DOI: 10.5281/zenodo.4058353

MANAGEMENT OF CYBERCRIME IN THE FINANCIAL FIELD - PERSPECTIVES TO COMBAT THE PHENOMENON

Robert HELLVIG, PhD Student
Athenaeum University, Bucharest, Romania

Cătălin DUMITRESCU, PhD Lecturer
Athenaeum University, Bucharest, Romania
catalindumi@yahoo.com

Matei DUMITRESCU, BA Student
Department FABIZ, University of Economic Studies
mateidumi7@gmail.com

Abstract: *The contemporary context requires us to be efficient, and to achieve this goal we must be up to date with the latest information and the latest technological innovations. Human society is in a new stage of development whose vectors are represented by digitalization, innovation and globalization. Through intelligent systems and techniques in the form of computer systems and artificial intelligence, the degree of satisfaction of human needs has reached a much higher level. Information and telecommunications technology takes control in more and more aspects of life, in the vast area of benefits and huge transformations induced by the digitalization of society finding an unprecedented speed of information flow, reducing distances and response time, the development of e-commerce (e-commerce), the crystallization of the highly digitized goods and services sector which includes digitally delivered products and services with predominantly digital content, the development of distance learning (e-learning), bank cards, transfers and electronic payments intensify cash flows, allowing capital movements to move to all corners of the world in a fraction of a second, the restructuring of companies and business in general, management being forced to adapt to the stresses of globalization and diversification, changing social relations.*

Keywords: *Blockchain, Ledger Technology, Bitcoin, IT crimes, Money Laundering, cryptography, technology*
JEL Classification : *C23, C26, C38, C55, C81, C87*

Introduction

Seen from this perspective, of the digitalization and globalization of activities, in which corporations expand their sphere of action beyond national borders, creating networks of strategic alliances, it is predictable the phenomenological change of large financial scams that endanger national, regional or even international economic stability. In the context of the information explosion in all fields, traditional crime has adapted to the economic, financial and social situation, increasing the degree of refinement of activities. The dominant role of state-of-the-art information and communication technology, the new realities outlined in the sphere of financial innovations, makes some criminal acts more effective, aspects that are reflected in a new dimension of traditional crime, cybercrime. Unlike traditional crime, the specificity of cybercrime is given by the complexity of the means used and the magnitude of the result. Similar to classic crime, cybercrime can take a wide range of ways and can be found in a variety of social settings. Thus, the computer is becoming more and more involved in all forms of delinquency.

The issue of cybercrime and the management of the activity of preventing, investigating and combating this form of crime is a concern for both the theoretical side, the profile literature and the practical side, large private corporations, companies that offer security solutions cybernetics, law enforcement agencies, implicitly the level dedicated to public order and national security, but also a concern of individuals. In the context of the intensification of cybercrime, there is a broad convergence of opinions among specialists in the field, when they describe the changes in traditional crime in general and in economic and financial crime, in particular, in the sense that they claim with the more urgent changes in the tools for detecting and countering cybercrime, as well as in the field of cyber security strategies. The increase of attention on the approach of cybercrime is justified on the one hand by the ambiguity of the definition of theoretical terms and concepts, which find a severe invalidation in practice taking into account the diversity of reality, on the other hand the low level of training of persons in the field of cyber security explainable by the high level of technology in the field, and on the other hand by the specificity of cybercrime to launch large-scale attacks and operations, escalating national borders and defying time zones.

1. Cybercrime trends

The cybercrime landscape continues to evolve as criminals seek to adopt increasingly effective and profitable attack tactics. Cybercriminals are increasingly busy identifying new and advanced attack techniques, ranging from „families" of malicious programs to personal computers to malicious programs for smartphones, from viruses to personal computers to illegal cloud-based facilities. At the same time, the cybercrime sector is advancing rapidly amid competition from malicious software vendors, which is leading to increased innovation. The underworld continues to develop service packages that allow more and more evaders to get cash, without having to understand what the fraudulent circuit is, how to carry out a phishing or spamming attack, or what are the requirements of IT infrastructure. The market for services in the range of cybercrime is growing so fast that providers of such services are forced to work harder than ever to win and retain customers. Attractive options for potential customers include demo versions of products that can be tested before they can be purchased (for example, smartphone apps that buy compromised payment cards), money back guarantees, or reparation of damages (as an example we mention the case in which a purchased payment card is canceled by the legal holder-victim, the buyer is given another card or refunded), forums that allow grades to be given to sellers and services provided, posting comments, reporting sellers scamming buyers.

Smartphones are gaining an increasingly important role in everyday life. Smartphones are used for an increasing number of activities and often store sensitive data, such as contact information and passwords. Recent innovations in e-commerce allow users to make transactions on smartphones. As the penetration rate of smart phones in society reaches record levels globally, cybercriminals are increasingly targeting these smart mobile computing devices. Lately, the most significant increase has been registered by the banking Trojans that penetrate smart phones.

Recent studies have revealed a development of the types of cyber attacks as cybercriminals have sought new ways to steal credit cards and gain unauthorized access to money. Instead of wasting time launching phishing attacks or using online social engineering on individuals, cybercriminals break into the computer systems of major trade concerns and steal identification data stored in databases. To counter these trends, law enforcement organizations and agencies need to opt for information-based security and fraud prevention approaches that can take place in mobile and cloud environments, make more use of behavioral analysis, and take advantage of the capabilities of smart mobile devices to protect users and the data stored on them. Even if attacks cannot be completely blocked, access to the right information makes it possible to detect a cyber attack faster, significantly reducing the attacker's area of operation and opportunities and minimizing the potential for loss or damage to computer data. In the process of identifying and locating international cybercriminals related to cyber intrusions, bank fraud, data breaches, and other crimes related to computer systems, law enforcement agencies are required to prioritize the recruitment and training of technical experts, to develop standardized methods of investigation and exchange of best practices and response tools on cyber incidents. Cybersecurity investigators and experts face the challenge of understanding in detail the ways and malicious techniques used by cybercriminals, as well as the vulnerabilities that are their potential targets, to effectively respond to and investigate security incidents cybernetics. Against the background of the diversification of cyber attacks, the development and use of Blockchain technology, mainly in the financial sector, will become a tool to stop financial crime.

2.Blockchain applications in the financial sector and their impact in the fight against money laundering and terrorist financing

The analysis of the specialized literature carried out in the first two parts of the paper, allowed me to acquire essential knowledge about the analyzed concepts - the magnifying glass against money laundering and the financing of terrorism and blockchain technology. The information collected from credible sources and authors provided a solid knowledge base, necessary to understand the relationship between the two topics addressed. Furthermore, the next section will address the impact of blockchain technology on the prevention of money laundering and terrorist financing by financial institutions. To do this, I will analyze how blockchain-based solutions for financial institutions implement the basis of the major components of money laundering / terrorist financing prevention (data quality, reporting to regulators, data security and confidentiality).

After discussing the problems caused by money laundering activities through an institutional framework, this paper aims to present a feasible solution to combat money laundering, specially designed for Bitcoin. Game theory serves as a powerful tool for observing and analyzing incentives, which is why this paper invents several theoretical game models, aiming to create incentives to prevent the attractiveness of money laundering. The feasibility of the above-mentioned model will be carefully examined. Before analyzing the applications of the blockchain on the financial sector, especially in the banking field, it is important to look back and understand how the financial sector has evolved as we know it today.

The traditional banking industry follows a centralized structure. In its primary and basic form, it consists of individuals who use banks to deposit their fiat money. Of course, banks offer useful services, deposit accounts being the most important products of banking. If a third party manages the funds and transactions of customers, it is obviously subject to payment for services. So why do people pay these taxes instead of keeping their own financial assets? The answer is as simple as a cost-benefit analysis - the benefits of using centralized banking services outweigh the costs. We can conclude that there are three main advantages in using centralized banks, the first being security. If individuals would deposit their funds in their homes or choose to carry their monetary assets on them, there would be some associated risks - natural disasters or theft that would lead to the disappearance of money. In fact, not claiming funds can, in some cases, be considered tax evasion or money laundering.

The second reason why individuals choose to place their funds in a bank is, so far, the most efficient way to store and manage money. Banks facilitate day-to-day financial activities, such as paying bills, transferring money to others, and purchasing goods or services. In fact, accessing personal finance has become increasingly easy with online banking and mobile applications that allow individuals to check their accounts and balances through mobile devices. Finally, banks generate added value to their customers, rewarding them with interest, even if interest rates are low (Egilsson, 2017). Until the creation of Bitcoin, there was no alternative to centralized financial services. Digital banking has become a reality, raising the issue of double spending. However, Bitcoin has emerged as the first cryptocurrency that has not allowed spending to be doubled, making digital banking a feasible reality. Blockchain allows users to convert fiat money into cryptocurrencies without the need for an intermediary. Also, due to the decentralized structure of the technology, peer-to-peer transactions can take place without the permission of a central entity, such as a bank, because the validation of transactions is done through consensus mechanisms. The high level of security offered by the blockchain is largely caused by the principle of immutability.

As mentioned earlier in the report, it is extremely difficult to change any data embedded on the blockchain, as it would require a large amount of time, effort and computing power. In addition, each information is encrypted using a hash function that is a one-way function, which means that the hash code cannot be returned to the data originally converted to code. The decentralized structure of the technology implies that blockchains cannot be modified from a single computer, because they are not located in a single location, but distributed in peer-to-peer networks. Therefore, for a single party or group of entities to gain control over the blockchain, an extraordinarily large amount of computing power would be required to simultaneously access and modify a minimum of 51% of the blockchain (Miles, 2017). The 51% attack is more common in public networks that use Proof-of-Work to validate transactions. The security level of a blockchain varies depending on the type of network - public or private. Public networks can be accessed by anyone with an Internet connection, but blockchain actors remain anonymous. Thus, public blockchains, such as Bitcoin or other cryptocurrencies, pose a higher risk due to the lack of access restrictions - anyone can be part of the network without first having to declare their identity. In a private setting, access is usually restricted to members of an organization. Here the principle of anonymization is not valid, because the organization controls read and write permissions. Moreover, all participants are required to identify themselves in order to have access to the network (Ometoruwa, 2018). Miles points out that the potential security problems of private networks, coming from malicious people, can be solved with a highly secure infrastructure. According to the author, such an infrastructure must prevent unauthorized parties from accessing sensitive data - even root users and system administrators, refusing any attempt to change blockchain information that would cause illegal activity and save encryption keys (Miles, 2017).

Compared to centralized systems, blockchain offers increased efficiency in cross-border transfers and transactions. In a traditional banking structure, cross-border transfers are subject to a longer validation process than domestic transfers, often taking longer, often several days, until the transfer is completed. Blockchain does not have a separate procedure for validating domestic or cross-border transactions. Therefore, the process of verifying cross-border transactions is more efficient with blockchain, which is an important feature, given the importance of global trade today. As mentioned earlier, banks have service fees associated with their range of financial products. These fees are necessary for banks to cover their costs and continue their business. On the other hand, financial institutions also reward customers with interests. When it comes to costs, a blockchain network, once established, does not require additional expenses on behalf of members, but only the usual maintenance costs. There are cases where cryptocurrencies are offered as incentives to reward participants in transactions, as previously explained when using Proof-of-Work.

It is reasonable to imagine a future with both centralized and decentralized banking. From the customer's point of view, the fact that both options are available is a positive aspect, as there will be more alternatives for managing finances. However, from the point of view of financial institutions, decentralized banking is a new competitor. In addition, it is extremely important for financial institutions to develop appropriate strategies to deal with this new reality. In fact, banks have begun to adopt blockchain-based structures to capitalize on the benefits of technology.

The benefits of adopting Blockchain ecosystems by financial institutions

Trading. The traditional asset trading process can be divided into three distinct phases - execution, clearing and settlement. The first occurs when the individual or organization selling the guarantee finds an entity willing to buy. Once the counterparties agree to the terms of exchange, the procedures for transferring the collateral property to the buyer and the payment to the seller begin. These procedures are part of the clearing stage, the most complex of the three stages (Fronda, 2019), because this stage includes - placement, calculation of financial margins, and management of risks associated with the transaction (Rodgers, 2019). Finally, the settlement takes place once the transaction is completed, which means that the security guarantee is fully assigned to the buyer and the money is available in the seller's account. According to Benos and Gurrola from the Bank of England, the traditional asset trading process, namely the clearing and settlement stages, can be time and money consuming. To ensure that the risks inherent in the exchange are properly managed and mitigated, banks use several complex procedures. Consequently, transaction costs increase and the settlement can take up to three days to complete (Benos, 2017: 2-5). Blockchain eliminates the need for third party intervention in the exchange of securities, because the payment goes directly to the seller's wallet and vice versa. Distributed ledger technology also allows the settlement time to be reduced from two to three days to a maximum of a few seconds or a few minutes. However, real-time settlement is only possible if a cryptocurrency is used as a method of payment, otherwise banks are required to convert fiat money into cryptocurrencies in order to complete the transaction. Due to currency volatility, this process could be difficult to accomplish. McKinsey suggests using stable currencies as a solution to the problem of volatility, because the value of these currencies is related to real-world assets. However, an intermediary must still perform the conversion (Higginson, 2019).

Cross-border payments. Similar to asset transactions, cross-border transactions are also associated with high costs when it comes to settlement time. Thus, distributed ledger technology could be a suitable alternative. However, conversion and volatility are significant when talking about cross-border payments, as each transaction involves at least three distinct currencies: the sender's national currency, the cryptocurrencies to which fiat money must be converted to be used in the blockchain network, and the national currency of the recipient. Compared to asset trading (assuming the buyer and seller are from the same country), each transaction requires at least two currency conversions, instead of one. Volatility issuance also increases when we use an additional currency. However, several companies have managed to develop appropriate cross-border blockchain-based payment systems. In the financial sector, Santander Bank has pioneered the development of a cross-border payment service based on distributed ledger technology. On April 12, 2018, the Spanish bank launched Santander One Pay FX. The technology behind it is xCurrent, a distributed ledger technology developed by Ripple. The service allows international transfers to be settled on the same day, in most cases, or the next day. In addition, senders can view, in consultation, the exact amount that the correspondent will receive at the destination, in case of transfer (Santander, 2018).

Data Base. Auditors face certain challenges in their work, especially when auditing large companies that have a multinational field of activity. The information is dispersed through various databases within the organization, which makes it difficult to examine it globally and detect any problems. The blockchain would allow the standardization of accounting and data storage, while providing a relevant analysis of customer activity in a single data warehouse. The transparency and immutability features inherent in this technology make it attractive to auditors and regulators. Because all transactions on the blockchain are endowed with a "time stamp," it is possible to perform an unrestricted audit trail, as auditors can easily track and reconstruct the records of all transactions. The quality and veracity of records kept by financial institutions is another predominant issue, which not only makes auditing a long and difficult process, but also harms the day-to-day business of financial institutions. After design, all transactions must be validated and verified to be part of the blockchain. Regardless of the consensus mechanism chosen, the veracity of the records kept in the distributed register is ensured.

Identity and data privacy. Although confidentiality and transparency seem to be opposing concepts, a distributed record technology allows both attributes to coexist perfectly. In public networks, the degree of confidentiality is higher compared to the degree of transparency, because members are allowed to choose what identity elements they transmit to the network - because blockchain data is cryptographically secure, individuals can act anonymously if they wish to do so. this thing. On the other hand, not all members have the same permissions in private blockchains. If regulators belong to the Blockchain network, they may be allowed to disclose the identity of other members of the blockchain, while another element, such as a customer of a financial institution, will not receive this access. Therefore, transparency goes beyond confidentiality in this case.

However, if permissions are allocated correctly and carefully, confidentiality can continue to be maintained, providing the necessary transparency for regulators and supervisors.

3. Disadvantages in Blockchain adopting

Despite the advantages offered by the distributed registry, there are several obstacles that prevent financial organizations from adopting blockchain-based strategies. Between February and March 2019, Deloitte conducted an international blockchain opinion poll on a sample of 1,386 senior executives from various financial organizations, along with 31 Blockchain ecosystem developers. The main barriers to adopting and investing in blockchain technology, which respondents specified are: regulatory issues (30%), replacement of old systems (30%), potential security threats (29%) and lack of knowledge, and internal skills (28%). However, 86% of respondents agreed that the blockchain is sufficiently scalable to obtain use validation, and 83% of respondents mentioned that blockchain use is the perspective in the financial system (Deloitte Global Blockchain Survey, 2019). PricewaterhouseCoopers (PwC) conducted a similar survey in 2018. The sample used was much smaller compared to the Deloitte sample size but was more significant as it included 600 CFOs from 15 different geographical regions. Respondents listed similar barriers to the adoption of distributed networks, namely regulatory uncertainty (48% 2), lack of trust among employees (45%) and the ability to benefit from the effects of the network (44%). The authors of the study predict that, by 2030, distributed ledger technology will generate a larger annual business by three trillion US dollars, compared to 2018 (PwC, 2018, Global Blockchain Survey).

Conclusions

After analyzing the information identified on each main topic, as part of the study of the literature, it was possible to reach some conclusions about the impact of blockchain-based solutions on the management of the fight against money laundering and terrorist financing by financial institutions. In the article, the focus was on use cases that can directly contribute to the fight against money laundering and the financing of terrorism. However, the answer is not yet simple. Here, the main differences come from the type of blockchain used. As we mentioned there are three types of blockchain - public, private and hybrid.

The results of the analysis show that private and hybrid blockchains work better in terms of compliance with the fight against money laundering and the financing of terrorism standards. On the other hand, public blockchains fail to provide the characteristics needed to be adopted by a financial institution. As the name suggests, public networks can be accessed by anyone with an Internet connection, which is not ideal, given the internal amounts of sensitive and private data on the systems of financial institutions. In addition, public blockchains are completely immutable - because once entered into the network, the data cannot be modified and deleted. Full immutability is not desirable in an organizational context, as data entered on systems may undergo further changes. In addition, a completely immutable network does not comply with the GDPR. Customers must be able to exercise their rights, if they so wish, which implies the possibility to modify or delete personal data from the systems of the institutions. Unlike public networks, private and hybrid blockchains can comply with legal requirements to combat money laundering and the financing of terrorism.

References

Benos, E., Garratt R. & Gurrola-Perez P. (2017). *The economics of distributed ledger technology for securities settlement*. Staff Working Paper no. 670, Bank of England. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.

Deloitte. (2019). *Deloitte 2019 Global Blockchain Survey.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.

Egilsson, J. H., & Valfells, S. (2017). *Blockchains and the future of financial services.* Retrieved from http://monerium.com/content/monerium-reportweb-2017-07.pdf.

Fronda, A. (2019). *The future of clearing and settlement.* Retrieved September 14, 2019, from https://www.theglobaltreasurer.com/2019/02/15/the-future-of-clearing-and-settlement/.

Higginson, M., Hilal A. & Yugac E. (2019). *Blockchain and retail banking: Making the connection.* Retrieved September 14, 2019, from https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection

Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J. C., Badev, A. I., ... & Ellithorpe, M. (2016). *Distributed ledger technology in payments, clearing, and settlement.* Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System.

Ometoruwa, T. (2018, May 16). *Solving the Blockchain Trilemma: Decentralization, Security & Scalability.* Retrieved May 17, 2018, from https://www.coinbureau.com/analysis/solving-blockchain-trilemma/.

Peters, G. W., & Panayi, E. (2016). *Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money.* In Banking Beyond Banks and Money (pp. 239-278). Springer, Cham.

PwC. (2018). *Global Blockchain Survey.* Retrieved from https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html.

Redman, J. (2017, January 31). *Bitcoin in Numbers – a Collection of Interesting and Recent Charts.* Retrieved March 25, 2018, from https://news.bitcoin.com/bitcoin-in-numbersa- collection-of-interesting-and-recent-charts/.

Rodgers, D. (2019). *A Primer About Clearing and Settlements*. Retrieved September 14, 2019, from https://www.thebalance.com/a-primer-about-clearing-and-settlements-1290415.

Santander. (2018). *Santander launches the first blockchain-based international money transfer service across four countries.* Retrieved from https://www.santander.com/csgs/Satellite/CFWCSancomQP01/en_GB/Corporate/Press-room/Santander-News/2018/04/12/Santander-launches-the-first-blockchain-based-international-money-transfer-service-across-four-countries-.html.

Vasek, M., Thornton, M., & Moore, T. (2014, March). *Empirical analysis of denial-of service attacks in the Bitcoin ecosystem.* In International Conference on Financial Cryptography and Data Security (pp. 57-71). Springer, Berlin, Heidelberg.

Vasin, P. (2014). *Blackcoin's proof-of-stake protocol v2*. URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf.

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger.* Ethereum Project Yellow Paper, 151, 1-32.