopt financial instruments based on new technologies, and regulations evolution in this area will undergo significant transformations [39].

While the Chinese authorities strongly condemned virtual currency transactions, the Central Bank of China, however, has studied the possibility of adoption in the future of a system allowing for the issuance of its own digital currency and lending to the interbank market in the future when the need for liquidity will make itself felt. The central banks in Denmark, Sweden, Canada and Singapore took into account also to produce their own cryptocurrency in the future, to decrease, on the one hand, the expenses incurred with the issuance and management of existing coins, in order to reduce transaction costs and to adapt to new technological trends, on the other hand. The Danish central bank also wants to outsource cash production by the end of 2018. As I mentioned at the beginning of the article, as a concept introduced simultaneously with the bitcoin currency, a blockchain aims, among other things, chronological record of all electronic transactions and, therefore, it is considered in Denmark the possibility that a blockchain variety to allows for in series (serial-number) of the E-kroner coin, which would provide the desired control from the central bank. Would be increased security and could be more easily sustained the fight against money laundering and tax evasion. Even if there are no in-depth studies indicating the imminence of replacing cash or electronic transactions with those using cryptocurrencies, small-scale scenarios can be developed to analyze the payer's reaction and its effects. Russia, according to the statement of Communications Minister Nikolai Nikiforov, announced in mid-October of 2017 that it will issue its own cryptocoin, CryptoRubla, with the consent of the country's president. The decision would be motivated by the desire to tax

all the revenues from the transactions carried out in this area, without legalizing bitcoin in any case. The speculations have not been delayed to appear, and two of the currents support diametrically opposed views. Stimulating the online economy with fraud prevention measures versus tacit encouragement of the profits derived from money-laundering operations [9]. Experts in geopolitics and geo-economics areas are trying to identify the connection between the positions of the two states, Russian and Chinese, who adopted the same attitude toward the phenomenon generated by digital currencies, at about the same time.

The cryptocurrency market is marked by the emergence of new strategies for fundraising and promotion of new platforms, registering successes or failures depending on the degree of penetration and capitalization. One of the examples is New Economy Movement (NEM) which began with a call to active participants to join a new movement that builds a new decentralized NEMcoin network, as can be seen through the bitcointalk.org (2017) site. Fundraising has as its stated objective the promotion of fairness and egalitarianism according to the principle of 1 account / 1 stake, the idea being to spread NEM on a large scale and equally. The initiative group policy foresees for the distribution of 4 billion NEM, a detention being represented by 1 million NEM. Information may be provided in response to the question "how many shares of NEM you can get?" The basic codes are completely written from scratch (from the beginning) and is intended to combine the best features of Bitcoin, NXT and Bitshare systems, to which their own innovations have been added, making the difference:

- Unlike Bitcoin and other mined coins, all NEMs are distributed directly by the genesis block. Participants (owners) are even their own network nodes that check transactions and protect the network with a hybrid Proof of Stake / Proof of Importance;
- The new method of "harvesting" Proof of Importance rewards nodes that become more important for the network and not necessarily the nodes with the largest number of NEM's; - Support is provided for implementing and assets are listed with a clear expiry date, the asset exchange being designed with automatic settlement functions. Practically, NEM focuses on asset-sharing usability to turn them into a premium platform and fundraising, listing, issuing tokens, and so;
- It provides secure messaging for communication and documents / contracts attached storing.

Discussing about another concept, Crypto20 (C20) is announced as being the "First; Cryptocurrency Index Fund" with the declared aim to manage, depending on capitalization, a diversified portfolio composed of the first twenty most rated cryptocurrencies [34]. The idea is based on the same principle as a fund, whose portfolio is based on the first five hundred companies listed in the United States of America, accessible at investor.vanguard.com. The C20 Fund which should not be confused in any case with a trading platform, was launched in May 2015 and in the first twelve months following the inauguration were run over $ 300 billion. That is why there have been made considerable efforts to ensure that the fund's security policies are adapted so that the level of protection against cyber-attacks is the right one. On the same subject, pioneer researchers who helped develop software for Bitcoin, which is known now as the blockchain, launched a new concept of "block of blocks" at the end of October 2017, which should maintain the value of a cryptocurrency and ensure longevity [20].

The new cryptocurrencies market is trying to consolidate its niche position now and expand its addressability. The wishes proposed cannot be achieved as long as the sector is placed under the incidence of instability susceptibility. Money can be classified as value carriers or as commodity exchange, digital currencies tilting more toward the second category. Unregulated exchange makes the vary effect depending to the parties involved interest. As an example, a transaction which results in the sale / purchase of a real estate trough bitcoin will be accepted by the authorities so as to be considered perfectly legal transfer of ownership of real estate? The question is natural as

long as Sant'Agostino Italian auction house announced in mid-October of 2017 that items putted up for sale can be purchased with bitcoin [43]. If jewelry, watches, paintings and valuable furniture items can be purchased subject to anonymity, how long it will take until land, buildings and immovable property will be evaluated in the same way? And especially how it will be influenced the functioning of the state institutions by the new trend? The question is relevant in circumstances when the second of the world's largest service companies reported for the public that they agreed at the end of November 2017 to be paid with bitcoins as a consideration for the services offered [32]. It is possible that the answer to be provided sooner than we are expecting and in 2018 to witness the development of an interesting experiment on the cryptocurrency market equated as "commodities". Recent measures taken by Venezuela denote in addition to a desperate attempt to recover the economy and a strategy to avoid economic sanctions, as the central bank has declined its responsibility in this regard. Launched in the second half of February 2018 and affirming itself as a first virtual currency officially supported by a state, although it is difficult to identify exactly the institution / government entity in charge of managing it, "Petro" is considered to be be rated at the same value as an oil barrel and guaranteed by existing underground reserves. One of the essential differences toward a bitcoin or another cryptocurrency is the absence of anonymity. It is allowed to be purchased only in US dollars, which implies another limitation, but even under these constraints, it seems that after being initially quoted at $ 60 / unit, it soon became one of the most traded cryptocurrencies on the New Economy Movement [31].

3 Cryptocurrencies and Cyber - Crime

If at the beginning of the year 2016 Loky malware took the first position in the ranking granted to cybercrime interest, 2017 was marked by a rather well-coordinated attack and that allowed rapid infiltration and distribution of an "improved" form of ransomware WannaCry in the networks of the several national / international institutions. Concentrated infections first appeared in Ukraine before spreading worldwide. And this time, the criminals refugee regarding collecting of redemption and hiding traces were constituted the crypto-coins, the amounts varying according to the importance and volume of the information targeted by hackers. The way of action of WannaCry presented in figure nr. 3 [13]. More and more frequent use of digital coins and the growing diversity of attack instruments has led to increasing the complexity of aggressions, frequency, number and intensity. With the appropriate tools can be obtained illegal consistent profits or can be executed, to third parties order, seepage actions, penetration of computer systems or/and destroying them - Crimeware-as-a-Service (CaaS). During of the same operation, the request tactics and redemption collection are changed several times in order to cover up the trails and to make difficult the tasks for the investigators. Therefore, if in the year 2014 the average redemption amount was around 373 USD, in the year 2016 the average went up to USD 1,077 and a South Korean web hosting firm agreed to pay in 2017 an amount of one million dollars to unlock the information stored on their own servers [40]. According to an IBM study, the evolution can be said to be somewhat proportional with the amount of spam that contains the ransomware. At the rate of 0.6% recorded in the year 2015, has grown to about 40 percent at the end of the year 2016 [19]. Two main categories are identified: relatively small sums that allow any domestic victim to pay redemption and significant sums like value when the victim is a corporation or a national / international organization.

The study conducted by Norton Cyber Security Insight has highlighted the fact that globally around 34% of natural victims are willing to pay the requested amount, the percentage in United States of America being 64%. Besides the two above-mentioned reasons, the importance and the volume of infiltrated information, the growth in the percentage of payers may be another reason for increasing the redemptions value. In the case of WannaCry,

even though the average amount demanded like ransom is not considered particularly high, the impact has been felt in over 159 countries, being affected hundreds of thousands of computer systems. We are witnessing a migration of traditional transactions to the online space and especially to the transactions made using mobile phone. Under these circumstances, DoubleLocker, which affected the functioning of Android systems and demanded "payable" redemption, felt its presence in mid of October 2017 and followed a suite of ransomware that caused enough victims in their turn. It is considered an innovative malware because it manages to encrypt the files from mobile phone and changes the access pin [44].

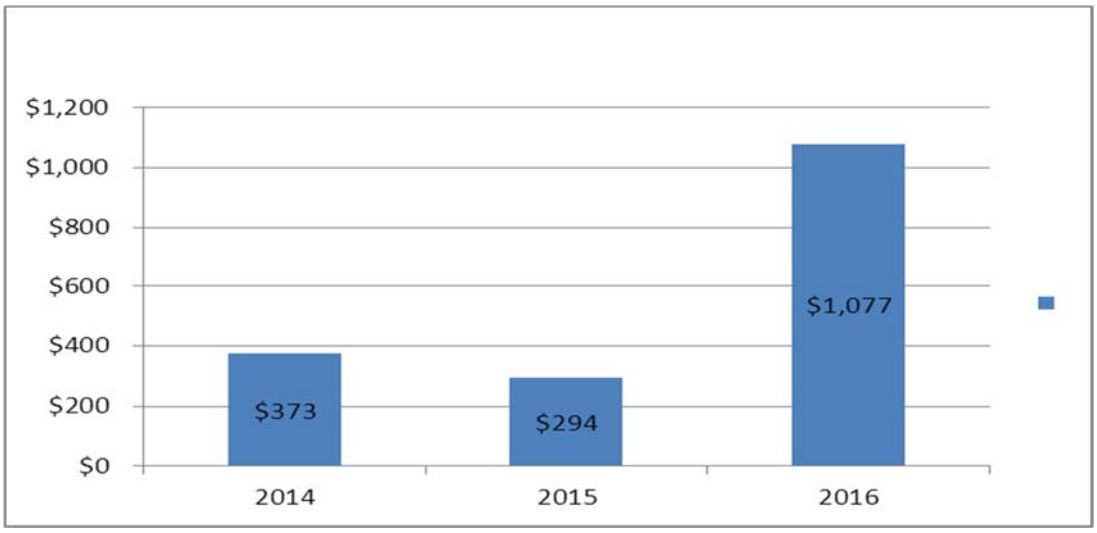

Fig. 2. Average ransom demand [40]

Based on the remote exploitation of a MS Windows vulnerability, known as the SMB protocol (Server Message Block - file sharing protocol on a network), WannaCry is a combination of a worm with the ability to spread across networks without any user interaction, and a file encryption software that requires later redemption for decryption.

In another case related to the infiltration strategy of another Trojan called SamSam, unlike WannaCry, the attackers had penetrated an insufficiently protected public server and have it used as an access / entry point, exploiting a vulnerability to compromise it. With a f.bat script help, a public encryption key and a sqlsrvtmg1.exe executable, have identified and stopped backup processes, have compromised data, and have demanded a 1.5 Bitcoin redemption (about $ 1,587) for each infected computer, but also have provided the "discounts" for multiple unblocked computers belonging to the same proprietary company [30].

No any organization we cannot say that it is sufficiently protected. Even if financial-banking institutions are the main targets of attackers, any company that has financial resources, no matter of the field activity, may become one of the targets of criminal groups. Fraud in the year 2014 of 5000 bitcoin (about $ 1.85 million) was based on a phishing attack directed at a company's CFO. There are cases where the legal shortage in the cryptocurrency field may trigger subsequent conflicts, in the above mentioned case the parties involved being the insuring company and client provided [16].

Other attacks that have used various types of malware were directed to municipalities (San Francisco was one of the victims - Ransom.HDDCryptor), public transport systems, water, gas or energy power supply networks, the redemption requests ranging from one case to another. Even though don't know that there have been directed attacks against medical systems so far, any attack made on a

structure / infrastructure that is directly correlated with public health, can cause collateral damages and loss of lives not taken into account in the first instance by the aggressors and uninvolved / unwatched by them as the main target. An example is the malware that took advantage of vulnerabilities in the Windows operating system, used an exploit called EternalBlue in order to spread itself and forced the closure of several wards of hospitals in the United Kingdom of Great Britain. At the end of June and beginning of July of the year 2017 the Petya virus has speeded rapidly from Russia and Ukraine in almost all of the Europe and the United States of America, the average amount of redemption for each infected computer being $ 300. Have suffered the government systems from Kiev, the French national railway system, port operators in Rotterdam, New York and Argentina, container transport lines operators, oil and gas producers, media companies etc.

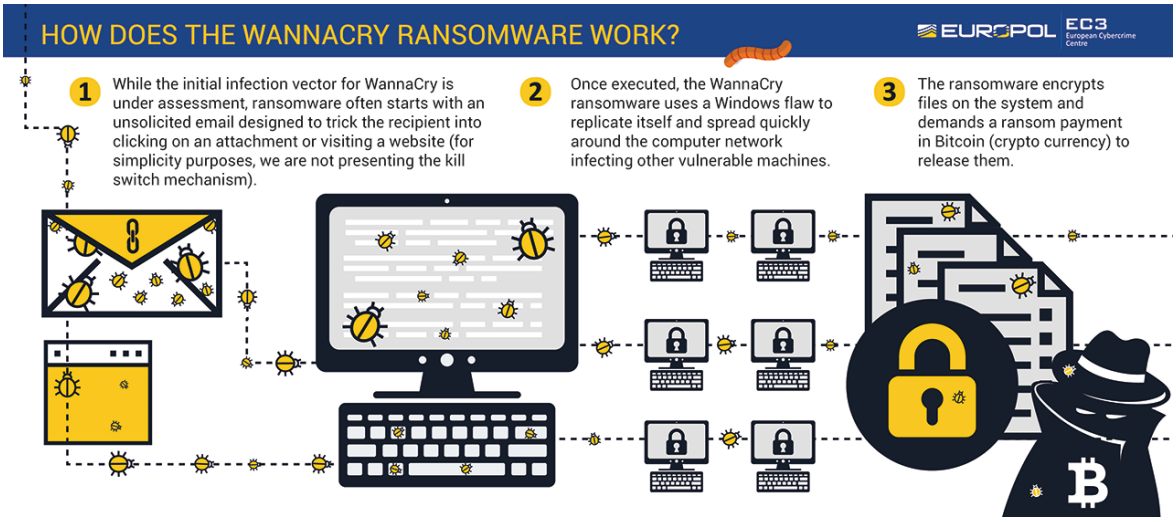

Fig. 3. The way of WannaCry action [13]

It was noted, however, that some attacks did not have registered the same features typically associated with hacker groups who wanted to maintain control of computers in order to obtain incomes, the profile being rather assimilated to powerful corporations or states, leading finally to the idea of an APT (Advanced Persistent Threat). It is more difficult to assign the distribution center of a cyber attack when states or companies aggressor copies the operating modalities and tools that have proven their "efficiency" and reuse them against other enemy states or competing companies [38]. Ukraine is one of the critical areas of hostilities hat also involve components of cyber attacks, the targets being among others the energy sector, the financial sector and last but not least, media organizations. A special case of the year 2016 is the demand for a ransom worth 222 Bitcoin (equivalent to approximately $ 210,000). The procedure of masking the real intentions has failed to fool anyone, especially since Disakil malware, that encrypts key system file functions and erases discs [29], has indicates the direct involvement of Russian Sandworm cyber spy group [35]. Also, the attack based on Petya malware whom I mentioned, was considered to be one of the most powerful ever in Ukraine and directed to destabilize the whole country. Applications for redemption disguised in the form of a simple scheme of extortion were just a simple transparent screen.

Sabotage actions similar to those described above took place previously in the year 2012 and subsequently in the year 2017 in countries considered as allied to peacekeeping groups, one of the victims being Saudi Arabia. Some of the on-line maps (fireeye.com/cyber-map, threatmap.fortiguard.com, cybermap.kaspersky.com) showing cyber attacks

and their geographical location may indicate the idea of an ongoing global conflict.

The particularly virulent and powerful attacks have attracted the attention of the European Cybercrime Center (EC3) and led to the mobilization of the Joint Cybercrime Action Taskforce (J-CAT) so as to establish the response in face of the threat, to limit losses, helping the victims and identify the perpetrators. In addition to the benefits offered, digital currencies represent a threat to the activity of combating money laundering and terrorist financing, there being a clear consensus in this sense At the beginning of 2017, at the joint organized conference by Interpol, Europol and the Basel Institute on Governance in Doha, Qatar, attended by over four hundred investigators specialized in investigating money-laundering operations, the severity of these threats was recognized in the context in which the digital currencies have become part of the payment systems [14]. The most advanced form of money laundering, which is currently considered and the biggest challenge today facing AML departments, is "transaction laundering". The platform for unauthorized financial activities is based on the global aspect of e-commerce and the minimum "know your customer" requirements [15]. Reality obliges to be adopted the necessary measures to meet the challenges:

- To intensify the exchange of information in the field of money laundering and of the digital currencies;
- Regulation of the trade in digital currencies and the activity of portfolios suppliers , in line with the current legislation;
- The adoption of measures aimed to combat transaction anonymization procedures.
- For investigative actions to be successful, cryptocurrencies are used by law enforcement agencies themselves.

An important success was achieved in the year 2016 when it was decomposed one of the largest networks of producers of false euro coins / counterfeit, online offered for sale on the black market (Darknet). Bitcoin has been used to pay for banknotes, in this case have been cooperating law enforcement authorities from Netherlands, Sweden, Germany, Austria, France, Lithuania, Italy, Spain and Portugal [12]. In the conference held in mid-June of the year 2017 at Europol's Hague headquarters, talks have been resumed on the "Bitcoin ATM" network and on the new criminal areas where cryptocurrencies are used. There have been registered over 55 million illegal transactions were have been washed more than $ 6 billion, a large portion of the sum coming from drug trafficking and smuggling activities [11]. With the desire to prevent and to limit the use of blockchain technology for criminal purposes, a group of fifteen members, including international institutions, government institutions, educational / research institutions and financial institutions from several countries, initiated a project funded by European Union. The idea is to develop a technical solution for the investigation of crime, combating terrorism involving virtual currencies, limiting black market transactions and protect legitimate users while respecting the rights referring to confidentiality [23].

4 Conclusions

The word "digital" has become so present and used in dissertations that's meaning is no longer always very clear [4]. The concept behind the virtual currency trading provides the necessary anonymity screen for criminal groups, money laundering operations being felt as a necessity for the offenses based on cybercrimes. The reality presents the need for a legislative uniformity, which to provide resolution to some of the controversies that have led to a decrease in confidence in an IT field collaboration within the European Union. In an attempt to prevent crimes, the measures must be imposed even globally and must be implemented on all levels, especially as the on-line environment offers tools becoming more sophisticated and difficult to monitor. An important step was completed in of the year June 2016 when was adopted the NIS Directive [10] concerning on common measures to security of networks and information systems in the European Union, date 9 May 2018 being the deadline until which "Member

States must transpose and adopt in the national law the normative acts by law and regulatory and administrative acts for transposition and implementation" [25], [26]. In September of the year 2017 Information Security Forum (ISF) launched the European Union's General Data Protection Regulation (GDPR) Implementation Guide**.** There are presented the latest information regarding best practices, which can be benchmarks to which the Member States of the European Union can relate, this aspect being also mentioned by Global Security Mag [17]. Population awareness programs and active involvement of high school and university students can contribute to the development of culture in the field of security. Public-private partnerships, timely reporting of incidents to State bodies that have responsibilities in maintaining state security, and a positive attitude needed to build a common front against cyber-aggression will make the reaction times and losses significantly diminish. An example is presented by Interpol, the official statement in which it is mentioned that "Interpol and Kaspersky Lab signed a new threat exchange agreement in October 2017, which will lead to increased cooperation between the two organizations for prevention and fight against cybercrime" [22]. The fight against cybercrime will suffer mutations dictated by technological evolution and new strategies adopted by criminals in their efforts to disguise illicit activities among legal ones. The cryptocurrencies era I think it can offer many surprises in the future - bad and good. Under the conditions of adopting a common law enforcement taxonomy and developing / supporting national networks of cyber security response teams (CERT / CSIRT), the continuous effort of international organizations will be directed as before to prevent and combat cybercrime.

References

[1] Bech, M. and Garratt, R. (2017, September) Central bank cryptocurrencies. *Bank for International Settlements*, *International banking and financial market developments*. Available: https://www.bis.org/publ/qtrpdf/r_qt1709.pdf.

[2] Bloomberg, (2017, February 10). China Bitcoin Exchanges Halt Withdrawals After PBOC Talks [Online]. Available: https://www.bloomberg.com/news/articles/2017-02-10/china-bitcoin-exchanges-halt-withdrawals-after-central-bank-talk.

[3] Bordo, M. & Levin, A. (2017, August). Central Bank Digital Currency and the Future of Monetary Policy. Available: https://www.hoover.org/sites/default/files/research/docs/17104-bordo-levin_updated.pdf.

[4] Broadbent, B. (2016, March 2). Central banks and digital currencies, speech given at the London School of Economics [Online]. Available: https://www.bis.org/review/r160303e.pdf.

[5] Charpal, A. (2017, October 19). Criptocurrencies like bitcoin are not 'mature' enough to regulate, ECB chief Mario Draghi says. *CNBS.* Available: https://www.cnbc.com/2017/10/19/cryptocurrencies-are-not-mature-enough-ecb-chief-mario-draghi.html.

[6] Chavez-Deifuss, G. (2017, October 20). Bitcoin soars to record high above $6,000. *Business News, Reuters.* Available: https://www.reuters.com/article/us-markets-bitcoin/bitcoin-soars-to-record-high-above-6000-idUSKBN1CP2K1.

[7] CPMI. (2015, November). Digital currencies. *Bank for International Settlements.* Available: https://www.bis.org/cpmi/publ/d137.pdf.

[8] CPMI. (2017, February). Distributed ledger technology in payment, clearing and settlement, An analytical framework. *Bank for International Settlements.* Available: https://www.bis.org/cpmi/publ/d157.pdf.

[9] Coldewey, D. (2017, August). Russia may soon issue its own official blockchain-based currency, the CryptoRuble. *TechCrunch.* Available: https://techcrunch.com/2017/10/15/russia-may-soon-issue-its-own-official-

blockchain-based-currency-the-crypto-ruble/.

[10] EU. (2016). Directive 2016/11481 [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.193.01.0001.01.ENG.

[11] Europol. (2014, June 14). Cybercrime Experts Tackle the Criminal Exploitation of Virtual Currencies [Online]. Available: https://www.europol.europa.eu/newsroom/news/cybercrime-experts-tackle-criminal-exploitation-of-virtual-currencies.

[12] Europol. (2016, December 16). Eight Arrests in Counterfeit Euro Operation Supported by Europol [Online]. Available: https://www.europol.europa.eu/newsroom/news/eight-arrests-in-counterfeit-euro-operation-supported-europol.

[13] Europol. (2017). Wannacry Ransomware [Online]. Available: https://www.europol.europa.eu/wannacry-ransomware.

[14] Europol. (2017, January 18). Global Conference on Countering Money Laundering and the Misuse of Digital Currencies [Online]. Available: https://www.europol.europa.eu/newsroom/news/global-conference-countering-money-laundering-and-misuse-of-digital-currencies.

[15] EverCompliant. (2017, January 23). Transaction Laundering is the New, Advanced form of Money Laundering [Online]. Available: http://evercompliant.com/transaction-laundering-new-advanced-form-money-laundering/.

[16] Finextra. (2015, September 17). BitPay loses $1.8m in phishing attack [Online]. Available: http://www.finextra.com/news/fullstory.aspx?newsitemid=27865&topic=security.

[17] Global Security Mag. (2017, September). Information Security Forum Releases GDPR Implementation Guide, White paper [Online]. Available: http://www.globalsecuritymag.com/Information-Security-Forum,20170928,74049.html.

[18] Kelly, J. (2017, November 1). Criptocurrencies' total value hits record high as bitcoin blasts above $6,500. *Fintech, Reuters.* Available: https://www.reuters.com/article/us-globalmarkets-cryptocurrencies/cryptocurrencies-total-value-hits-record-high-asbitcoin-blasts-above-6500-idUSKBN1D14BM.

[19] Kesern, L. (2016). Ransomware: How consumers and businesses value their data. *IBM Security, IBM.* Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN&.

[20] Kharif, O. (2017, October 24). Bitcoin Pioneer Says New Coin to Work on Many Blockchains. *Bloomberg Technology.* Available: https://www.bloomberg.com/news/articles/2017-10-24/bitcoin-pioneer-says-new-coin-to-work-on-multiple-blockchains.

[21] Kharif, O. & Leising, M. (2018, January 29). Bitcoin and Blockchain. *Bloomberg QuickTake.* Available: https://www.bloomberg.com/quicktake/bitcoins.

[22] Interpol. (2017) Interpol and Kaspersky Lab sign new threat intelligence exchange agreement [Online]. Available: https://www.interpol.int/News-and-media/News/2017/N2017-137.

[23] Interpol. (2017, May 24). Project to prevent criminal use of blockchain technology launched by international consortium [Online]. Available: https://www.interpol.int/News-and-media/News/2017/N2017-069.

[24] Johnson, K. (2016, June 14). Cryptocurrency a Response to Financial Crisis, Says CEO. *The Wall Street Journal.* Available: http://www.wsj.com/video/cryptocurrency-a-response-to-financial-crisis-says-ceo/D28A8012-413F-447E-AA5A-F1911BA64FC3.html.

[25] MCSI. (2017). Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. Proiect [Online]. Available: https://www.comunicatii.gov.ro/wpcontent/uploads/2017/06/Proiect-lege-NIS-20171002.pdf.

[26] MCSI. (2017). Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. Expunere de motive [Online]. Available: https://www.comunicatii.gov.ro/wp-content/uploads/2017/06/NotaFundamentare-NIS-20171002.pdf.

[27] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[28] Novinite. (2017, December 20). Bitcoin Might Soon Face Tougher Regulations in Europe [Online]. Available: http://www.novinite.com/articles/186410/Bitcoin+Might+Soon+Face+Tougher+Regulations+in+Europe.

[29] Paganini, P. (2017, January 12). BlackEnergy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure. *Infosec Institute.* Available: http://resources.infosecinstitute.com/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/#gref.

[30] Paganini, P. (2017, June 25). SamSam ransomware attacks increase and crooks demand higher ransom. *Security Affairs.* Available: http://securityaffairs.co/wordpress/60396/malware/samsam-ransomware-higher-ransom.html.

[31] Perera, F. S. (2018). Bitcoin, move over. There's a new cryptocurrency in town: The Petro. *Analysis, The Washington Post.* Available: https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/26/bitcoin-move-over-theres-a-new-cryptocurrency-in-town-the-petro/.

[32] Russolillo, S. (2017, November 30). Bitcoin Goes to the Big Four: PwC Accepts First Digital-Currency Payment. *The Wall Street Journal.* Available: https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/ articles/pricewaterhousecoopers-accepts-fee-in-bitcoin-1512036992.

[33] Schroeder, S. (2017, December 21). Cryptocurrency exchange EtherDelta got replaced with a fake site that steals your money. *Tech, Mashable.* Available: http://mashable.com/2017/12/21/etherdelta-hacked/#7C4LnGMwgaq3.

[34] Schwartzkopff, D., Schwartzkopff, L., Botha, R., Finlayson, M. & Cronje F. (2017). CRYPTO20: The First Tokenized Cryptocurrency Index Fund [Online]. Available: https://static.crypto20.com/pdf/c20-whitepaper.pdf.

[35] Seals, T. (2016, January 5). Sandworm Team Could Be Behind Ukraine Power Grid Attack. *Magazine, InfoSecurity Group.* Available: https://www.infosecurity-magazine.com/news/sandworm-team-ukraine-power-grid/.

[36] Selgin, G. (2008). Milton Friedman and the Case Against Currency Monopoly *Cato Journal.* Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.170.4468&rep=rep1&type=pdf.

[37] Shafik, M. (2016, January 27). A New Heart for a Changing Payments System, speech given at the Bank of England [Online]. Available: https://www.bankofengland.co.uk/-/media/boe/files/speech/2016/a-new-heart-for-a-changing-payments-system.pdf?la=en&hash=1449DFDBB245C185C706C155D5282ACF15B11CDB.

[38] Sheridan, K. (2017, April 10). Nation-State Attackers Steal, Copy Each Other's Tools. *Threat Inteligence, Dark Reading, InformationWeek.* Available: https://www.darkreading.com/threat-intelligence/nation-state-attackers-steal-copy-each-others-tools/d/d-id/1330052.

[39] Smart, E. (2014). IMF's Cristine Lagarde Says Bank Will Adopt Digital Currencies in 5 Years Time. *Cointelegraph.* Available: https://cointelegraph.com/news/imfs-christine-lagarde-says-bankswill-adopt-digital-currencies-in-5-years-time/.

[40] Symantec. (2017, April). Internet Security Threat Report, volume 22 [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[41] Titcomb, J. (2017, October 23). Wolf of Wall Street Jordan Belfort says initial coin offerings are 'the biggest scam ever'. *Technology, The Telegraph* Available: http://www.telegraph.co.uk/technology/2017/10/23/wolf-wall-street-jordan-belfort-says-cryptocurrency-offerings/.

[42] The Economist. (2017, August 5). Bitcoin divides to rule, The crypto-currency's split into two versions may be followed by others. *Knives and forks.* Available: https://www.economist.com/news/business-and-finance/21725747-crypto-currencys-split-two-versions-may-be-followed-others-bitcoin.

[43] The Local. (2017, October 19). Italian auctioneers to accept bids in Bitcoin [Online]. Available: https://www.thelocal.it/20171019/italian-auction-bitcoin.

[44] WeLiveSecurity. (2017, October 16). DoubleLocker Android ransomware explained [Online]. Available: https://www.welivesecurity.com/2017/10/16/doublelocker-android-malware-explained/.

[45] Yap, C.W. (2017, October 4). After Bitcoin Crackdown, Cryptocurrencies Go Clandestine in China. *The Wall Street Journal.* Available: https://www.wsj.com/articles/in-china-cryptocurrency-sales-persist-in-the-shadows-1507109400.

Mircea Constantin ȘCHEAU has graduated the Faculty of Automation, Computers and Electronics in 1996.and Faculty of Economic in 2008. He is PhD Candidate in Public Order and National Security, "Alexandru Ioan Cuza" Police Academy of Bucharest, with a theme of interest for the economic and national security domain - Cyber Crime regarding Financial Transfers. Until now, he is the author of 2 books and more than 15 journal articles in the field of economic, security and informatics.

Pop Ștefan ZAHARIE has graduated School of Officers of the current "Alexandru Ioan Cuza" Police Academy of Bucharest in 1982 and Faculty of Law from Sibiu in 1995. He is PhD in Law, "Alexandru Ioan Cuza" Police Academy of Bucharest, with the theme "The role of community police in the rule of law". Until now, he is the author of more than 25 books and more than 30 journal articles in the field of human rights, criminality and security. Currently he is Professor Assistant at "Dimitrie Cantemir" Christian University.