

The Globalization of Cashless Transactions Using Blockchain Technology to Preventing Money Laundering and The Changing Trends in The Cryptocurrency Market: A Learning Experience of Polish and EU Laws

Abhishek Thommandru

&

Benarji Chakka*

Summary: The COVID-19 pandemic experience has driven us to rely on technology so much on the development and expansion of technology, including cashless transactions. Criminal groups may become more interested in electronic payments and virtual currencies because of increased traffic in these areas. When comparing the second half of the 2019 to the first half of the 2020, the number of fraudulent card transactions increased by 11.4%. New developments in virtual currency trading regulations, including the digital finance package, which includes, among other things, a draught regulation from the European Parliament and an amended act to combat money laundering and terrorist financing, among others. For the reasons stated above, these regulations may lead to a virtual currency market collapse and the withdrawal of investors and the siphoning of money into Asian markets as a result. The current regulations are a manifestation of total regulation and do not encourage technological advancement.

Keywords: AML; CTF; counteracting; money laundering; KNF (PFSA); FinTech; RegTech; MiCA regulation

Citation: THOMMANDRU, A., CHAKKA, B. The Globalization of Cashless Transactions Using Blockchain Technology to Preventing Money Laundering and The Changing Trends in The Cryptocurrency Market: A Learning Experience of Polish and EU Laws. *European Studies – the Review of European law, Economics and Politics*. 2022, vol. 9, no. 2, pp. 213–242 DOI: 10.2478/eustu-2022-0021.

* Abhishek Thommandru is a Research Scholar (PhD), VIT-AP School of Law, VIT AP University, India; e-mail: abhithommandru@gmail.com. Benarji Chakka is a Dean and Professor, VIT AP School of Law, VIT-AP University, India; e-mail: benarji.chakka@vitap.ac.in

1. Introduction

Cryptocurrency is booming for its credibility of utility using different platforms and technologies involved and by evaluating the European and Polish laws on crypto assets (including virtual currencies), trading, and money laundering and terrorism financing (practices in which crypto-assets are very often used) would be guided in better path of learning experience.

First, we'll discuss COVID-19's impact on non-cash payments. The legal definitions of crypto assets, virtual currencies, and attempts to regulate their supply are next. Legal provisions have so far ignored regulations protecting cryptocurrency users' interests (the regulations issued so far focused only on counteracting money laundering and financing of terrorism). Whether the aforementioned legal regulations on virtual currencies affect their growth dynamics and whether or not these regulations impact the costs associated with their supply, these analyses will be carried out.

Everything about the recent global COVID-19 pandemic has contributed to the advancement and expansion of digital technology, including cashless transactions. COVID-19 has had no effect on new anti-money laundering and terrorist financing regulations, but that doesn't matter because the changes we're dealt with were already planned before the pandemic by the World Health Organization.

Recommendations from the organisation for many years before a pandemic, the so-called „regulating sandbox“ would be stuck in the „measuring and piloting“ phase, but with physical distancing, the implementation of the „social distancing“ occurred immediately (regulators sandbox). Those companies still using traditional business models and not yet ready for remote work could implement solutions like ZOOM, cloud computing in the SaaS model, Google Hangouts, or Microsoft Teams in just a few weeks.

Increased electronic payment and virtual currency use may result in criminal groups becoming more interested in these areas, such as illegal mining of virtual currencies, theft of computing power to the mining of virtual currencies and social engineering scams (e.g., by opening fake cryptocurrency exchanges, creating fake cryptocurrency emission offers and impersonating the perpetrator of known and reputable company), attacks on token management systems. On When it comes to investing in stocks, dangers are involved with an unregulated crypto-asset market. The Warsaw Stock Exchange's „GPW Private Market“ initiative, which involves investment in financial instruments built on blockchain and digital tokens with the cooperation of a respectable partner (GPW SA), is one example of how to minimise this risk. Figures reveal that when investors and users lose money because of fraud, we are dealing with large sums. Losses in this industry totalled USD 4.26 billion in the first six months of 2019. Drug gangs in

Latin America utilise virtual currencies to launder cash and pay for psychoactive and intoxicated substances in the so-called hidden markets and darkness.¹

Most cryptocurrency-related crimes in Poland occur on exchanges. Money obtained illegally (for example, by unauthorised access to electronic banking) is traditionally invested in cryptocurrency and subsequently paid to the so-called „poles“ after their exchange for cash.

2. The Polish payment system, COVID-19, and virtual currencies

A payment system is a collection of entities, instruments, procedures, and systems used to facilitate the free flow of funds within a specific geographical area's financial markets and institutions. Among the participants in the payment system, there are four distinct groups: first-level participants (such as banks and payment institutions), second-level participants (such as clearinghouses), and third-level participants (such as clearinghouses and payment service providers) (e.g., the „National Bank of Poland and the National Depository for Securities“).

An upsurge in cash withdrawals was noticed during the early stages of the pandemic. A significant increase of PLN 59.1 billion (or 26.4 percent) in the quantity of cash in circulation outside bank vaults at the time. 20 Banknote and coin withdrawals daily NBP grew by a whopping 121.7% in March 2020 compared to the same month last year.

For non-cash transactions, the adoption of COVID-19 has hastened the anticipated increase in the contactless transaction limit (from PLN 50 to PLN 100) that eliminates the requirement for users to provide a PIN (Personal Identification Number). Restrictions imposed by the pandemic's current status, which hampered the ability of stationery businesses to operate, sparked an increased demand in online payments and transactions.

Infrastructure for non-cash transactions was also affected by the pandemic. By the end of June 2020, the number of POS (point-of-sale) terminals had increased by 7.5% over that of December 2019. 707 thousand new POS terminals were installed in retail locations within the same period. The number of online retailers accepting card payments climbed by 8.8% and reached 55.8 thousand, while the total number of card transactions in these establishments increased by 6.7% and reached 66.7 million (an increase of 10%). According to data from June 2020 and the first half of the 2018, online store transactions surged by 97.9%

¹ United States: Treasury Regulations on Financial Recordkeeping and Reporting of Currency and Foreign Transactions. International Legal Materials 11, no. 3 (1972): pp. 648–51.

over this period. For the first half of the 2020, card non-present transactions (CNP) climbed by 35,7% over the same period last year and by 75,6% over the same period last year. Despite these increases, non-cash card transactions fell in volume and value, totaling PLN 2.796 billion at the time (a decrease by 8 percent). The public's aversion to spending money during a pandemic explains this.²

An increase in payment instrument fraud is directly related to the aforementioned trends. In the first half of the 2020, banks reported 126.7 thousand fraudulent (unauthorised) transactions, while acquirers reported 17.6 thousand scams. Comparing the second half of the 2019 to the first half of the 2020, banks reported an 11.4% increase in the number of fraudulent card transactions (113.7 thousand fraudulent transactions). Cards issued to me in Poland were used to make most fraudulent card transactions in 2020, although they were all made outside Poland's borders. This quarter saw a 5.6 percent decrease in transaction value despite an increase in the number of fraudulent transactions.³

The European Central Bank (ECB) reports that Poland has the lowest level of card transaction fraud in the EU, based on the total number and value of card transactions. Studies on consumer payment patterns show that the COVID-19 epidemic has affected the growth of cashless transactions. Statistical data show that during the epidemic, 38% of the polled respondents verified that they paid without cash more frequently, 29 percent more frequently than before the pandemic, and 65% of respondents stated that this tendency would continue after the outbreak ended. According to the survey results, 48% of people said that the pandemic affected how they paid for goods in physical businesses. These findings were from a study conducted in the latter half of the 2020. Estimated more than 4,000 virtual currencies and tokens to choose from. As a result, 2020 was a record year for Bitcoin, with its price increasing by 400 percent despite the crash on March 31 of 2019.⁴

Seventy-four percent of those polled said they increase their bitcoin holdings in the future, while a further forty-seven percent of those polled who do not presently have any bitcoin said they plan to do so by 2021. Other digital currencies, such as bitcoin cash, ethereum, litecoin, and ripple, are in a similar position. More and more inexperienced investors may put their money into this form of investing in the near future, given the ease with which it may be done, such as using an app on a smartphone (e.g., Revolut).

² ZAMORA, S., EDWARDS, R. W. Capital Flight and the Creditworthiness of Developing Countries. *Proceedings of the Annual Meeting (American Society of International Law)*. 1989, vol. 83, pp. 100–106.

³ WOPPERER, W. Fraud Risks in E-commerce Transactions. *The Geneva Papers on Risk and Insurance. Issues and Practise*. 2002, vol. 27, no. 3, pp. 383–394.

⁴ WALTER, N. The Euro: A New Currency for the World? *The Brown Journal of World Affairs*. 1999, vol. 6, no. 2, pp. 113–23.

Chart. 1. Changes in the bitcoin exchange rate against the dollar in 2012–2021.

Source: <https://pl.investing.com> [access: 10 May 2021]⁵

3. Virtual currencies – General Issues

Customers may be exposed to risk because several virtual currencies (VC) in EU jurisdictional control are only partially regulated. Risks posed by virtual currencies have been the subject of EBA reports for some years (such as: exchange rate instability, lack of liquidity).⁶

An alternative to money that has not been issued by any central bank, credit institution, or e-money institution is defined as „cryptocurrencies“ by the European Central Bank. However, this definition is not obligatory to EU Member States, but rather merely a guide.

Virtual currencies are divided into the following:

- Cryptocurrencies,
- **Tokens** – computer game developers, for example, who create and regulate the rules of the virtual communities in which they work (Amazon Coins or already discontinued Facebook Credits).

⁵ TABOR, P. *The Bitcoin (BTC) price has been manipulated many times, the research of the scientist shows*. Available at: <https://pl.investing.com/analysis/kurs-bitcoina-btc-wielokrotnie-ma-nipulowany-wskazuja-badania-naukowca-200230146>

⁶ STEPHENSON, R. G., POINDEXTER, O. O., MARTZ, D. J. Developments in Cyberbanking. *The Business Lawyer*. 2003, vol. 58, no. 3, pp. 1215–1228.

The trading model for virtual currencies is what sets them apart from typical fiat currencies. It can be broken down into the following:

- **Distracted** – You will not find hierarchies or central organizations here. There is no superior-inferiority relationship between any of these people. Each trader has a way to get in touch with the rest of the group. In this system, each member can be a currency issuer, to supervise trading, and to keep a record of all transactions in the system.
- **Centralize** – In the case of a single currency, just one body is responsible for issuing and regulating trading. Only one entity handles all transactions, and that entity maintains a record of all those transactions.
- **Decentralized** – Some of the authority and responsibilities are delegated to the subordinate structures by the central body.

The bit coin is the most well-known and widely publicized example of virtual money. This paper, Bitcoin: The Basic Assumptions, lays forth the fundamental assumptions that underlie the Bitcoin system. An unidentified creator using the pseudonym „Satoshi Nakamoto“ created a peer-to-peer electronic cash system. Some individuals assume that this alias refers to Samsung, Toshiba, Nakamichi, and Motorola, all of which are Japanese technology companies. Bitcoin has been credited to Elon Musk or Nick Szabo, according to some ideas. Even now, the originators of Bitcoin remain a mystery.

The Bitcoin technology was used to facilitate direct and anonymous e-commerce transactions. It was meant to be a completely new method for financial institution, one that did not rely on global financial systems or central settlement mechanisms for its operations. When it comes to electronic money and online anonymity, David Chaum is regarded as „the father“. He highlighted that a third-party financial intermediary should be restricted in what information it may gather about a transaction's date, time, location, value, and purpose of payment (big data). Even though the financial intermediary may be interested in sensitive (sensitive) information related to the payment (such as the location of a traveler, his or her lifestyle (e.g. payments for a hotel or restaurant during a trip, as well as payments for medicine or the press), the financial intermediary does not need this information.

People who use new technologies aren't thinking too hard about how processed by these data by financial intermediaries. In contrast, the above-mentioned data is essential and used by most systems to detect payment frauds and counter-act money laundering (AML) and counter terrorist financing (CTF).⁷

⁷ WINN, J. K. Catalytic Impact of Information Technology on the New International Financial Architecture. *The International Lawyer*: 2000, vol. 34, no. 1, pp. 137–147.

4. Virtual currencies and electronic money

The term „electronic money“ is often used to describe virtual currencies. While e-money has the legal tender status, virtual currency does not (fiat currency). The so-called open-source characteristic of cryptocurrency programming is its openness to the public. The following supports the claim that a certain instrument should be considered as a cryptocurrency:

- A distributed transaction system is used, and
- Cryptography was used to build the framework.

The establishment of a worldwide, open, and distributed database of cryptocurrency transactions is also required. Bitcoin uses the peer-to-peer communication technology to facilitate direct transactions between Internet users.

This eliminates the requirement for a transaction intermediary and eliminates the necessity for a central server (store of transaction information). The so-called „trusted third party“ does not mediate. Rather, the 5th Directive AML (hereinafter: AMLD5) and Polish legislation implementing it, as well as the laws in the draught regulation on the cryptoasset market (Markets in Crypto-Assets, MiCA, hereinafter: MiCA Regulation), are the only regulatory bodies that apply to the Bitcoin system.

Blocks of approved uses – the blockchain – are created by combining the records of transactions completed using bitcoin coins. As a result, they built a public book (database) that is accessible to all computers on the Bitcoin network. Transactions cannot be reversed in the Bitcoin system’s public distributed transaction register, which is advantageous to payment merchants (e.g., a store that accepts bitcoin payments) but may pose a risk to the payer.⁸

5. Legal regulations regarding virtual currencies – new regulatory trends AML/CTF

New AML/CTF rules for virtual currency include:

- There will be an amendment to the Act on Counteracting Money laundering and Terrorist Financing on 30 March 2021 (hereinafter: the modified AML Act), which would include the AMLD.
- The digital finance package was approved by the European Commission on September 24th, and it includes the following:

⁸ VISHIK, C. Intermediation and Quality Uncertainty in the Internet Environment: New Opportunities for LIS. *Journal of Education for Library and Information Science*. 1999, vol. 40, no. 4, pp. 263–81.

- Digital finance strategy,
- Retail payment strategy,
- Legislative proposals for an EU regulatory framework for crypto assets and digital operational resilience.

There many European Union directives governing money laundering and terrorist financing risk management in the EU. AMLD5, which replaced the fourth AML Directive, is currently in charge of preventing money laundering and terrorist financing (TF) (hereinafter: AMLD).

As part of the AML directives, the FATF has established worldwide standards for countering money laundering and funding terrorism, which are incorporated into the AML/CTF system in the guidelines (Financial Action Task Force).

The risk-based approach is a guiding element for AMLD4. From one country to the next, the level of ML/TF risk might vary greatly. Countries and their competent authorities (CA) as well as anyone involved in legal transactions must therefore identify and manage these risks by enacting the necessary legislative measures.

The EU Member States have until 10 January 2020, to implement the 5th AML Directive, which was adopted on 30 May 2018. On 30 March 2021, the Sejm of the Republic of Poland passed legislation adopting AMLD5, and on 8 April 2021, President Andrzej Duda signed it into law. In 2021, the law went into effect in its entirety.

As defined by AMLD, digital determinants of value that are frequently accepted as a channelized medium of exchange by natural and legal persons, but are not issued or guaranteed by any central bank or public authority, and do not need to be linked to a legally binding currency, but may be transferred, stored, or sold electronically, are defined as virtual currencies. The Act on Countering Money Laundering and Terrorism Financing in Poland has a definition of virtual currency (hereinafter: the AML Act). Non-tangible value is what „virtual currency“ refers to:

- The currency of another country, issued by its central bank or another public institution,
- An international unit of account established by an international organisation and accepted by individual countries belonging to this organisation or co-operating with it,
- Electronic money within the meaning of the Payment Services Act,
- A financial instrument within the meaning of the Act on Trading in Financial Instruments financial,
- A bill of exchange or a check, and is tradable for legal tenders and is accepted as a medium of exchange.

Virtual currencies are an example of what is referred to as „property values“, which also includes other rights to both moveable or immovable property,

payment methods, legally specified financial instruments, other securities, and foreign exchange values.

AML/CTF laws only apply to so-called „obligated institutions“, which include, among others, the following insofar as they are pertinent to the topic of this study:

- Entities conducting business activities consisting in the provision of services:
- Exchanges between virtual currencies and means of payment,
- Exchanges between individual virtual currencies,
- Intermediation in the exchanges referred to above,
- Maintenance of accounts;
- Local banks, outposts of international banks, and outposts of lending organisations based in the Republic of Poland territory;
- The National Cooperative Union Savings and Credit, as well as cooperative savings and credit unions;
- This category includes small payment institutions, payment service offices, and acquirers, in addition to domestic payment institutions, domestic electronic money institutions, and EU and foreign payment institutions.
- Investment firms, trust banks;
- Foreign legal persons conducting brokerage activities in the territory of the Republic of Poland;
- Regulated markets were been controlled under several companies;
- Investment funds, alternative investment firms, investment fund firms, and alternative investment firms that manage investments;
- Insurance companies;
- The national depository for securities;
- Entrepreneurs running bureau de change offices;
- Entrepreneurs, not being other obligated institutions, providing services consisting in the following:
 - Creating a legal person or an organisational unit without legal personality,
 - Carrying out the duties of a management board member or assisting another person in doing so, as well as equivalent duties in the context of a legal entity or an organisational unit lacking legal identity,
 - Giving a legal person or an organisational unit without legal identity a registered office, a business address, a communication address, and other relevant services,
 - functioning as a trustee, or allowing another person to operate in that capacity, which was established by a legislative act,
 - acting or permitting another person to act as a person exercising stocks or shares for a non-listed firm that is subject to EU disclosure laws or a comparable international norm,

- Foundations, to the extent that they accept or make cash payments with a value equal to or exceeding the equivalent of PLN 10,000; euro;
- Associations with legal personality, to the extent that they accept or make cash payments with a value equal to or greater than PLN 10,000; the euro;
- Entrepreneurs, to the extent that they accept or make payments for goods in cash with a value equal to or exceeding the equivalent of PLN 10,000; the euro;
- Loan institutions.

Based on the joint opinion of the European Supervisory Authorities (ESA) 72 on numerous risks connected to money laundering and terrorism financing that affects the EU financial sector and shared by all other EU financial sectors, one can distinguish, among other things:

- New technology risk,
- Virtual currencies risk,
- Danger relating to differing supervisory techniques and legislative fragmentation among EU nations (legislative divergence risk and divergent supervisory practices risk),
- Risk related to weaknesses in internal constraints
- Troll risk,
- Risk related to the de-risking risk,
- Terrorist financing risk.

The terms „FinTech“ and „RegTech“, which have been prevalent in the realm of digital finance for many years, must be approximated to characterise virtual currencies. According to the consensus of the European Supervisory Authorities, these challenges pose particular dangers connected to the advancement of new technology. The following intech solutions should be distinguished:

- Online services include factoring, loans, and tools for determining a customer's creditworthiness (payment). This review is conducted electronically and remotely, and the companies offering these services use social media sites like Facebook, LinkedIn, and Instagram as well as databases from business information departments;
- Mobile application at bank.

The use of technological solutions in financial innovation, or fintech⁷⁸, results in the development of new business models (e.g., the BLIK⁷⁹ payment system, payment systems on mobile devices: Apple Pay, Google Pay, Samsung Pay). The most significant Polish-based intech companies are PayU, Blue Media, Polish Payment Standard (BLIK), Currency One, Finanteq, VoicePIN, and ZenCard. Among the overseas organisations, Revolt and N26 should be mentioned.⁹

⁹ REDÍN, D. M., CALDERÓN, R., & FERRERO, I. Exploring the Ethical Dimension of „Hawala.“ *Journal of Business Ethics*. 2014, vol. 124, no. 2, pp. 327–337.

RegTech is the application of cutting-edge technology to comply with and assist regulatory standards. RegTech products allow organisations to acquire and analyze data more quickly, more affordably, and more easily. It making financial processes more transparent, is crucial in the battle against money laundering and terrorist financing. The automated verification of lists of politically exposed individuals (PEI), who, according to AMLD5, include, among others, presidents, prime ministers, deputies, ministers, and their families, is one use of RegTech., inter alia, presidents, prime ministers, deputies, ministers and their families.¹⁰

6. Digital Finance Strategy (Digital Finance Package)

The digital finance package outlines the routes the EU will take concerning FinTech. To meet the needs of new technology, EU legislation must be modified. Thanks in part to the use of technologies based on distributed registers and artificial intelligence (AI), the digital revolution should be complete by 2024. (One example of such registers is blockchain). The strategic objective is to support sound legislative frameworks that will permit the adoption of interoperable digital identification systems and to advance financial management to the advantage of businesses and consumers. They will make it simpler for consumers get banking services (the so-called onboarding). The strategy focuses on four priorities:

- ensuring that the adopted regulations facilitate and does not block, the development of other digital novelties,
- tackling the fragmentation of the digital single market in financial services great,
- meeting the threats and challenges of digital transformation,
- Establishing a European financial data area to promote data-driven innovation, including increasing data access and sharing of data within the financial sector.

The approach should be seen favourably to the degree that it aims to standardise digital financial concerns for the EU, particularly those involving digital identity and identification.¹¹

¹⁰ MIDDLEBROOK, S. T., SARAH J. H. Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services. *The Business Lawyer*. 2013, vol. 69, no. 1, pp. 263–73.

¹¹ RIMMER, S., PRASAD, R. Electronic Money and Regulatory Responses. *Agenda: A Journal of Policy Analysis and Reform*. 1997, vol. 4, no. 3, pp 371–378.

6.1. Retail Payment Strategy

Increasing the speed of non-cash retail payments is a priority for the EU in its retail payment strategies. The norm for payment transactions is to use instant payments. To achieve this, it is essential to boost consumer acceptance of this payment method and make the advantage of the potential of electronic identity for customer authentication. The aforementioned plan has no direct bearing on cryptocurrencies; it only serves to motivate that they will become more important and will face competition from more established payment systems and convertible currencies (bank transfer, payment card). It should be highlighted that if bitcoin trading becomes more commonplace in retail payments, it will become important to alter this technique and incorporate the topic of cryptocurrencies sooner rather than later.¹²

6.2. MiCA regulation – regulatory proposals

The aforementioned rule is an initial attempt to address problems with products based on distributed ledger technology (DLT) and capital-raising techniques using virtual assets.

(Ex: an ICO, or initial coin offering). Currently, this subject is governed differently in each EU member state. The omission of topics relating to fighting money laundering and terrorism financing, which are governed by EU AML directives, is the common denominator. This position indicates that businesses engaging in cryptocurrency asset trading activities do so legally in favourable legal jurisdictions (Estonia, Lithuania, and Malta).

The MiCA regulation applies to:

- Requirements for transparency and disclosure in connection with the issuance of cryptocurrencies and their inclusion in trading,
- Authorization of cryptocurrency asset service providers, cash-token and asset-linked token issues electronic equipment,
- Exercising supervision over the above issuers,
- Providers of services connected to crypto-assets, electronic money token issuers, and asset-related token issuers, in terms of their operations, how they are organized, and the management principles they employ,
- Regulations regarding the protection of consumers investing in cryptocurrency,
- Crypto market abuse prevention measures.

¹² TUBA, MAPHUTI D. The Technology-Neutral Approach and Electronic Money Regulation in the EU: Identifying the Promises and Challenges for Future Regulation in South Africa. *The Comparative and International Law Journal of Southern Africa*. 2014, vol. 47, no. 3, pp 372–400.

The MiCA Regulation also defines „crypto-related services“ as any services or activities connected to cryptocurrencies, including

- Storing and managing crypto assets on behalf of third parties,
- Running a crypto asset trading platform,
- Exchange of crypto assets for fiat currency, which is legal tender,
- Exchange of crypto assets for other crypto assets,
- Execution of orders related to third-party crypto assets,
- Sub-issue of crypto assets,
- Accepting and transferring orders related to crypto assets on behalf of third parties,
- Consulting in the field of crypto assets.

A „cryptocurrency“ is a digital representation of values or rights that can be electronically transmitted and maintained using distributed ledger technology or comparable technology, according to the MiCA legislation. Virtual currencies are among the most well-known crypto-assets on the market at the moment (bitcoin, Ethereum).

Distributed ledger technology is a type of technology that supports distributed recording of encrypted data within the context of the MiCA law. The MiCA rule classifies cryptocurrencies into three groups, each of which has its own set of statutory standards for classification:

- **Utility tokens** – A type of crypto-assets designed to give users virtual access to a particular item or service; they operate in distributed ledger technology and are only recognised by the token’s creator;
- **Asset tied tokens** – The type of crypto-assets they must own have a stable value because of their connection to:
 - the market value of many legal tender fiat currencies, many commodities, many cryptocurrencies, or a mix of these assets;
 - **E-money tokens** – a type of crypto-assets that are primarily intended to be used as a means of exchange; as they are connected to the fiat currency that is considered legal tender, they are meant to retain a constant value.¹³

The major goal of the MiCA law is to guarantee security and transparency for users of cryptoassets, so specific requirements have been placed on the businesses issuing these assets and offering services related to their trade. The establishment of the requirement for a public offering when offering crypto-assets is one of the fundamental tenets of the MiCA regulation, from which there may be exceptions.

¹³ MOSAKOWSKI, E., ZAHEER, S. The Global Configuration of a Speculative Trading Operation: An Empirical Study of Foreign Exchange Trading. *Organization Science*. 1999, vol. 10, no. 4, pp. 401–423.

The MiCA rule puts various duties on token issuers based on the types of tokens. The publication of a document describing the fundamental and crucial details about the project (the so-called white paper) will be a requirement shared by all issuers; nevertheless, the amount of information offered varies significantly.

The format and contents contained in such an information document are regularized by the MiCA Regulation. If the entire amount of the cryptoasset offer is less than EUR 1 million within a 12-month period, or if it is free, and it is made to qualified investors and less than 150 natural or legal persons, the disclosure document is not required.¹⁴

Utility token issuers are subject to the fewest limitations possible. Through marketing materials and the so-called information document, they must give investors with comprehensive information, understandable, trustworthy, and not deceptive. The information document just must be notified; it is not ex-parte approved by the relevant governmental authorities.

According to the MiCA rule, every consumer must be able to withdraw their consent to purchase bitcoin assets within 14 days of the day on which they gave it. All funds made in this case are returned to the consumer. This right is invalid when crypto-assets are permitted to trade on a cryptoasset trading platform.

Issuers of asset-related and e-money tokens are in quite different situations. These issuers have a duty to:

- Obtaining a licence from an appropriate government to conduct a public cryptocurrency offering. Under the so-called passport uniform, the permission will be issued by the government of the specific country where the issuer has its headquarters and will be valid throughout the EU. No authorization is required when a public offering of cryptocurrency assets is undertaken, where the average token value over the course of a year is less than EUR 5 million, or when the offer is made to only qualified investors;
- Preparation and publication of an information document (in accordance with the standards set out in the ordinance) on the offered cryptocurrencies;
- Preparation of clearly marked marketing materials in which the information is reliable, clear and not misleading;
- Implementation of appropriate liquidity management mechanisms;
- • Having a suitable organizational structure, as well as internal policies and procedures for its regulation. Members of the issuer's management team must exhibit the necessary training, expertise, and knowledge, while also adhering to AML/CTF regulations. The responsibility to mitigate the different

¹⁴ MAURER, B. Data-Mining for Development: Poverty, Payment, and Platform. In: A. ROY, A., CRANE, E. S. (eds.). *Territories of Poverty: Rethinking North and South*. University of Georgia Press, 2015, pp. 126–143.

hazards linked with information and communication technology will fall on cryptocurrency service providers;

- implementation of an effective mechanism to prevent conflicts of interest, their identification and disclosure;
- have adequate funds and reserve assets.

The MiCA legislation also gives businesses who want to test particular business models (during the start-up phase) under the watchful eye of competent supervisory authorities the option of a temporary exemption from the execution of its provisions.¹⁵

The MiCA legislation should be thoroughly analyzed because it is an example of legal inflation. With the offering of crypto-assets, too many formal duties are introduced (an analogy to similar regulations on regulated markets, and exchanges, where securities are traded is noticeable here). The author claims that this will be a significant barrier to market access and result in high entry costs (e.g., related to legal and economic consultancy).¹⁶

6.3. AML Act

Currently, most cryptocurrency trading platforms are on the list of public warnings by the Polish Financial Supervision Authority. These platforms did not have to use any AML/CTF measures (including customer identification and verification), which more than once led to a situation specifically unknown funds transferred from unauthorized modes is been used in many ways because of misappropriation of access data to the bank account were transferred by instant payment systems to these platforms and then deposited in bitcoin. Such an operation made it impossible to identify the perpetrators of the appropriation and to bring them to criminal liability, and the proceedings were discontinued at the stage of preparatory proceedings in the case.¹⁷

In the amended AML Act, the legislator regulated the activities of such entities as virtual Bureau de change offices, virtual most bitcoin trading platforms are currently included on the Polish Financial Supervision Authority's 98 list of publicly issued warnings. Because these platforms were exempt from AML/CTF requirements (including customer identification and verification), it frequently happened that funds from allegedly illegal payment transactions because of stolen

¹⁵ RICE, D. T. The Past and Future of Bitcoins in Worldwide Commerce. *Business Law Today*. 2013, pp. 1–4, JSTOR. Available at: <http://www.jstor.org/stable/businesslawtoday>

¹⁶ PARK, Y. S. Currency Swaps as a Long-Term International Financing Technique. *Journal of International Business Studies*. 1984, vol. 15, no. 3, pp. 47–54.

¹⁷ MARTIN, A. Endogenous Multiple Currencies. *Journal of Money, Credit and Banking*. 2006, vol. 38, no. 1, pp. 245–262.

bank account access data were transferred by instant payment systems to these platforms and then deposited in bitcoin. Due to this operation, it was impossible to identify the appropriation's perpetrators and hold them criminally accountable, and the case's preliminary processes were terminated.¹⁸

The actions of organizations like virtual Bureau de change offices, virtual currency exchanges, and suppliers of wallets for holding virtual currencies under regulation made by legislator in the modified AML Act.

Before the adoption of the modified AML Act, European and Polish laws only partially addressed virtual currencies in terms of preventing money laundering and terrorism financing by designating a limited number of firms as required institutions. They were forced to implement the so-called financial security measures, such as customer identification and verification, and have suitable AML/CTF procedures as a result, among other things.¹⁹

Some hidden places have been into market to trade currencies and companies that make wallets for storing virtual currencies. Before the AML Act was changed, Polish and European laws against money laundering and funding for terrorism only partially applied to virtual currencies by recognizing certain types of organizations as „obligated institutions“. This meant that, among other things, they had to use so-called financial security measures like identifying and verifying customers and having the right AML/CTF procedures.²⁰

The scope of these obligations has been significantly added and in amended AML Act by the following:

- Requiring service providers in the virtual currency field to sign up in the register of activities in the virtual currency field (it will therefore be an economic activity),
- Putting in place-specific rules for companies that offer virtual currency services and the people who run them (no conviction for a specific crime). The above rules also apply to governing legal entities (limited liability companies, joint-stock companies) and partners of organizational units without legal personality, but having legal capacity (general partnerships, limited partnerships),
- Requires people who do business with virtual currencies to have a good reputation and know what they are doing,
- Putting in place the need to use financial security measures when doing a one-time transaction in the virtual currency field that costs more than pln

¹⁸ O'MALLEY, P. Simulated Justice: Risk, Money and Telemetric Policing. *The British Journal of Criminology*. 2020, vol. 50, no. 5, pp. 795–807.

¹⁹ NEWBURG, A. W. G. Financing in the Euromarkets by U.S. Companies: A Survey of the Legal and Regulatory Framework. *The Business Lawyer*. 1978, vol. 33, no. 4, pp. 2171–2194.

²⁰ PORTES, R., REY, H., DE GRAUWE, P., HONKAPOHJA, S. The Emergence of the Euro as an International Currency. *Economic Policy*. 1998, vol. 13, no. 26, pp. 307–343.

1,000 or €100. Activities involving trading in virtual currencies may be performed.

- A natural person who has not been legally convicted of a crime against the activities of state institutions and local government, the administration of justice, the credibility of documents, property, economic turnover and property interests in civil law transactions, trading in money and securities, for financing terrorism, for crime committed for material or personal gain, or for an intentional fiscal offence.
- A legal person or an organizational unit without legal personality in which the partners in charge of running the partnership's business or with the power to represent the partnership or members of its management bodies have not been convicted of any crime listed above.

The new thing is that the same requirements about not having a criminal record also apply to people who run these entities (like managers and directors) and run activities related to virtual currencies (like partners of limited liability companies and shareholders of joint-stock companies).²¹

The new version of the AML Act says that people who perform the said activity must know about it or have experienced it. This responsibility can be followed by:

- Performing activities related to virtual currencies for at least one year, which will be confirmed by relevant documents,
- Completing a training or course covering the legal or practical topic of virtual currency activities.

The minister of public finances is the person in charge of registration issues (these powers may be entrusted to the „National Revenue Administration“ by means of a regulation). Minister as a registration authority:

- Keeps a register,
- Process information about entities that enter into it,
- Examines applications for entry in the register,
- Imposes fines of up to 100,000 pln. Pln on entities that didn't meet the requirements of article 153b of the updated aml act and weren't in the register of activities related to virtual currencies.

In addition to administrative powers, the registration authority has special powers that can stop an entity from working in the field of virtual currencies:

- Doesn't meet the legal requirements to do business in the field of virtual currencies,
- Submits a false statement about the truthfulness and completeness of the application for entry in the register, knowledge of the rules for conducting

²¹ SAEED, S., ANCKAR, P. Currency Choice in Industrial Pricing: A Cross-National Evaluation. *Journal of Marketing*. 1998, vol. 62, no. 3, pp. 112–127.

business with virtual currencies, and criminal awareness for submitting a false statement.

It looks like the administrative fine of 100,000 PLN is not even close to being sufficient to cover the amount of volume (quantity and value) of buying and selling virtual currencies.²² At the price of bitcoin right now, it costs less than half of the one bitcoin. The provisions of the Regulation on the cooperation of national authorities responsible for enforcing consumer protection law (also known as the „CPC Regulation“) listed to be a much more effective way to enforce AML/CTF violations. For example, if a website's content violates consumer interests in the digital space, the content can be blocked (in Poland, such powers are provided for the President of the Office of Competition and Consumer Protection). Polish law already has a rule that requires telecommunications companies to block websites that offer gambling games that are against the law.²³

The new parts of the AML Act (which agree with AMLD) make the current AML/CTF rules in Poland even stronger. According to them, the risk of money laundering and funding for terrorism in the exchange of virtual currencies can be reduced by recognizing as obligated institutions 108 entities that do business in the following:

- Converting virtual currencies into means of payment,
- Exchange between virtual currencies,
- intermediation in the indicated exchanges,
- Keeping accounts in electronic form as a set of identification information, so that authorized people can use virtual currency units and do exchange transactions with them.

Polish law enforcement agencies have created a way of working based on the way things are done and the laws that are in place right now in the area of AML/CTF. This method consists of the following:

- Initiating a procedure for blocking funds derived from crime,
- Defining the platforms used for criminal activities,
- Learning about the policy for assessing the risk of money laundering and the risk of funding terrorism, familiarization with an organisation's aml/ctf procedures and an analysis of those procedures to see if the organisation is following these rules in a specific case,
- Asking the organisation to protect the digital traces left by the perpetrators,

²² NEWMAN, D. B. Tax Consequences of Foreign Currency Transactions: A Look at Current Law and An Analysis of The Treasury Department Discussion Draft. *The Tax Lawyer*. 1983, vol. 36, no. 2, pp. 223–292.

²³ SHEARER, R. A. The Foreign Currency Business of Canadian Chartered Banks. *The Canadian Journal of Economics and Political Science / Revue Canadienne d'Economie et de Science Politique*. 1965, vol. 31, no. 3, pp. 328–357. <https://doi.org/10.2307/139733>

- Considering appointing an expert in computer forensics to examine digital traces,
- Considering the advisability of establishing cooperation with other entities whose statutory task is aml/ctf.

7. Conclusion

The way and length of consultations, opinions, and procedures on the rules about virtual currencies and the related AML/CTF rules mean that when they go into effect, they will not match the new reality at all.²⁴ Policymakers in Europe are trying to change the laws to keep up with methods that are changing at a geometric rate, which is a plan that is doomed to fail from the start. Positive changes happened after virtual currencies had been used in the European market, including the Polish market, for a long time. For example, the AML Act was changed to include rules that require service providers who work with virtual currencies to register. This was done to increase the credibility and transparency of their work.²⁵ The crypto-asset market should be regulated, but it's important to remember that the current rules could cause it to break down (for example, by including – as if automatically – on the list of public warnings of most platforms where crypto-assets are traded) and cause investors and money to flee to Asian markets.

The current legal rules are an example of how the law is constantly being changed and expanded. This won't help technology grow eventually. Disposition MiCA is an example of how the law is getting more complicated, so it should be looked at critically. It adds too many rules about how to do business with cryptocurrencies. According to the author, the requirements in the MiCA regulation will make it hard for new companies to enter these markets. They will also make it expensive for new companies to enter these markets (for example, by making them pay for legal and economic advice), which will cause cryptocurrency providers to move to places with more friendly laws.

List of references

MARTIN, A. Endogenous Multiple Currencies. *Journal of Money, Credit and Banking*. 2006, vol. 38, no. 1, pp. 245–262.

²⁴ NAYLOR, R. T. *Quartermasters of Terror: Inscrutable Orientals and Underground Banks. In Satanic Purses: Money, Myth, and Misinformation in the War on Terror*. McGill-Queen's University Press, 2006, pp. 152–166.

²⁵ MAURER, W. Alternative Globalizations: Community and Conflict in New Cultures of Finance. *Political and Legal Anthropology Review*. 2000, vol. 3, no. 1, pp. 155–172.

- MAURER, B. Data-Mining for Development: Poverty, Payment, and Platform. In: ROY, A., CRANE, E. S. (eds.). *Territories of Poverty: Rethinking North and South*. University of Georgia Press, 2015, pp. 126–143.
- MAURER, W. Alternative Globalizations: Community and Conflict in New Cultures of Finance. *Political and Legal Anthropology Review*. 2000, vol. 3, no. 1, pp. 155–172.
- MIDDLEBROOK, S. T., SARAH, J. H. Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services. *The Business Lawyer*. 2013, vol. 69, no. 1, pp. 263–73.
- MOSAKOWSKI, E., ZAHEER, S. The Global Configuration of a Speculative Trading Operation: An Empirical Study of Foreign Exchange Trading. *Organization Science*. 1999, vol. 10, no. 4, pp. 401–423.
- NAYLOR, R. T. *Quartermasters of Terror: Inscrutable Orientals and Underground Banks. In Satanic Purses: Money, Myth, and Misinformation in the War on Terror*. McGill-Queen's University Press, 2006, pp. 152–166.
- NEWBURG, A. W. G. Financing in the Euromarkets by U.S. Companies: A Survey of the Legal and Regulatory Framework. *The Business Lawyer*. 1978, vol. 33, no. 4, pp. 2171–2194.
- NEWMAN, D. B. Tax Consequences of Foreign Currency Transactions: A Look at Current Law and An Analysis of The Treasury Department Discussion Draft. *The Tax Lawyer*. 1983, vol. 36, no. 2, pp. 223–292.
- O'MALLEY, P. Simulated Justice: Risk, Money and Telemetric Policing. *The British Journal of Criminology*. 20120, vol. 50, no. 5, pp. 795–807.
- PARK, Y. S. Currency Swaps as a Long-Term International Financing Technique. *Journal of International Business Studies*. 1984, vol. 15, no. 3, pp. 47–54.
- PORTES, R., REY, H., DE GRAUWE, P., HONKAPOHJA, S. The Emergence of the Euro as an International Currency. *Economic Policy*, 1998, vol. 13, no. 26, pp. 307–343.
- REDÍN, D. M., CALDERÓN, R., & FERRERO, I. Exploring the Ethical Dimension of „Hawala.“ *Journal of Business Ethics*. 2014, vol. 124, no. 2, pp. 327–337.
- RICE, D. T. The Past and Future of Bitcoins in Worldwide Commerce. *Business Law Today*. 2013, pp. 1–4, JSTOR. Available at: <http://www.jstor.org/stable/businesslawtoday>
- RIMMER, S., PRASAD, R. Electronic Money and Regulatory Responses. *Agenda: A Journal of Policy Analysis and Reform*. 1997, vol. 4, no. 3, pp 371–378.
- SAEED, S., ANCKAR, P. Currency Choice in Industrial Pricing: A Cross-National Evaluation. *Journal of Marketing*. 1998, vol. 62, no. 3, pp. 112–127.
- SHEARER, R. A. The Foreign Currency Business of Canadian Chartered Banks. *The Canadian Journal of Economics and Political Science/Revue Canadienne d'Economie et de Science Politique*. 1965, vol. 31, no. 3, pp. 328–357. <https://doi.org/10.2307/139733>
- STEPHENSON, R. G., POINDEXTER, O. O., MARTZ, D. J. Developments in Cyberbanking. *The Business Lawyer*. 2003, vol. 58, no. 3, pp. 1215–1228.
- TABOR, P. *The Bitcoin (BTC) price has been manipulated many times, the research of the scientist shows*. Available at: <https://pl.investing.com/analysis/kurs-bitcoina-btc-wielokrotnie-manipulowany-wskazuj-a-badania-naukowca-200230146>
- TUBA, MAPHUTI D. The Technology-Neutral Approach and Electronic Money Regulation in the EU: Identifying the Promises and Challenges for Future Regulation in South

- Africa. *The Comparative and International Law Journal of Southern Africa*. 2014, vol. 47, no. 3, pp. 372–400.
- United States: Treasury Regulations on Financial Recordkeeping and Reporting of Currency and Foreign Transactions. *International Legal Materials* 11, no. 3 (1972): pp. 648–51.
- VISHIK, C. Intermediation and Quality Uncertainty in the Internet Environment: New Opportunities for LIS. *Journal of Education for Library and Information Science*. 1999, vol. 40, no. 4, pp. 263–81.
- WALTER, N. The Euro: A New Currency for the World? *The Brown Journal of World Affairs*. 1999, vol. 6, no. 2, pp. 113–23.
- WINN, J. K. Catalytic Impact of Information Technology on the New International Financial Architecture. *The International Lawyer*. 2000, vol. 34, no. 1, pp. 137–147.
- WOPPERER, W. Fraud Risks in E-commerce Transactions. *The Geneva Papers on Risk and Insurance. Issues and Practise*. 2002, vol. 27, no. 3, pp. 383–394.
- ZAMORA, S., EDWARDS, R. W. Capital Flight and the Creditworthiness of Developing Countries. *Proceedings of the Annual Meeting (American Society of International Law)*. 1989, vol. 83, pp. 100–106.