The Anti-money Laundering Challenges of FinTech and Cryptocurrencies

Heidimaria Manninen[*]

Abstract

In the aftermath of the 2008 global financial crisis, the foundation was developed for the protocol we know as blockchain. Blockchain is a system through which money can be sent from one person to another without using any financial service providers. It has been argued that the security of blockchain technology could be the answer to people's mistrust and lost confidence in the financial market. However, blockchain technology and cryptocurrencies go much further than a mere transfer of money. New forms of value exchange have been created, in addition to providing access to financial services in locations where only limited services are offered by traditional banks. As the use of such innovation gains popularity, the legislator is slowly catching up, but how much is covered?

This paper studies FinTech and cryptocurrencies in respect of money laundering. It is found that the current regulatory landscape has several weaknesses that can be attractive for those wishing to exploit them.

Keywords: *FinTech, Anti-Money Laundering, Cryptocurrencies*

[*] Heidimaria Manninen holds an LL.M. from the University of Edinburgh and is currently pursuing an additional LL.M. degree at the University of Helsinki. This paper is based on the author's course paper.

doi:10.51421/njls-2023-0026

1 Introduction

Paper money is highly anonymous and has thus traditionally played an important role in criminal activities[1]. It has been estimated that the amount of money laundered globally is up to 5% of global GDP equalling $2 trillion yearly[2]. The first successful blockchain-based digitally encrypted cryptocurrency, Bitcoin, was invented in 2009 by the pseudonym of Satoshi Nakamoto[3]. The interest around the innovation combining anonymous cash with digital transactions exploded, and it was soon argued that cryptocurrencies have not only revolutionised the financial world[4] but also facilitated anonymous money laundering (ML) to a larger extent[5]. Moreover, this rapid and disruptive technological innovation has been criticised due to its potential to threaten the monetary sovereignty in the Euro area[6].

The FBI has raised concerns over the use of Bitcoin for multiple criminal purposes, such as ML, as the popularity of cryptocurrencies continues to grow[7]. In March 2022, the total market capitalisation of over $2 trillion was divided between over 18,000 cryptocurrencies and 476 exchanges[8]. Bitcoin is the number one cryptocurrency by market capitalisation, and it has been

[1] Kenneth S. Rogoff, The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy, Princeton University Press, 2017, p. 57.

[2] Sisira Dharmasri Jayasekara, How effective are the current global standards in combating money laundering and terrorist financing? Journal of Money Laundering Control 24(2) 2021, p. 257.

[3] Bitcoin Wiki, Research. http://bitcoin.org/bitcoin.pdf, Accessed 29 March 2022; see also prior attempts: Conor Grant, A decade before crypto, one digital currency conquered the world – then failed spectacularly, the Hustle, 30 June 2018. https://thehustle.co/beenz-pre-bitcoin-digital-currency/, Accessed 13 April 2022.

[4] Nicole D. Swartz, Bursting the bitcoin bubble: the case to regulate digital currency as a security or commodity. Tulane Journal of Technology and Intellectual Property 17(1) 2014, p. 322.

[5] Sean Foley – Jonathan R. Karlsen – Tālis J. Putniņš, Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies 32(5) 2019, p. 1799.

[6] CJEU C-422/19 (Dietrich, Häring v. Hessischer Rundfunk), judgment 26 Jan 2021, ECLI:EU:C: 2020:756, para 82.

[7] Kim Zetter, FBI Fears Bitcoin's Popularity with Criminals, Wired, 9 May 2012. http://www.wired.com/2012/05/fbi-fears-bitcoin, Accessed 1 April 2022.

[8] Josh Howarth, How many Cryptocurrencies Are There In 2022, exploding topics, 25 March 2022. https://explodingtopics.com/blog/number-of-cryptocurrencies, Accessed 18 April 2022; see also, CoinMarketCap, https://coinmarketcap.com/, Accessed 18 April 2022.

doi:10.51421/njls-2023-0026

estimated that up to 46% of its transactions are used for criminal purposes, corresponding to a value of €72 billion[9]. When compared to the estimated minimum retail value of the EU drug market of €30 billion in 2017 alone[10], the significance of transaction surveillance can be noted.

Even though the future of cryptocurrencies is still unclear[11], this paper seeks to analyse the anti-money laundering (AML) challenges of FinTech and cryptocurrencies. For this reason, the main concepts of FinTech, blockchain, cryptocurrency and ML are first discussed before moving forward to analyse the topic at hand. Even though this paper does not focus on the legal perspective, it is important to note that the scope set by the regulators has an important impact on what players must implement activities aimed at mitigating ML. This study finds that the AML challenges of FinTech and cryptocurrencies arise from, for example, the decentralised nature of blockchain, anonymity, and the level of transparency (such as pseudonymous Bitcoin or Ethereum, and anonymous privacy coins) afforded by the technology. In addition, the unregulated cryptocurrency operators, such as tumblers and decentralised exchanges, facilitate avenues from crypto-to-fiat[12], the goal of money launderers, and thus provide challenges for crime prevention.

2 Introduction

2.1 FinTech and blockchain technology

FinTech is a general term used for a wide range of technologies disrupting the way traditional financial service providers, like banks, provide financial services, such as mobile payments, digital wallets, peer-to-peer funding platforms or digital assets[13]. These technologies exploit data analytics[14],

[9] Foley – Karlsen – Putniņš, 2019, p. 1800: ”equivalent to $76 billion in April 2017”.

[10] European Monitoring Centre for Drugs and Drug Addiction and Europol, EU drug market report 2019, p. 13. https://www.emcdda.europa.eu/publications/joint-publications/eu-drug-markets-report-2019_en, Accessed 9 May 2022.

[11] See possible future scenarios in, William J. Luther, Bitcoin and the Future of Digital Payments, SSRN 15 July 2015. http://dx.doi.org/10.2139/ssrn.2631314, Accessed 30 March 2022.

[12] A non-exhaustive list.

[13] Jelena Madir, FinTech: Law and Regulation, Edward Elgar Publishing 2019, p. 4-5; see also, Gang Kou et al., Fintech investments in European banks: a hybrid it2 fuzzy multidimensional decision-making approach, Financial Innovation 7(1) 2021, p. 1–28.

[14] For example, big data, AI and machine learning.

cybersecurity[15] and distributed ledger technology (DLT/blockchain)[16], such as cryptocurrencies[17].

Blockchain technology has been a great contributor to FinTech innovation. It consists of blocks of information that have been stored in open-source decentralized distributed ledgers as tokens by using algorithms. The members of a peer-to-peer blockchain network have an individualized key that provides a perpetual cryptographic signature, a hash to protect the transactions. Each transaction is irrevocable and needs to gain an agreement from more than 50% of the network to be recorded to the blockchain. This is also known as the consensus mechanism of reaching an agreement through protocols such as proof-of-work and proof-of-stake[18]. All blocks are visibly chained to each other by computer code ensuring the integrity of each transaction. This means that altering or hacking a blockchain would require controlling more than 51% of the network to be successful.[19] This has also been described as “trustless trust” suggesting a level of security embedded into the technology[20].

The potential of blockchain-based technologies facilitating ML is closely linked to their popularity. As Fintech has been considered the most important facilitator of financial inclusion providing easier, affordable use and access to financial services[21], and thus improving the lives of individuals[22], it could be argued that the basis for such global scale popularity exists. However, the regulators

[15] For example, encryption, authentication, and biometrics.

[16] For example, private key encryption, smart contracts and protocols like proof-of-work and proof-of-stake.

[17] Madir 2019, p. 6.

[18] Hosseini Mojtaba Seyed Bamakan – Motavali Amirhossein – Bondarti Babaei Alireza, A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria, Expert systems with applications 154(1) 2020, p. 1–21; see also, Wenting Li et al., Securing proof-of-stake blockchain protocols, Data privacy management, cryptocurrencies and blockchain technology 10436(1) 2017, p. 297–315.

[19] Sandra Hirsh – Susan Alman, Blockchain, American Library Association 2019, p. 14-15.

[20] Helen Eenmaa-Dimitrieva – Maria José Schmidt-Kessen, Creating Markets in No-Trust Environments: The Law and Economics of Smart Contracts, Computer Law & Security Review 35(1) 2019, p. 69; Usman W. Chohan, Are Cryptocurrencies Truly Trusless? in Stéphane Goutte – Khaled Guesmi – Samir Saadi (eds.), Cryptofinance and Mechanisms of Exchange, Springer International Publishing 2019, p. 77, 79; Riccardo de Caria, Blockchain and Smart Contracts: Legal Issues and Regulatory Responses Between Public and Private Economic Law, Italian Law Journal 6(1) 2020, p. 376.

[21] Douglas W. Arner et al., Sustainability, FinTech and Financial Inclusion, European business organization law review 21(1) 2020, p. 7.

[22] Thi-Hong Van Loan et al., Financial Inclusion and Economic Growth: An International Evidence, Emerging Markets Finance and Trade 57(1) 2021, p. 239.

have recognised that among the growing opportunities there are risks that have not yet been fully understood[23]. Therefore, sandboxes have been established to first test innovative technologies without the obligation to fully comply with regulatory requirements, such as AML measures[24]. Furthermore, it could be argued that such cooperation facilitates knowledge sharing and thus building trust between legislators and the developers.

2.2 Cryptocurrencies and money laundering

The scope of cryptocurrency, also known as virtual currency or digital currency, may vary. The EU Fifth Anti-Money Laundering Directive (AMLD5) refers to cryptocurrencies as virtual currencies[25], whereas the Swiss Financial Market Authority (FINMA) calls them payment tokens[26]. However, even though considered synonymous in broad respect, closer consideration reveals differences. For example, the AMLD5 definition includes stable coins[27] with underlying fiat money deposit, whereas the FINMA approach excludes tokens with a right in rem[28].

It is important to note that tokens or crypto units[29] can be divided into three categories. Payment tokens are used as means of payments, utility tokens give access to service or application, and asset tokens provide a claim against an

[23] Arner et al. 2020, p. 26.

[24] Dirk A. Zetzsche et al., Regulating a revolution: from regulatory sandboxes to smart regulation, Fordham Journal of Corporate Financial Law 23(1) 2017, p. 76.

[25] Directive 2018/843, OJ L 156/43, Article 3(18): "Virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."; see also, Financial Action Task Force (FATF), Virtual Currencies – Key Definitions and Potential AML/CFT Risks June 2014, p. 4, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, Accessed 31 March 2022.

[26] Swiss Financial Market Authority, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16 February 2018, p. 3: "tokens which are intended to be used, now or in the future, as a means of payment for enquiring goods or services or as a means of money or value transfer. Cryptocurrencies give raise to no claims on their issuer".

[27] The value of a stable coin is tied to an external asset, such as a fiat currency (for example, US dollar) or a precious metal (for example, gold), making it less volatile to market price fluctuations.

[28] Thomas A. Frick, Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland, ERA Forum 20(1) 2019, p. 100–101.

[29] Tokens operate on a third-party blockchain unlike crypto coins that have their own blockchain.

issuer, such as a debt or equity. In practice, however, for example, Ethereum provides Ether, a hybrid token, that seeks to combine both payment and utility token functions.[30] Furthermore, cryptocurrencies may be convertible or non-convertible into a fiat currency[31] which makes a paramount difference from ML perspective.

To convert illicit gains to usable assets in the legal economy the typical steps of ML include placement[32], layering[33] and integration[3435]. ML using cryptocurrencies could be done, for example, by exploiting different mixing portfolios offering false transaction networks with higher anonymity and lower traceability[36]. A study argued that those using cryptocurrencies for criminal purposes are more likely to transfer smaller amounts on a repetitive basis and hold fewer cryptocurrencies in one wallet compared to other users[37]. Furthermore, gaming services and token purchases provide vulnerabilities allowing criminals to integrate funds into legitimate circulation[38].

The characteristics making ML through cryptocurrencies appealing are ease, the high volume of transactions, and the low level of costs and detection[39]. On one hand, the benefits of cryptocurrencies also arise from, for example, unlimited control over one’s funds, accessibility via the internet, fast fund

[30] Frick 2019, p. 101.

[31] Financial Action Task Force 2014, p. 5.

[32] Small amounts of cash are deposited to different bank accounts or wallets in cyber space.

[33] The funds are transferred several times from one account/wallet to another in order to conceal where they originally came from.

[34] The target is to integrate the funds into the legal economy by for example, purchasing luxury products or assets such as cars, houses, yachts or by transferring cryptocurrencies into fiat currencies.

[35] Nicholas Gilmour, Illustrating the incentivised steps criminals take to launder cash while avoiding government anti-laundering measures, Journal of Money Laundering Control 23(2) 2020, p. 515.

[36] Rolf van Wegberg – Jan-Jaap Oerlemans – Oskar van Deventer, Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin, Journal of Financial Crime 25(2) 2018, p. 427–428.

[37] Foley – Karlsen – Putniņš 2019, p. 1801.

[38] Sondes Mbarek – Donia Trabelsi – Michel Berne, Are Virtual Currencies Virtuous? Ethical and Environmental Issues. In Stéphane Goutte – Khaled Guesmi – Samir Saadi (eds.), Cryptofinance and Mechanisms of Exchange: Springer International Publishing 2019, p. 42.

[39] Angela Samantha Maitland Irwin – Kim-Kwang Raymond Choo – Lin Liu, An Analysis of Money Laundering and Terrorism Financing Typologies, Journal of money laundering control 15(1) 2012, p. 100.

transfers worldwide,[40] privacy[41] and start-ups raising capital through ICOs[42]. On the other hand, there are concerns related to unclear valuation creation and high volatility[43], in addition to alarming consumption of energy needed for proof-of-work protocols[44], the realised level of anonymity and transferability[45]. Undoubtably, many qualities of cryptocurrencies have potential to facilitate criminal activities such as tax evasion, ML and terrorist financing[46]. However, it has been argued that the global AML threats arise mainly from the blockchain-based technologies, and therefore in minor respect from the cryptocurrencies themselves[47].

3 The AML challenges of FinTech and cryptocurrencies

3.1 Decentralisation and anonymity

When it comes to crime prevention and surveillance of crypto transactions, the decentralised nature of blockchain and the quasi-anonymity of cryptocurrencies create challenges to anti-money laundering efforts. The decentralised nature of blockchain allows placing and transferring criminal proceeds across borders in real-time and through multiple wallets. This makes it hard to stop

[40] Ahmad Al-Naimi – Esra Al-Trad – Razan A. Yousef, Trends of FinTech and cryptocurrencies Jordan recapitulation, International Journal of Entrepreneurship 25(4) 2021, p. 12.

[41] Chris Richter – Sascha Kraus – Ricarda B. Bouncken, Virtual currencies like bitcoin as a paradigm shift in the field of transactions, International Business & Economics Research Journal 14(4) 2015, p. 582.

[42] Giancarlo Giudici – Saman Adhami, The impact of governance signals on ICO fundraising success, Journal of Industrial and Business Economics 46(2) 2019, p. 283–312.

[43] Giancarlo Giudici – Alistair Milne – Dmitri Vinogradov, Cryptocurrencies: Market analysis and perspectives, Journal of Industrial and Business Economics, 47(1) 2020, p. 5.

[44] John Vaz – Kym Brown, Sustainable development and cryptocurrencies as private money' Journal of Industrial and Business Economics 47(1) 2020, p. 181.

[45] Pierluigi Martino, Blockchain and Banking: How Technological Innovations Are Shaping the Banking Industry, Palgrave Macmillan 2021, p. 22.

[46] Robby Houben – Alexander Snyers, Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax Evasion, Study requested by the TAX3 Committee European Parliament July 2018, p. 11.

[47] Malcolm Campbell-Verduyn, Bitcoin, crypto-coins, and global anti-money laundering governance, Crime, Law and Social Change 69(2) 2018, p. 283.

suspicious transactions in the layering step and to obstruct the transfer of funds into avenues providing access from crypto-to-fiat.[48]

In traditional transactions a third-party, typically a licensed bank, has had an important role in guaranteeing the authenticity and the integrity of fund transfers. On one hand, with the rise of efficient and low-cost blockchain technology, some argue that such mediating role has run its course[49]. On the other hand, as the process relies on security provided by the public key cryptographies, there is no third-party safety net available if the personal key linked to blockchain assets goes missing[50].

Criminals can exploit the quasi-anonymity of blockchain and place assets on the market without being identified. Furthermore, the transactions are even harder to detect when criminals use mules in the layering phase, Moreover, cryptocurrencies provide opportunities to cash out illicit gains by transferring them anonymously to individuals which can be challenging, if not impossible, to trace.[51]

The traceability of cryptocurrencies can be considered both easy and complex depending on the anonymity protocols in use[52]. Most cryptocurrency transactions can be traced to the original owner with over 90% probability[53]. Moreover, when the custodial solution, the crypto wallet[54], provides only an access code and the private/public key without owner ID[55], this means that cryptocurrencies placed in the crypto wallet remain anonymous and only

[48] Kim-Kwang Raymond Choo, Cryptocurrency and virtual currency: Corruption and money laundering/terrorism financing risks? In David Lee Kuo Chuen (Eds.), Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data, Academic Press 2015, p. 302–304.

[49] Hirsh – Alman 2019, p. 18.

[50] Ibid., p. 19.

[51] Campbell-Verduyn 2018, p. 287.

[52] Kuo Lee David Chuen – Robert H. Deng, Handbook of Blockchain, Digital Finance, and Inclusion: Cryptocurrency, FinTech, InsurTech, and Regulation, Elsevier Science & Technology 1(1) 2017, p. 240.

[53] Philip Koshy – Diana Koshy – Patrick McDaniel, An analysis of anonymity in bitcoin using P2P network traffic, Financial Cryptography and Data Security: 18th International Conference FC 2014, Revised Selected Papers 18. Springer 2014, p. 469–485.

[54] There are different types of wallets such as hardware, desktop, online, mobile apps or paper. They can also be described as hot wallets (connected to internet) or cold wallet (offline).

[55] Daniel Dupuis – Kimberly Gleason, Money laundering with cryptocurrency: open doors and the regulatory dialectic, Journal of Financial Crime 28(1) 2021, p. 63.

transactions in/out are transparently recorded to the blockchain[56]. However, it could be argued that anonymity is not enough to make cryptocurrencies popular on the universal scale due to weaknesses, such as the lack of negotiability[57], the high volatility[58] and security issues related to the crypto wallets and cryptographic keys[59]. Furthermore, to mitigate AML with cryptocurrencies it has been argued that implementing due diligence processes could be an effective way to tackle the major challenge of anonymity and traceability[60].

3.2 Decentralisation and anonymity Beyond crypto-fiat gatekeepers: the un-regulated avenues exploited by money launderers[61]

Crypto exchanges and wallet custodians[62] that want to operate in the EU single market need to register with the local authority, and thus also, for example, implement know your customer (KYC) onboarding procedures, monitor transactions, and report suspicious activity. It could be argued that these obligations are crucial from crime prevention perspective. Furthermore, it also means that relevant authorities will have access to information revealing

[56] Dupuis – Gleason 2023, p. 64.

[57] Victor Dostov – Pavel Shust, Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?, Journal of Financial Crime 21(3) 2019, p. 249.

[58] Milind Tiwari – Adrian Gepp – Kuldeep Kumar, A Review of Money Laundering Literature: The State of Research in Key Areas, Pacific Accounting Review 32(2) 2020, p. 281–282.

[59] Valeonti Foteini et al., Crypto Collectibles, Museum Funding and OpenGLAM:Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs), Applied Sciences 11(21) 2021, p. 6; see also, Johathan Ponciano, Second Biggest Crypto Hack ever: $600 Million In Ether Stolen From NFT Gaming Blockchain, Forbes, 29 March 2022. https://www.forbes.com/sites/jonathanponciano/2022/03/29/second-biggest-crypto-hack-ever-600-million-in-ethereum-stolen-from-nft-gaming-blockchain/, Accessed 14 April 2022; Jonathan Greig, Report: $2.2 billion in cryptocurrencies stolen from Defi platforms in 2021, ZDNet, 6 January 2022. https://www.zdnet.com/finance/blockchain/22-billion-in-crypto-currency-stolen-from-defi-platforms-in-2021-report/, Accessed 14 April 2022.

[60] Valentina Covolo, The EU Response to Criminal Misuse of Cryptocurrencies: The Young, already Outdated 5th Anti-Money Laundering Directive, European Journal of Crime, Criminal Law and Criminal Justice 28(3) 2020, p. 217–251.

[61] Daniel Dupuis – Kimberly Gleason, Money laundering with cryptocurrency: open doors and the regulatory dialectic, Journal of Financial Crime 28(1) 2021, s. 60–74.

[62] Most cryptocurrency exchanges provide wallet services, but there are also wallet providers who offer only a service to store cryptocurrencies online or offline, but not crypto exchange services.

crypto users.[63] For those seeking privacy, this is an issue. However, there are several blind spots available for criminals to exploit when converting crypto-to-fiat, and thus facilitating ML, such as mixers and tumblers, over the counter (OTCs) trading, privacy coins, decentralized exchanges, direct retail purchases using cryptocurrencies and miners.

Tumblers provide mixing services aiming to conceal or recharacterize the proceeds gained through illegal activities making it difficult to trace[64]. This could happen using, for example, known tumbling services like Coin Fog or by one user sending bitcoins to another user who then sends them back in one or more transactions[65]. It should be noted that using a mixing or tumbling service is not illegal as such, especially if complying with certain reporting and record-keeping requirements[66]. However, when exploiting services on the dark web the risk of taking part in criminal activities might rise[67].

OTC market provides trading opportunities through crypto brokers, like Kraken[68], or person-to-person without supervision enabling the selling and buying of cryptocurrencies directly between parties[69]. The lack of organised exchange opens an opportunity for users to swap their public keys or convert cash to crypto by simply scanning a QR code when making transactions[70].

Contrary to pseudonymous coins, like Bitcoin and Ethereum, privacy coins have been created to exploit the anonymity of blockchain technology to a

[63] Vitalii Rysin – Mariia Rysin, The money laundering risk and regulatory challenges for cryptocurrency markets. In: Marek Dziura – Andrzej Jaki – Tomasz Rojek (Eds.), Restructuring Management: Models – Changes – Development, Cracow University of Economics 2020, p. 188–189.

[64] Rainer Böhme et al., Bitcoin: Economics, technology, and governance, Journal of Economic Perspectives 29(2) 2015, p. 230.

[65] Foley – Karlsen – Putniņš 2019, p. 1813.

[66] Alicia Schmidt, Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model, International Journal of Law and Information Technology 29(4) 2022, p. 16.

[67] Kollen Post, US Financial Watchdog Fines early Bitcoin Mixer $60M for Money Laundering, Cointelegraph, 19 October 2020. https://cointelegraph.com/news/us-financial-watchdog-finesearly-
bitcoin-mixer-60m-for-money-laundering, Accessed 13 April 2022.

[68] See, Kraken. https://www.kraken.com/, Accessed 1 April 2022.

[69] Liz Louw, OTC Cryptocurrency Markets – An Introduction, Bitstocks, 4 January 2019. https://blog.gravity.eco/otc-cryptocurrency-markets-an-introduction?hs_amp=true, Accessed 2 April 2022.

[70] Daniel Dupuis – Kimberly Gleason, Money laundering with cryptocurrency: open doors and the regulatory dialectic, Journal of Financial Crime 28(1) 2021, p. 57–58.

higher extent[71]. For example, Zcash promises to hide the transactions using a shielded pool, however, a recent study revealed that almost all Zcash transactions can be traced in practise by looking into identifiable patterns of usage[72]. Furthermore, at least some past Monero transactions with one or more mixers can be traced using advanced mathematical analysis[73]. This is good news from crime prevention perspective as it allows identifying ML transactions and take preventive action.

Cryptocurrency exchanges allow users to trade cryptocurrencies[74]. Many of the cryptocurrencies operate on decentralized blockchain platforms which means they are not controlled by any authority or administrator[75]. The main transaction types are, crypto-to-crypto, crypto-to-fiat with client an identification KYC[76] and crypto-to-fiat without client identification[77]. However, some exchanges provide hybrid solutions meaning that they offer both crypto-to-crypto and crypto-to-fiat trading with the requirement to implement identification process only when converting cryptocurrencies into fiat currencies[78]. Furthermore, there are also output platforms available, such as PayPal, Perfect Money, Westerns Union and Bitonic, that facilitate anonymity enhanced cash-out strategies with a minimum registration requirement of disclosing only the user's Tor email address[79].

The Financial Action Task Force (FATF) has recommended imposing AML requirements on entities relating to cryptocurrencies[80]. However, from the perspective of crime prevention, its weakness arises from the focus to the relationship between traditional banks and cryptocurrencies leaving

[71] Christoph Wronka, Money Laundering through Cryptocurrencies - Analysis of the Phenomenon and Appropriate Prevention Measures, Journal of money laundering control 25(1) 2022, p. 84.

[72] Kappos George et al., An Empirical Analysis of Anonymity in Zcash, 27th USENIX Security Symposium, USENIX Security 18 2018, p. 1.

[73] Malte Möser et al., An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies 3 2018, p. 158.

[74] Fan Fang et al., Cryptocurrency Trading: A Comprehensive Survey, Financial innovation 8(1) 2022, p. 7.

[75] Doron Goldbarsht – Luis de Koker, Financial Technology and the Law: Combating Financial Crime, Law, Governance and Technology Series 47, Springer 2022, p. 239.

[76] See for example Coinbase, Kraken, Gemini, itBit, OKCoin, Bitstamp.

[77] Dupuis – Gleason 2021, p. 64.

[78] Ibid.; See for example Binance, BitMax, KuCoin and StormGain.

[79] Van Wegberg – Oerlemans – van Deventer 2018, p. 429.

[80] Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers June 2019, para 8. http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf, Accessed 31 March 2022.

cryptocurrency networks largely out of its scope. In addition, the implementation relies on the domestic regulators. Therefore, only small exchanges like OKEx and BitBay have ended up delisting some suspicious cryptocurrencies[81].

From a ML perspective, the scope of unregulated exchanges provides a challenge to crime prevention. For example, the wording of the AMLD5 provides a loophole in implying that the decentralized exchanges are not considered to be custodian wallet providers if the users enter the privacy keys for each transaction manually, and thus not be stored by the exchange providers themselves[82]. However, both ESMA and EBA have agreed that crypto-to-crypto exchanges should be included in the definition of obligated entities[83].

To take advantage of the positive features of blockchain technologies, innovations create opportunities to buy valuable assets, such as real estate,[84] gold,[85] luxury cars[86] or diamonds[87] with cryptocurrencies. Furthermore, lending platforms not only connect lenders and borrowers but also facilitate several repayment options in cryptocurrencies[88]. Lastly, crypto mining can be used as a front for ML activities. As it is relatively difficult for others to analyse the efficiency of miners, these operators can mix illegal coins with mined coins to hide their true origin[89].

[81] Dupuis – Gleason 2021, p. 69.

[82] Directive 2018/843, OJ L 156/43, Article 1(1)(c).

[83] European Securities and Markets Authority Advice 9 January 2019: Initial Coin Offerings and Crypto-Assets, p. 36; European Banking Authority Report 9 January 2019: Advice for the European Commission on crypto-assets, p. 20–21.

[84] Bitpay, How to Buy a House with Cryptocurrency, bitbay, 19 December 2021. https://bitpay.com/blog/buy-a-house-with-cryptocurrency/, Accessed 14 April 2022; compare, Fausto Martin de Sanctis, International Money Laundering Through Real Estate and Agribusiness A Criminal Justice Perspective from the "Panama Papers", Springer International Publishing, 1 2017.

[85] See for example, Vaultoro, Exchange your cryptocurrencies to gold or silver and back within seconds. https://vaultoro.com/, Accessed 14 April 2022.

[86] See for example, BitCars, https://bitcars.eu/collections/buy-supercars-cars-with-bitcoin-and-crypto, Accessed 14 April 2022.

[87] See for example, Hyde Park Design, Buy Diamond Engagement Rings with Cryptocurrency, https://hydeparkdesign.com/pages/buy-diamonds-bitcoin-cryptocurrency, Accessed 14 April 2022.

[88] David Lee Kuo Chuen – Robert H. Deng, Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation, Elsevier Science & Technology 2017, p. 217.

[89] Dupuis – Gleason 2021, p. 71.

Undoubtedly, unregulated operators provide avenues for illicit proceeds to make their way amongst the legitimate circulation and thus challenge crime prevention in a new way. However, some jurisdictions, such as the US, have classified cryptocurrencies as property, and thus extending the definition of gross income to cover the exchange of cryptocurrencies for products or services making them taxable income[90].

It has been argued that common AML controls could lower the risk of illegal use of cryptocurrencies[91]. In addition, there are computer programs available that use clustering and proprietary algorithms to deanonymize crypto transfers[92]. Furthermore, authorities may seek to form partnerships with private entities that provide crypto tracking services[93]. Such mitigating actions can prevent the negative consequences ML operations have on society[94].

4 Conclusion

It could be argued that the borderline from crypto-to-fiat can be relatively well monitored if deemed necessary for AML purposes. Criminals who want to convert assets gained by illicit means must go through crypto-to-fiat exchanges, which on organized markets must comply with AML requirements. Even though crypto wallets do offer a certain level of privacy, most of the transactions can be traced, which then also provides ways to identify the owners of the wallets after analysing transaction patterns. The lack of government control makes cryptocurrencies an intriguing option for criminal exploitation. However, the level of opportunities for ML activities varies depending on what products and services are being offered to the users and how much money and resources are being invested into AML and crime prevention.

[90] Diedre A. Liedel, The taxation of bitcoin: How the IRS views cryptocurrencies, Drake Law Review 1 2018, p. 117–118.

[91] Chad Albrecht et al., The use of cryptocurrencies in the money laundering process, Journal of Money Laundering Control 22(2) 2019, p. 215.

[92] See for example, Ethical hacking and penetration testing, How to trace a Bitcoin wallet transaction: Bitcoin transaction visualization. https://miloserdov.org/?p=3231, Accessed 24 March 2022.

[93] David Klasing, How Does the IRS Track Bitcoin and Other Cryptocurrencies?, Klasing Associates, 3 January 2022. https://klasing-associates.com/irs-track-bitcoin-cryptocurrencies, Accessed 24 March 2022.

[94] Goldbarsht – de Koker 2022, p. 83.

Legal regulation provides the rules of what is considered legal and what is not. Currently, the risks of ML via cryptocurrencies are not efficiently covered. This paper identified several blind spots that provide challenges to AML, FinTech and cryptocurrencies arising from the very nature of the blockchain technology and the unregulated players offering products and services that in practice make available avenues to convert illicit funds from crypto-to-fiat nominated assets.