

BLOCKCHAIN BASED ASSETS AND ANTI-MONEY LAUNDERING:
A LAW AND ECONOMIC ANALYSIS

Lukas Müller^{*}, Irina Langenegger^{**} & Samathida Kem^{***}

The emergence of blockchain technology will impact the world in many aspects. By recording the provenance of digital assets, the decentralized, distributed ledger technology provides many advantages and opportunities to society but not without potential negative impact that requires careful examination. This paper investigates the relationship between blockchain technology and money laundering to provide a theoretical framework evaluating whether the technology could potentially encourage money laundering activities. To analyze the relationship, this paper develops an expected utility function of money laundering derived from the expected utility function of a crime. This model explores the changes in the expected utility from money laundering as a function of a number of explanatory variables adopted specifically to fit the elements of money laundering and the two most widespread blockchain asset classes—payment and asset tokens. Through this theoretical analysis, the majority of the aspects of the blockchain applications are found to have the potential to increase the expected utility from money laundering, therefore making the technology appear attractive to money launderers. The conclusion drawn in this paper sets an important first step in understanding the potential impact of blockchain and identifies certain aspects of it that require the attention of regulators to ensure that society can reap the benefits of this complex yet valuable technology while limiting its negative impact related to criminal activities.

I. INTRODUCTION

The rise of technology in recent years has changed the world faster than ever imagined in the past. While many are bracing for the transformation, much of it is still puzzling everyone, from engineers, programmers and

^{*} Lukas Müller, Attorney-at-Law (Switzerland), Ph.D. (University of St. Gallen), MLaw (University of Zurich), M.A. (University of Zurich), LL.M. (Columbia University).

^{**} Irina Langenegger, M.A. of Law and Economics (University of St. Gallen) and LL.M. in International Law (The Fletcher School of Law and Diplomacy) double degree program, B.A. HSG in Law and Economics (University of St. Gallen), Switzerland.

^{***} Samathida Kem, Master of International Affairs, International Finance and Economic Policy (Columbia University), B.A. in Economics (American University, Washington, DC), B.A. in Interdisciplinary Studies: Communications, Legal Institutions, Economics and Government (American University, Washington, DC).

developers to scholars, journalists, policy-makers and regulators. The ascent of the distributed ledger technology¹ has therefore unsurprisingly led to a wide and immense quantity of expert opinions, public discussions as well as regulatory debates and amendments. Regarding the crypto hype, the stakeholders approach a dilemma. While the new technology allows for significant opportunities for the economy, it also opens up to possibilities of illicit activities, particularly money laundering.² Interestingly, the connection of tokens with money laundering is usually assumed based on a few features such as

¹ See Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG 1, <https://bitcoin.org/bitcoin.pdf> (last visited Jul. 29, 2020), with the Bitcoin for a famous application of the distributed ledger technology. *United States v. Costanzo*, 956 F.3d 1088, 1091 (9th Cir. 2020) (“Bitcoin is an alternative currency that can be transferred electronically anywhere in the world with no bank and no government forms.”). According to *United States v. Brown*, 857 F.3d 334, 341 (6th Cir. 2017) Bitcoin is a “virtual, sovereign-free currency.” A recent court decision defines Bitcoin as “Bitcoin is a decentralized form of electronic or digital currency that exists only on the [i]nternet.” *United States v. Lord*, 915 F.3d 1009, 1013 n.1 (5th Cir. 2019). According to the memoranda opinion in *United States v. Harmon*, No. 19-cr-395, Memoranda Opinion, Jul. 24, 2020 (D.D.C. 2020), persons who are converting virtual currencies like Bitcoin to fiat money need a money transmitter license; see 18 U.S.C. § 1960 and the DC Money Transmitter Act. However, these decisions do not confer Bitcoin the same legal status of a legal tender like US Dollar or any other currency issued by a sovereign state.

² See e.g. Brandon M. Peck, *The Value of Cryptocurrencies: How Bitcoin Fares in the Pockets of Federal and State Courts*, 26 U. MIAMI BUS. L. REV. 191, 213-221 (2017) (discussing the possibilities of money laundering using cryptocurrencies and how a court was missing the money laundering potential of cryptocurrencies; see Order Granting Defendant’s Motion to Dismiss the Information, *State v. Espinoza*, No. F14-2923, at 7 [Fla. Cir. Ct. dismissed July 22, 2016]). Other jurisdictions, for example, the Member States of the European Union or Switzerland, are applying money laundering laws on cryptocurrencies; see e.g. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU 2018 O.J. (L 156) 43–74; see Swiss Fin. Mkt. Supervisory Auth. [hereinafter “FINMA”], Guidance 02/2019, Payments on the Blockchain (Aug. 26, 2019); see also Press Release, FINMA guidance: stringent approach to combating money laundering on the blockchain, (Aug. 26, 2019), available at <https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/> (last visited Jul. 29, 2020). See also Christopher Whyte, *Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise*, STUD. IN CONFLICT & TERRORISM 1, 6–7 (2019), available at <https://doi.org/10.1080/1057610X.2018.1531565> (last visited Jul. 29, 2020); Steven Mnuchin, Sec’y, U.S. Dep’t of Treasury, Panel Discussion at the World Economic Forum: The Remaking of Global Finance (Jan. 25, 2018), available at <https://www.weforum.org/events/world-economic-forum-annual-meeting-2018/sessions/the-remaking-of-global-finance> (last visited Jul. 29, 2020) (declaring his primary goal is “to make sure that [virtual currencies are] not used for illicit activities” and, to do this, he has suggested “the world have the same regulations”).

anonymity and decentralization.³ With the distributed ledger technology and the immense amount of different applications arisen so far, however, a more fundamental analysis of the different aspects of the blockchain is necessary in order to conclude if the distributed ledger technology is vulnerable to money laundering.

To provide such analysis, this paper focuses on the two most widespread asset classes on blockchains: payment and asset tokens.⁴ Payment tokens are issued as means of payment.⁵ Asset tokens represent underlying assets, such as shares, art and real estate.⁶ The question central to this paper is whether or not the two asset classes are likely to be used as money laundering instruments—particularly compared to traditional means.⁷ To provide an encompassing view, no particular typology of money laundering is analyzed and illegal funds stemming from cybercrimes as well as regular crimes are included. Where necessary, differentiations are undertaken. As with modern money laundering methods the differentiation among placement, layering and integration is outdated,⁸ the whole money laundering process is analyzed. The research is limited to decentralized tokens with an underlying blockchain, excluding centralized systems. Centralized tokens—for example, Ripple—are fundamentally different from decentralized tokens and a lot closer to a regular currency or a form of security issued by a private party.⁹ Thus for centralized tokens, the conventional policy against anti-money laundering is applicable.¹⁰

This paper first presents a model from the economics of crime to identify when criminals actually decide to launder money. The model is then analyzed

³ See e.g. *United States v. Le*, 902 F.3d 104, 107 (2d Cir. 2018); Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441, 447 (2014).

⁴ See FINMA, Guidelines for Enquiries regarding the Regulatory Framework for Initial Coin Offerings (ICOs) 3 (Feb. 16, 2018); Eric D. Chason, *How Bitcoin Functions as Property Law*, 49 SETON HALL L. REV. 129, 135 (2018).

⁵ See FINMA, Guidelines for Enquiries regarding the Regulatory Framework for Initial Coin Offerings (ICOS) 3 (Feb. 16, 2018).

⁶ See *id.*

⁷ Regarding the legal point of view see the sources and legislative materials *supra* note 2.

⁸ See Stefan D. Cassella, *Toward a new Model of Money Laundering: Is the “placement, layering, integration” Model obsolete?* 21 J. MONEY LAUNDERING CONTROL 494, 495–96 (2018) (who argues that this threefold model is outdated and has little application to most money laundering scenarios).

⁹ A centralized virtual currency or token has a central administrator or repository. See e.g. FREDERIK ARMKNECHT ET AL., *RIPPLE: OVERVIEW AND OUTLOOK*, INTERNATIONAL CONFERENCE ON TRUST AND TRUSTWORTHY COMPUTING, 163-165 (2015).

¹⁰ See e.g. the Bank Secrecy Act (Currency and Foreign Transactions Reporting Act of 1970), Pub. L. No. 91-508; see also C.F.R. § 103.22(a); and the Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001), Pub. L. No. 107-56; JOHN ARMOUR ET. AL., *PRINCIPLES OF FINANCIAL REGULATION*, 69 (2016).

based on the different aspects of payment and asset tokens in comparison to traditional money laundering instruments. The result will shed light on whether or not payment and asset tokens are favorable money laundering instruments. The paper provides a theoretical framework for regulatory authorities, investigative agencies, developers of new tokens and researchers. It facilitates the identification of aspects of payment and asset tokens that are susceptible to money laundering, as well as of aspects facilitating the discovery of money laundering.

II. ECONOMICS OF MONEY LAUNDERING

A. *Utility Function of the Criminal*

A rational person will commit a certain crime if the utility of perpetrating the crime is higher than the utility of not doing so, according to the economics of crime¹¹ and the usual analysis of rational choice.¹² The foregone utility of not committing a crime is an opportunity cost, a part of the total expected costs.¹³ From the perspective of a utility-maximizing person, the expected benefits of committing a crime need to exceed the expected costs in order for them to choose this course of action. The benefits of committing a crime include monetary values of the proceedings of the crime, such as money or asset values, as well as psychological and emotional values, such as the pleasure derived from the fulfillment of revenge, feelings of superiority or similar benefits.

On the other hand, the costs are divided into certain and uncertain costs. There are three different categories in the certain costs of the crime. The first and most obvious category is the direct costs of committing a crime. The second category contains what is called opportunity costs. While the illegal act is executed, a legal occupation or a different illegal action¹⁴ that could

¹¹ See e.g. RICHARD E. POSNER, *ECONOMIC ANALYSIS OF LAW* 253–267 (9TH 2014); JEREMY BENTHAM, *PRINCIPLES OF PENAL LAW*, Chap. 6 Rule 1 (1788).

¹² See Joras Ferwerda, *The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?*, 5 *REV. L. & ECON.* 903, 904 (2009).

¹³ It is an opportunity cost of committing a crime because when a person commits one crime, she or he lose an opportunity to do something else. That opportunity to do something else is the utility of not committing a crime, so the utility of not committing a crime is an opportunity cost of committing a crime. So, let us say if the person does not commit the crime, she or he can drive a taxi and make \$100 (that is the utility they get from not committing a crime). That \$100 is also an opportunity cost of committing a crime because if the person commits the crime, then she or he could not make \$100 by driving a taxi. So basically, if committing the crime only makes the person \$50, she or he would not commit the crime because their utility from not committing the crime is higher. This variable presents in our equation too, in the form of opportunity cost.

¹⁴ See *supra* note 12, at 904.

otherwise be pursued is foregone—simply put, a lost opportunity. Thus, the possible net proceeds from the alternative action need to be added as opportunity costs of committing the specific crime. These opportunity costs can be determined as the amount the person could otherwise earn.¹⁵ The third category is the psychological and moral costs of having committed a crime.¹⁶

As for the uncertain costs, which are derived from the probability of getting caught, the possible punishment and the consequential probable future costs are considered. These include a fine and the monetary value of imprisonment as well as the opportunity costs for being incapable of working whilst in jail. A possible disgorgement is also recognized under this category.¹⁷ These costs need to be weighted according to the expected probability of conviction, as it is not certain that the criminal will be detected, apprehended or convicted.¹⁸

The utility function of the criminal is elaborated to ascertain whether a rational person commits a crime. Simply, there are two possible outcomes for every crime—either the criminal is convicted and punished or the criminal is not caught or convicted and thus not punished.

If we then denote EU as the expected utility derived from committing a certain crime, U as a utility function, y as the benefits originating from the crime, tc as the transaction costs summarizing the three different types of certain costs of committing the crime, f as the monetary value of the uncertain costs/the punishment and p as the probability of conviction, the utility function of a regular crime can be developed as follows:¹⁹

$$EU = pU(y - f - tc) + (1 - p)U(y - tc)$$

Where the first part of the utility function represents the event where the

¹⁵ Here, the direct energies invested in the analyzed illegal pursuit are meant. In their studies, L. Armeij & F. Melese, *Minimizing Public Sector Corruption: The Economics of Crime, Identity Economics, and Money Laundering*, DEF. & PEACE ECON. J. 1, 3–8 (April 2017). follow a different approach. These authors assume that legal and illegal activities are not exclusive but instead can be combined.

¹⁶ Where high differences depending on the considered person can be found, as a person with high moral standards will regard these costs as immense, whilst an amoral criminal will consider them as equating to zero. However, certain approaches examine the utility of a rational, amoral person, and thus exclude these costs, see ROBERT COOTER & THOMAS ULEN, *LAW AND ECONOMICS* 463 (6th ed. 2016).

¹⁷ Which is the reason why the benefits derived from the crime are still received even if the criminal is convicted.

¹⁸ See COOTER & ULEN, *supra* note 16, at 465.

¹⁹ See COOTER & ULEN, *supra* note 16; see E. H. Warren, Jr., *The Economic Approach to Crime*, 20 CANADIAN J. CRIMINOLOGY 437, 441 (1978) (who argues that the economic approach to crime is especially suited to give insights for property crime and derives different models for its analysis).

criminal is convicted and punished, and the second part describes the event where the criminal is not convicted and thus not punished.

If *EU* has a positive value, a positive expected utility is achieved through the perpetration of the crime and thus the crime will be committed. If the expected utility function has a negative outcome,²⁰ then the person will expect to derive no utility from committing the crime and will refrain from perpetrating the illegal action.

B. *Utility Function of the Money Launderer*

To apply the utility function elaborated in the previous chapter to money laundering, the specialty of this crime needs to be considered. Money laundering is a dual crime, which leads to the need for adapting the utility function of the criminal. Money is “dirty”, i.e., illicit, and needs to be laundered only if it proceeds from a crime which is a criminal felony or aggravated tax misdemeanor. Usually, proceeds from a minor criminal wrongdoing are not considered as illicit in the sense of anti-money laundering laws.²¹ The specific crimes qualify as predicate offenses to money laundering may vary depending on the laws of each jurisdiction. However, as the earnings need to arise from a criminal action, there must always be at least two crimes committed: first is the predicate offense generating some kind of asset values and second is the act of money laundering of those assets gained through the predicate offense.²² These two crimes do not have to be perpetrated by the same person; however, for simplicity this paper assumes that they are committed by the same person.

Through the necessary connection of the two crimes, the discovery of the money laundering act can lead to the discovery of the predicate offense. Thus, in addition to the previous two scenarios of conviction or no conviction, there is a third possible scenario in money laundering.²³ In the first scenario, the predicate offense and the money laundering process remain undiscovered, whereby the criminal enjoys all the proceeds of her or his crime with no repercussions. In the second scenario, the predicate offense is discovered through the detection of the money laundering activities, leading to

²⁰ *EU* is negative.

²¹ See Shawn Turner, *U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering*, 54 CASE W. RES. L. REV. 1389, 1405–1406 (2004) (who first analyses the social costs of money laundering to then assess a viable economic approach to cyberlaundering; the practice of laundering money online or in cyberspace is called “cyberlaundering”).

²² See FERWERDA, *supra* note 12, at 3.

²³ The fourth option, where the predicate offense is discovered before money laundering has taken place is ignored in this context, as the focus lies on money laundering and this process does not take place if the predicate offense is directly discovered.

convictions for both offenses. The third scenario is when the act of money laundering is discovered but without any trace to the predicate crime, leading to no conviction and punishment for the predicate crime.²⁴ In this case, there is a conviction and punishment for the act of money laundering but not for the predicate crime. These three different scenarios result in the following expected utility function:²⁵

$$EU_{ML} = (1 - p)U(y - tc) + pzU(y - f_c - f_{ML} - tc) + p(1 - z)U(y - f_{ML} - tc)$$

- Where EU denotes the expected utility derived from laundering the proceeds of a committed crime, thus transforming potential purchasing power into effective purchasing power²⁶ usable in the legal economy;
- Variable y represents the net proceeds that are laundered, calculated as the total income from the predicate offense deducted by the costs of the predicate offense and the part of the proceeds that are obtained but not laundered;²⁷
- Variable tc is the aggregate transaction costs of the money laundering process, which comprise of first-category certain costs arising from the technique and technology deployed in the money laundering process as well as legal transaction costs due to anti-money laundering regulation;²⁸
- The monetary loss due to disgorgement and incarceration and the arising opportunity costs due to loss of work whilst in jail is denoted by f_{ML} for money laundering and f_c ²⁹ for the predicate crime respectively;³⁰

²⁴ This is possible in certain legislations as it only has to be proven that the asset values derive from illegal actions and not that the illegal actions need to be evinced or even convicted themselves. Also, this option is not given in the individual utility function if the money launderer has not committed the predicate offense, as the money launderer would not be punished.

²⁵ See FERWERDA, *supra* note 12, at 3–5.

²⁶ See Donato Masciandaro, *Money Laundering: The Economics of Regulation*, 7 EUR. J. L. & ECON. 225, 238 (1999) (providing an economic framework to enable the assessment of money laundering and its regulation).

²⁷ These last two need to be subtracted as we want to ascertain the utility of laundering money, which implies that we only regard the actual amount of laundered money.

²⁸ See Masciandaro *supra* note 26, at 227.

²⁹ Which punishes the entire predicate crime and thus might surpass the value of y .

³⁰ The monetary value of a sentence can be determined as the maximum amount of money the convicted would be willing to pay to obviate his prison term. Warren, *supra* note 19, at 449. *Contra* Michael K. Block & Robert C. Lind, *Crime and Punishment Reconsidered*, 4 J. LEGAL STUD. 241, 243–44 (1975) (arguing that “ f_j [the monetary equivalent of the punishment] may fail to exist.”)

- And p denotes the probability of conviction for the money laundering act and z denotes the probability of conviction for the predicate offense when the criminal is convicted of money laundering.³¹

The decision to commit a money laundering offense is made based on the value of EU . If EU is positive, the person expects to derive utility from laundering the asset and will thus do so. If EU is negative, the person expects to obtain no utility from money laundering and will thus refrain from doing so.

As the values of the variables in the utility function depend strongly on the criminal's circumstances and thus vary accordingly,³² the elaboration of the criminal's expected utility function allows for an analysis of the variation in the expected utility driven by the circumstances. The focus is hereby laid on the new developments surrounding payment and asset tokens.

III. MONEY LAUNDERING WITH PAYMENT AND ASSET TOKENS

In order to evaluate the effects of blockchain-based applications on money laundering, this section will analyze different features of blockchain-based phenomena using the expected utility function developed in the previous section. Depending on the characteristics of the features a conclusion can be reached if blockchain-based money laundering is more favorable than traditional money laundering. Only after answering this question regulators or lawmakers should consider regulating blockchain-based money laundering, because else the regulation could be obsolete. The applications of interest are payment and asset tokens. If their features prove to be advantageous and therefore increase the expected utility of money laundering, three possible outcomes may occur. First, for people whose expected utility is already positive before the introduction of blockchain technologies, the increase in the expected utility derived from the use of blockchain-based applications leads to a shift from traditional means to blockchain-based money laundering. However, this does not change the number of money laundering cases as these people would have committed the offense anyway. In other words, it changes the methods used in money laundering but not the levels. Second, for those whose expected utility of money laundering without blockchain-based means is negative, the expected utility may become positive if the increase driven by the use of blockchain-based applications is big enough. This leads to an increase in overall money laundering, all other factors being constant. Third, the features of blockchain-based applications increase the expected utility for those whose expected utility of money laundering without blockchain is negative; however, the increase is not big enough to bring the

³¹ See FERWERDA, *supra* note 12, at 3–5.

³² See Warren, *supra* note 19.

expected utility to above zero. In this case, no new money laundering offenses will be committed and therefore the overall levels remain unchanged. However, if the features of the blockchain-based applications are not superior to traditional means and therefore do not increase the expected utility, these new technologies will not be used by any rational criminal and the overall money laundering levels will, *ceteris paribus*, remain unchanged.

The analysis is subdivided into inherent and external factors. The inherent factors describe aspects which are related to the payment and asset tokens themselves because they are programmed in the underlying blockchain or are intrinsic to the distributed ledger technology. All external factors arise because of the application of the tokens to their environment. This differentiation is important regarding the fast pace of technological changes within the distributed ledger technology. Future changes in the underlying blockchain of the tokens mostly affects the inherent factors described above. Alterations in the environment, such as revised legislation or higher awareness of money laundering among the public primarily, change the factors within the external category.

The factors are further subdivided into aspects that are important for money laundering. Within each subdivision, a differentiated view with regard to the variables in the utility function outlined above is applied. Thus, a differentiated analysis is facilitated, as the variables have dissimilar effects on the overall expected utility. For instance, the probability of conviction for the money laundering act p , the probability to trace the money laundering act back to the predicate offense leading to a conviction of that offense z , as well as the certain transaction costs³³ tc , change depending on the money laundering technique. Within the inherent factors, the subdivisions are traceability, rapidity, internationality and portability, irrevocability of transactions, and value constraint.³⁴ The external factors include eight subdivisions, namely administration, authentication, acceptability, liquidity, volatility, risk, fees, and novelty.³⁵

A. Inherent Factors

1. Traceability

Traceability reduces the information asymmetry in the transaction history and movement of funds between the investigative authorities and the money launderer. According to the Financial Action Task Force (FATF), financial

³³ Technical and legal transaction costs, opportunity costs and even moral costs.

³⁴ See *infra* section III.A.

³⁵ See *infra* section III.B.

institutions should save all records on transactions.³⁶ This enables the prosecution of criminal activities through reconstruction of transactions. Records are thus an important way to provide a paper trail. However, the paper trail is interrupted as soon as the values are converted into cash or assets without records. The traceability aspect of the blockchain-based applications is therefore of significant interest in understanding their impact on money laundering.

Blockchain underlying payment and asset tokens provide a new dimension of (digital) paper trails. Every transaction needs to be recorded on the distributed ledger (blockchain) of every single miner to be valid. It cannot be deleted or altered at any point without turning invalid. It often contains the public keys of the involved parties.³⁷ Different entities³⁸ are programming software to provide an analysis of transactions throughout. Methods used include mapping and clustering transactions as well as combining information from datasets and from external sources.³⁹ This enables the discovery of behavioral patterns, individual network users and transactions stemming from illicit sources.⁴⁰

The traceability of the transactions is especially useful considering retrospectivity. Particularly in the early usages of payment and asset tokens for money laundering, criminals underestimated the traceability effects of the blockchain. Thus, many money launderers did not obfuscate their paper trails enough. As the blockchain records all transactions, agencies can prosecute those acts as soon as regulation or enforcement mechanisms allow them to do so. This is risky for money launderers who rely heavily on weak

³⁶ See Fin. Action Task Force [hereinafter “FATF”], International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 66 Recomm. 3 (2018).

³⁷ See Malte Möser, Rainer Böhme & Dominic Breuker, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, 2013 APWG eCRIME RESEARCHERS SUMMIT, SAN FRANCISCO, CA, 1-14 (2013); see Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 2013, 230 (2015) (explaining the technology and functionality of Bitcoin).

³⁸ For example Elliptic Ltd., a London-based Blockchain analysis provider; see Angela S. M. Irwin & Adam B. Turner, *Illicit Bitcoin Transactions: Challenges in getting to the who, what, when and where*, 21 J. MONEY LAUNDERING CONTROL 297, 307 (2018) (mapping an optimal solution to clustering and identifying suspicious behavior on the blockchain).

³⁹ See *id.*; see Yaya J. Fanusie & Tom Robinson, *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services* 3 (2018).

⁴⁰ See Angela S. M. Irwin & Caitlin Dawson, *Following the Cyber Money Trail: Global challenges When Investigating Ransomware Attacks and How Regulation Can Help*, 22 J. MONEY LAUNDERING CONTROL 122–23 (2019) (analyzing a framework to effectively regulate cryptocurrencies); Angela S. M. Irwin & George Milad, *The Use of Crypto-currencies in Funding Violent Jihad*, 19 J. MONEY LAUNDERING CONTROL 407, 419 (2016) (analyzing the connection between cryptocurrencies and terrorism); Irwin & Turner, *supra* note 38, at 301, 307.

legislation, as in future the agencies in those countries could enforce new anti-money laundering regulations or enforcement mechanisms that lead to discoveries of old offenses and prosecute the criminals subsequently. However, it is more difficult to convict criminals the more time passes, so the effects might be limited.

On the other hand, three different aspects of payment and asset tokens can scrutinize the perfect traceability of all transactions. Firstly, many payment and asset tokens focus on privacy. Simply programming a private blockchain instead of a public one already interrupts traceability. Privacy tokens contain further technical measures to ensure address, transaction and data privacy. The means encompass master nodes, blending techniques, cryptography, ring signatures,⁴¹ fraudulent transactions, zero-knowledge pools,⁴² coding rings, passing transactions through the Tor network,⁴³ and usage of stealth addresses⁴⁴ among many others. Secondly, mixers are in place to enhance more privacy even for tokens without privacy features. Mixers anonymize the relations between senders and recipients and thus break the paper trail.⁴⁵ However, research has found certain mixers to be ineffective.⁴⁶ Thirdly, illicit actors can obfuscate the paper trail by combining payment and asset tokens with cash and other assets without records. Thus, the money flows within the crypto-world are identifiable but the record is broken as soon as the values are converted into classical non-trackable means.

Nonetheless, the effects of privacy-enhancing mechanisms should not be overstated as the connection between traceability and acceptability, which will be discussed later, may yield a trade-off effect. The higher the privacy levels, the less the acceptability of the payment and asset tokens by licit actors. Entities are starting to apply the “know your transaction” approach, where only tokens with a clean transaction history are accepted.⁴⁷ Accepting suspicious tokens could lead to a prosecution for facilitating money

⁴¹ See Philippa Ryan et al., *Sydney Node Part 2 of 2*, 2 STAN. J. BLOCKCHAIN L. & POL’Y, Jan. 5, 2019, at 9, available at <https://stanford-jblp.pubpub.org/pub/sydney-2> (last visited Jul. 29, 2020) (exploring the regulatory challenges of distributed ledger technologies).

⁴² *Id.* at 6–7.

⁴³ See Irwin & Dawson, *supra* note 40, at 122–123, 128.

⁴⁴ For an overview of most privacy tokens see Kevin Liu, *2019 Privacy Token Review*, February 16th, 2019, hackernoon, available at <https://hackernoon.com/2019-privacy-token-review-c28b6ceef637> (last visited July 29, 2020).

⁴⁵ See MÖSER, BÖHME & BREUKER, *supra* note 37, at 2; see Irwin & Dawson, *supra* note 40; see Irwin & Milad, *supra* note 40, at 419.

⁴⁶ See e.g., MÖSER, BÖHME & BREUKER, *supra* note 37, at 9–11. With the mixer services new problems arise, for example the lacking trustworthiness of these services as well as challenges regarding timing, values and fees (see Böhme, *supra* note 37, at 221–222; see MÖSER, BÖHME & BREUKER, *supra* note 37, at 9–11.)

⁴⁷ See MÖSER, BÖHME & BREUKER, *supra* note 37, at 11–12.

laundering, particularly for centrally administered entities.⁴⁸ Therefore, there may be some level of trade-off between privacy (lack of traceability) and acceptability.

The expected utility of the money laundering is altered depending on the implementations of traceability of transactions. If no privacy-enhancing technologies are used, perfect traceability combined with algorithms to identify money laundering increases the probability of conviction for the money laundering act p .⁴⁹ Furthermore, principally for values obtained from cyber-crimes, the chances of conviction for the predicate crime z increase if the money laundering activity is detected and can be traced to the initial crime through the paper trail. Both effects decrease the expected utility of the money launderer.

If strong privacy-enhancing mechanisms are used, the probabilities of conviction for the money laundering as well as the predicate offense p and z are reduced.⁵⁰ However, as later analyzed under the aspect of acceptability, through suspicious privacy-enhancing mechanisms, the transaction costs tc and the probability of conviction for the money laundering act p are increased. Furthermore, progress in the analysis of transaction graphs shows that what was seen as a safe mean of obscuring the paper trail in the past might be ineffective in the future.⁵¹ Thus, future developments in law enforcement possibilities could make privacy efforts of payment and asset tokens futile and enable prosecution of money laundering subsequently.⁵²

The overall effect on the expected utility therefore largely depends on future improvement of technical enforcement. However, with such improvement to balance privacy and acceptability, privacy tokens may increase the expected utility, as breaking the paper trail is usually the major concern of money launderers.⁵³

2. Rapidity

Rapidity, the quality of moving with great speed, is another aspect of the blockchain-backed applications that requires examination particularly in how

⁴⁸ See *id.*

⁴⁹ See Christopher P. Buttigieg, Christos Efthymiopoulos, Abigail Attard & Samantha Cuyle, *Anti-money Laundering Regulation of Crypto Assets in Europe's Smallest Member State*, 13 L & FIN. MKTS REV. 211, 212-215 (2019) (explaining how money laundering with cryptocurrencies works and how it can be regulated).

⁵⁰ See Irwin & Turner, *supra* note 38, at 302.

⁵¹ See Micha Ober, Stefan Katzenbeisser & Kay Hamacher, *Structure and Anonymity of the Bitcoin Transaction Graph*, in 5 FUTURE INTERNET 237, 245 (2013).

⁵² See CHRISTIAN BREINIG, RAFAEL ACCORSI & GÜNTER MÜLLER, ECONOMIC ANALYSIS OF CRYPTOCURRENCY BACKED MONEY LAUNDERING 9 (2015).

⁵³ See IRENE KLIPPL, GELDWÄSCHEREI [MONEY LAUNDERING] 8-9 (1994).

it makes money laundering more attractive. A fast transfer of funds comprises opportunities of rapidity.⁵⁴ The faster funds or other assets can be moved and transformed, the more difficult it is for investigative authorities to track and confiscate them.⁵⁵ Furthermore, with higher speed, more transactions can be completed.⁵⁶ A fast pace of transaction settlement is obviously tremendously important for time-efficient money laundering. When compared to the traditional money laundering techniques—such as bulk cash smuggling, registering fake companies or opening different bank accounts in various nations—payment and asset tokens enable a gigantic increase in rapidity. Single transactions are still slower than traditional forms such as wire transfers, because wire transfers are mostly executed in real time. A transaction with payment or asset tokens, on the other hand, needs to be implemented through enough miners solving mathematical puzzles to confirm the addition to the blockchain for it to be executed.⁵⁷ The speed for this implementation can vary significantly between different tokens and the current demand for transactions, from a couple of hours to several days.⁵⁸ However, money laundering almost always requires new accounts to be established. With the technologies, the overall process, from opening an account or a wallet to executing transactions and abandoning the account, is enormously faster.⁵⁹

The expected utility of the money launderer is affected through the increased velocity. From the rapidity aspect, the blockchain-based applications change the expected utility through a reduction of the probabilities of conviction of the two crimes—money laundering and the predicate crime—and lower direct and opportunity costs. Investigative authorities have less time to identify, monitor and prosecute suspicious transactions. As more transactions can be completed within the same period of time, the audit trail and a real-time analysis become extremely difficult.⁶⁰ The limited time for prosecution and the higher barriers to successfully monitor suspicious transactions reduce the probabilities of conviction p and z .

Moreover, because less time is needed to execute the process of money

⁵⁴ See Louis de Koker, *Money Laundering Compliance – The Challenges*, in 68 FINANCIAL CRIMES: PSYCHOLOGICAL, TECHNOLOGICAL, AND ETHICAL ISSUES 329, 339 (Michel Dion et al. eds., 2016).

⁵⁵ See *id.* at 339.

⁵⁶ See BRENIG, ACCORSI & MÜLLER, *supra* note 52.

⁵⁷ See Steven Buchko, *How long do Bitcoin Transaction take?*, COINCENTRAL (Dec. 12, 2017), <https://coincentral.com/how-long-do-bitcoin-transfers-take/> (last visited Jul. 29, 2020).

⁵⁸ See *id.*

⁵⁹ See Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L. J. 441, 442–444 (2014) (identifying that the US regulatory Scheme currently does not encompass the entirety of Bitcoin use).

⁶⁰ See BRENIG, ACCORSI & MÜLLER, *supra* note 52; see Irwin & Milad, *supra* note 40, at 420.

laundering, the direct costs and the opportunity costs⁶¹ of the crime are reduced, which leads to a decrease in the aggregate transaction costs tc of the money launderer.⁶² Overall, the effect is an increase in the expected utility of the money launderer.

3. Internationality and Portability

The prosecution of criminal acts becomes more difficult if different countries, jurisdictions, law enforcement agencies, and tribunals are involved. Thus, money launderers may obscure funds by transferring them through different countries.⁶³ This requires prosecution and conviction on an international level instead of the usual territoriality principle.

Therefore, controls often apply at the borders of countries—whether through controls at tolls, which make bulk smuggling more difficult, or through the Know-Your-Customer (KYC) controls specially applied by banks in international money transfers.⁶⁴ Special transportation of bulky or valuable goods draws attention to the cause of transport. This makes it difficult to avoid getting caught.

Payment and asset tokens do not know the principle of borders.⁶⁵ The transactions are controlled the same way regardless of whether any or how many different jurisdictions are crossed, by miners contributing with their computing power from all around the world.

Payment tokens make portability easier in comparison to cash smuggling in high quantities.⁶⁶ The way transfers are made through this method is similar to wire transfers and other electronic payment systems.⁶⁷ Asset tokens, on the other hand, increase portability substantially, especially if the underlying goods are very bulky, need special transportation or are immovable.⁶⁸

Internationality and portability affect the expected utility of the money launderer. These two factors are particularly cumbersome because the responsible authority needs to be identified and the monitoring of suspicious

⁶¹ As more time for other occupations is available.

⁶² See BRENIG, ACCORSI & MÜLLER, *supra* note 52.

⁶³ See Klippl, *supra* note 53, at 6; see CHRISTOF MÜLLER, GELDWÄSCHEREI: MOTIVE – FORMEN – ABWEHR [MONEY LAUNDERING: MOTIVES – FORMS – DEFENSE] 98 (1992).

⁶⁴ See *e.g.* 31 U.S.C. § 5318(g); see also BRENIG, ACCORSI & MÜLLER, *supra* note 52.

⁶⁵ See Nlerum S. Okogbule, *Globalization and the Challenge of Regulating Transnational Financial Crimes*, in 68 FINANCIAL CRIMES: PSYCHOLOGICAL, TECHNOLOGICAL, AND ETHICAL ISSUES 295, 300 (Michel Dion et al. eds., 2016).

⁶⁶ See MÜLLER, *supra* note 63, at 115.

⁶⁷ See MÜLLER, *supra* note 63, at 116.

⁶⁸ For example, asset tokens with underlying antiquities, art or realty. Little difference to conventional transfers exists for shares; See FABIAN M. J. TEICHMANN, UMGEHUNGSMÖGLICHKEITEN DER GELDWÄSCHEREIPRÄVENTIONSMASSNAHMEN [OPPORTUNITIES OF CIRCUMVENTION OF PREVENTION MEASURES AGAINST MONEY LAUNDERING] 18 (2016).

transactions requires the cooperation among different nations in terms of legislation and execution.⁶⁹ From the internationality and portability aspect, the expected utility increases through lower probabilities of conviction of both crimes and lower transaction costs. Firstly, the probability of being convicted of money laundering p is lower with an instrument that facilitates international transfers and transportation more efficiently. It is also easier to transfer funds to a country with weak anti-money laundering regulations⁷⁰ while there is no risk of being discovered on the way or at a physical or virtual border control.⁷¹ Secondly, the connection to the prior crime is weakened because of the obfuscation of sources in international transfers, lowering the chances of being convicted of the predicate crime z . Thirdly, the direct costs are lower as the costs incurred to circumvent the difficulties of transnational transactions do not apply for payment and asset tokens. Asset tokens reduce the costs of difficult and expensive transportation of the underlying goods. Furthermore, payment and asset tokens can be accessed from anywhere around the world. Thus, the costs of acquiring access to the funds are smaller. These effects decrease the direct costs of the money laundering act⁷² and therefore, decrease the aggregate transaction costs tc . In total, the facilitated international transfer for payment and asset tokens, as well as the unproblematic transport with asset tokens, increase the expected utility derived from money laundering.

4. Irrevocability of transactions

Trust in the counterparty is essential in every business. Normally, unfulfilled obligations can be enforced through legal means. However, the state does not intervene when illicit liabilities are not met. Especially with money laundering, the criminal needs to rely on the cooperation of different people, over which she or he cannot always control. Hence, there is a risk that any party involved may revoke their payment obligations because of the lack of enforceability of their agreement due to the illegality of the money laundering process. Furthermore, if state authorities discover a payment of illicit fundaments, financial institutions might be able to repeal the payment, in which case the money launderer would lose her or his funds.

Such uncertainty for the money launderer may be reduced by one aspect of the blockchain-based applications, the irrevocability of transactions. With the blockchain technology, every block incorporates what is called the hash value of the previous blocks. Thus, if the information in a block is modified,

⁶⁹ See MÜLLER, *supra* note 63, at 98; see Irwin & Dawson, *supra* note 40, at 121, 127.

⁷⁰ So-called jurisdiction shopping; see Irwin & Turner, *supra* note 38, at 303.

⁷¹ See BRENIG, ACCORSI & MÜLLER, *supra* 52.

⁷² *Id.*

the hash value of all the following blocks is consequently modified. A new block is considered faulty and, as a result, is not incorporated in the blockchain. The simple consequence is that new information needs to be added as a new block and cannot be modified in the previous blocks. This results in complete irrevocability of transactions for payment and asset tokens, which means it is impossible to annul a transaction that authorities find to be linked to a crime.⁷³

Regarding the expected utility of the money launderer, this certainly reduces the transaction costs *tc*, as the counterparty risk diminishes through the irrevocability of payments.⁷⁴

However, this effect can be regarded as rather minor, as the counterparty can simply not undertake a payment instead of revoking it afterwards, which is unlikely anyway as funds are normally moved at a high pace and thus it is improbable that institutions can annul certain transactions even in the case of traditional money laundering instruments being used.

5. Value constraint

Value constraints usually describe the maximum amount that can be held in an account or transferred per payment or within a timeframe.⁷⁵ In this aspect, there is an effective value constraint, which involves the amount under the threshold where authorities are alerted of potential money laundering activities.⁷⁶ Depending on the amount of money that needs to be laundered *y*, certain traditional money laundering instruments are inefficient or useless. The value constraint influences the expected utility only when *y* is bigger than the value constraint imposed by the money laundering means.

With payment and asset tokens, the existence of value constraints varies. For example, most cryptocurrency-ATMs have certain constraints regarding the withdrawable amount.⁷⁷ Real and effective value constraints can be

⁷³ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 9.

⁷⁴ See *id.*

⁷⁵ See Jun Tang & Lishan Ai, *New Technologies and Money Laundering Vulnerabilities*, in 68 FINANCIAL CRIMES: PSYCHOLOGICAL, TECHNOLOGICAL, AND ETHICAL ISSUES 368 (Michel Dion et al. eds., 2016).

⁷⁶ Allowing for the so-called structuring.

⁷⁷ Buy, sell, or withdrawal limits on a fiat cash basis per day are usually set up to US\$5,000 or 5,000 Swiss Francs; see e.g. Bity, *Crypto ATMs*, available at <https://bity.com/products/crypto-atms/> (last visited July 29, 2020). These limits are also consistent with anti-money laundering regulation in the United States and other countries; see e.g. *supra* note 10. In Switzerland, individuals or companies converting virtual currencies into fiat money, et vice versa, might be covered by art. 3 para. 3 of the BUNDESGESETZ ÜBER DIE BEKÄMPFUNG DER GELDWÄSCHEREI UND DER TERRORISMUSFINANZIERUNG [GELDWÄSCHEREIGESETZ, GwG], LOI FÉDÉRALE CONCERNANT LA LUTTE CONTRE LE BLANCHIMENT

present for payment and asset token exchanges and wallets that underlie KYC regulation. Either only a certain amount can be held in an account⁷⁸ or the administrators need to inform the investigative authorities if payments into the account surpass a certain value. Real as well as effective value constraints are mostly absent for privacy tokens and similar phenomena, as an unlimited amount can be paid to and held in the accounts. For most payment and asset tokens, the transfers within the system function without any constraints.⁷⁹

Thus, the value constraints into and out of the payment and asset tokens might be similar to or less than those for traditional financial instruments. However, they are inexistent for movements of tokens within the system. Therefore, the constraints are less than those for traditional financial instruments with transaction limits.

Real value constraints increase the transaction costs tc and effective value constraints alternatively either increase the transaction costs tc or increase the probability to be convicted for the money laundering act p . The reasoning behind this logic is that if the value constraint is surpassed, p will increase. Otherwise, many different and expensive steps need to be taken⁸⁰ and therefore will increase the transaction costs. Real and effective value constraints for the amount held in an account vary depending on the product used. They are absent for transactions with tokens, thus decrease either the probability of conviction p or the transaction costs tc . For either of the two, the expected utility of the money launderer is increased.

B. External Factors

1. Administration

A great part of money laundering prevention nowadays is shifted from state authorities to the intermediaries of the services, who bear the responsibility of anti-money laundering (AML) compliance risk assessment. These administrators of financial services usually act as a central oversight body. In identifying their customers to comply with KYC duties, they are able to restrict suspicious actors from opening accounts and freeze accounts of existing customers. According to the FATF, states should obligate intermediaries to

D'ARGENT ET LE FINANCEMENT DU TERRORISME [LOI SUR LE BLANCHIMENT D'ARGENT, LBA], LEGGE FEDERALE RELATIVA ALLA LOTTA CONTRO IL RICICLAGGIO DI DENARO E IL FINANZIAMENTO DEL TERRORISMO [LEGGE SUL RICICLAGGIO DI DENARO, LRD], FEDERAL ACT ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING [ANTI-MONEY LAUNDERING ACT, AMLA], Oct. 10, 1997, SR 955.0. If covered by the AMLA, these individuals or enterprises have to comply to anti-money laundering duties.

⁷⁸ See Irwin & Milad, *supra* note 40, at 413.

⁷⁹ See Turner, *supra* note 21, at 1407, 1408.

⁸⁰ Such as structuring funds across various banks in different countries.

report suspicious customers or transactions and transmit corresponding comprehensive information to the financial authority unit for investigative purposes.⁸¹ If the institutions breach these duties, they have to bear high penalties.⁸² This system implements anti-money laundering efforts on the actors with the most profound knowledge of transactions and the simplest way of collecting information, thus facilitating the detection of money laundering.

For payment and asset tokens, the transaction operation on the distributed ledger needs to be differentiated from the initial purchase and final disposal.

For the transaction operation, the administration is not assigned to a single point of contact. Part of it is implemented directly through the distributed ledger technology underlying the payment or asset tokens and the other part of it is executed through the decentralized peer-to-peer network.⁸³ The peers in this network are usually distributed in different countries⁸⁴ and hard to identify. The founders and programmers of tokens may be unknown. Thus, a central intermediary that could be obliged to implement KYC duties on the users is absent. Furthermore, the processing of transactions and the respective control are out of reach of a single party. As often the payment and asset tokens can only be controlled by the people knowing the respective private key for their accounts, illegal funds can hardly be confiscated while in the network.⁸⁵

This has different impacts on the expected utility of the money launderer. The first impact is through the probability of getting caught of money laundering. As the state cannot identify a responsible administrator, it cannot impose any duties on them. Thus, law enforcement agencies need to conduct the whole investigation. Information easily obtained through KYC routines is burdensome to collect from an outside standpoint. Moreover, individuals posing a high risk for money laundering can transact, something normally already prevented by intermediaries through disabling the opening of an account.⁸⁶ In addition to that, no intermediary reports suspicious transactions or

⁸¹ See FATF, *supra* note 36, at 17 Recomm. 20.

⁸² Especially for the so-called false negatives, when a financial intermediary fails to report a transaction or customer that authorities discover to be suspicious ex-post, see ELÖD TAKÁTS, A THEORY OF “CRYING WOLF”: THE ECONOMICS OF MONEY LAUNDERING ENFORCEMENT 4–5 (2005); see BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 10.

⁸³ See BRENIG, ACCORSI & MÜLLER, *supra* note 52.

⁸⁴ See Lukas Müller, Milena Reutlinger & Philippe J. A. Kaiser, *Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union [Developments of the Regulation of Virtual Currencies in Switzerland and the European Union]*, 3 EUR. L. J. 80, 83 (2018) (explaining the regulation of cryptocurrencies in different legislations); see also Lukas Müller & Malik Ong, *Aktuelles zum Recht der Kryptowährungen [News About the Law of Crypto Currencies]*, 29 AKTUELLE JURISTISCHE PRAXIS 198, 205 (2020).

⁸⁵ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

⁸⁶ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

customers to the investigative authority.⁸⁷ The effect on the expected utility is a diminution of the probability of being caught for the money laundering act p .⁸⁸

The next impact is through the probability of tracing back to the predicate crime and the conviction of the crime. As suspicious actors cannot be identified from the first point of contact onwards, time is lost for the investigative authority to inspect the predicate crime. Additionally, freezing accounts is a useful method of increasing the time for investigations. As this is not possible within the distributed ledger technology, as soon as the suspicion of the authorities investigating a certain account arises, the funds will be moved by the money launderer. This decreased time of investigation leads to a decreased probability of being convicted of the money laundering crime p as well as the probability of tracing the funds back to the predicate crime and thus the probability of conviction for it z .

Another impact on the expected utility is through the transaction costs. As circumventing KYC controls can be very costly, the missing or weak KYC controls with regard to payment and asset tokens mean that the legal transaction costs—therefore, the direct costs arising from anti-money laundering regulation—are substantially lowered. This reduces the overall transaction costs of the money laundering act tc .

Lastly and interestingly, even the punishment for the money laundering act f_{ML} and the predicate crime f_c might be reduced. This is due to the fact that the illegal funds within the network can hardly be confiscated. Even in the case that the money launderer is convicted for the crime at a later point in time, the values could already be either untraceable or spent. If the criminal is punished with a jail sentence, this fact will not have any effect on the monetary value of the punishment. However, if the punishment consists partly of a fine, the real amount of the fine is lowered if it is impossible to locate the money that the convicted money launderer hides.

The initial purchase and final disposal—the interface between the real world with fiat money and the world on the distributed ledger with tokens—partly ameliorate these prospects. Most payment and asset tokens are purchased via exchanges, of which there are two types—decentralized and centralized.

Decentralized exchanges are based on distributed ledger technologies and work on an autonomous technical protocol,⁸⁹ either on-chain through smart

⁸⁷ See Fabian M. J. Teichmann, *Financing terrorism through cryptocurrencies – a danger for Europe?*, 21 J. MONEY LAUNDERING CONTROL 513, 515 (2018) (using a qualitative interview technique to evaluate the possible use of cryptocurrencies to finance terrorism).

⁸⁸ See BRENIG, ACCORSI & MÜLLER, *supra* note 52.

⁸⁹ See Harsh Patel, *A Pure Block Chain Based Decentralized Exchange*, CRYPTOLOGY EPRINT ARCHIVE 1 (2014), available at <https://eprint.iacr.org/2014/1005.pdf>.

contracts or on second-layer networks.⁹⁰ The automated process and the missing central authority provide them with the same characteristics as the payment and asset tokens described above. Luckily, these exchanges are in the minority,⁹¹ which means they provide low liquidity and users can be traced more easily. This is the case because low liquidity means fewer transactions, so contextual information, such as input and output values or the timing of the transaction, can be associated to a person more easily.⁹²

Centralized exchanges are controlled by a central entity and fundamentally ameliorate the negative effects of administration. Thus, many legislations impose anti-money laundering duties on them or qualify them directly as financial intermediaries, which means they need to comply with KYC duties, prohibit suspicious actors from opening accounts as well as exchanging tokens for fiat, report suspicious transactions and customers and transmit comprehensive information to the investigative authorities. Furthermore, custodial exchanges, which hold the private keys of their customers,⁹³ are able to freeze accounts in case of suspicion.

Therefore, if centralized exchanges are used, the probability of conviction for the money laundering activities as well as the predicate crime p and z along with the transaction costs tc stay relatively unaltered in comparison to traditional money laundering instruments. However, purchasing already existing wallets or using alternative forms of exchange would alter these effects. Moreover, there are still many countries which do not implement such regulation on the centralized exchanges as described above, and certain applications may be used to circumvent the applicable regulations.

Lastly, it must be conceded that all of the comparative advantages of payment and asset tokens with regard to administration are only immanent if the funds are introduced in a country with stringent anti-money laundering regulation. Where bank secrecy is still fundamental and anti-money laundering prosecution is weak, the expected utility for laundering money can already be significantly high. Thus, the differences between money laundering with payment and asset tokens to other instruments are unremarkable. Further, even with existing regulation, it is usually only applied to certain financial institutions. Experts share the opinion that most money launderers swerve to money laundering forms and institutes with fewer controls,⁹⁴ where the comparative advantages of payment and asset tokens are smaller. However, if

⁹⁰ See Bennett Garner, *What is a DEX? Decentralized Exchanges, Explained*, COINCENTRAL (Aug. 28, 2018), <https://coincentral.com/dex-decentralized-exchanges-explained/> (last visited Jul. 29, 2020).

⁹¹ Apparently, they conduct less than one percent of the trading volume. *See id.*

⁹² See MÖSER, BÖHME & BREUKER, *supra* note 37, at 3, who give a simple example on how contextual information can be used to track an individual.

⁹³ *See id.*

⁹⁴ *See* TEICHMANN, *supra* note 68, at 85.

unregulated, they represent a new method of money laundering with weak controls that pose different advantages which are analyzed in the following chapters.

2. Authentication

Money laundering instruments should reach one important goal: to increase the information asymmetry between the investigative authorities and the money launderer.⁹⁵ Anonymity is an aspect that creates an information gap regarding the identity of the money launderer, which is beneficial for a successful money laundering process.⁹⁶ However, the FATF establishes that anonymous and pseudonymous accounts should be prohibited.⁹⁷ Hence, through traditional instruments, identity cannot be hidden this way.

While the blockchain can save various information, it is usually coded to not save any personally identifiable information.⁹⁸ It frequently contains a public key, which is linked to the involved accounts.⁹⁹ In this case, the public key is a pseudonym¹⁰⁰ for the person owning the account.¹⁰¹ As long as the pseudonym cannot be connected to a person's identity, the level of privacy is close to anonymity.¹⁰² Within the pseudonymity, the level of authentication varies largely among different payment and asset tokens.

The authentication level is increased through various means. Tying on the programmers of the tokens, the simplest method requires the blockchain to save vast amounts of personally identifiable information.¹⁰³ Authentication is further increased if KYC applies to exchange services, wallet providers or at

⁹⁵ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 3.

⁹⁶ See KLIPPL, *supra* note 53, at 39; see MÜLLER, *supra* note 63, at 99, 122.

⁹⁷ See FATF, *supra* note 36, at 13 Recomm. 11.

⁹⁸ See Bryans, *supra* note 59, at 441, 469–70; see Irwin & Dawson, *supra* note 40, at 110, 122.

⁹⁹ See Ryan, *supra* note 41, at 1, 6. For Bitcoin, Ethereum and Bitcoin Cash they can, for example, be seen under <<https://www.blockchain.com/explorer>>.

¹⁰⁰ See Böhme, *supra* note 37, at 228–29; see Müller, Reutlinger & Kaiser, *supra* note 84, at 82–83. See ANDREAS PFITZMANN & MARIT HANSEN, A TERMINOLOGY FOR TALKING ABOUT PRIVACY BY DATA MINIMIZATION: ANONYMITY, UNLINKABILITY, UNDETECTABILITY, UNOBSERVABILITY, PSEUDONYMITY, AND IDENTITY MANAGEMENT 21 (2010) define a pseudonym as an identifier of a subject other than one of the subject's real names.

¹⁰¹ Habitually defined as the person knowing the corresponding public key, see MÖSER, BÖHME & BREUKER, *supra* note 37, at 1.

¹⁰² See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

¹⁰³ Regarding the ideological values of privacy of the crypto-community as well as the cost of recording vast amounts of information on the blockchain make this option rather unfeasible.

Initial Coin Offerings (ICOs), which is the case in many countries.¹⁰⁴ There, information about the user of the wallet is collected and thus the wallet can be linked to a specific person. The authentication level depends on the amount and quality of the information collected.¹⁰⁵ Asset tokens and particularly security tokens are typically issued following comprehensive KYC-duties. Tying on individual transactions, they establish links to the outside world.¹⁰⁶ Research has found different heuristics to link accounts to the real world.¹⁰⁷

On the other hand, a stronger focus on privacy is possible as well. Programmers have developed privacy tokens with an extreme focus on low to no authentication.¹⁰⁸ Furthermore, wallet providers and exchange services can choose countries with weak anti-money laundering regulations or weak law enforcement.¹⁰⁹ Users reduce identifiable information by creating one-use email accounts, working on a public internet point or with the “Tor” web browser¹¹⁰ to not disclose their personal IP-addresses¹¹¹ and any information from non-virtual sources. In addition to that, KYC requirements can be circumvented by using others’ or false identities. These can be stolen, forged or bought at the black market.¹¹² Circumventing KYC requirements is more difficult but not impossible for higher quality identification requirements.

To compare the authentication level of payment and asset tokens to that of regular money laundering instruments, two aspects need to be considered: first is whether more privacy is fundamental to the instrument itself and

¹⁰⁴ See Niels Vandezande, *Virtual Currencies under EU Anti-Money Laundering Law*, 33 COMPUTER L. & SECURITY REV. 341, 352 (2017) (discussing the initiative of the European Commission to amend the anti-money laundering rules).

¹⁰⁵ For example, consider the differences between requiring an email address, an ID or video-authentications.

¹⁰⁶ Examples are when shipping addresses, email addresses, credit card or bank account information are provided to the counterparty or the IP address is identifiable. See Müller, Reutlinger & Kaiser, *supra* note 84; see Bryans, *supra* note 59; see Böhme, *supra* note 37, at 221, 233; see DORIT RON & ADI SHAMIR, QUANTITATIVE ANALYSIS OF THE FULL BITCOIN TRANSACTION GRAPH 4–5 (2013).

¹⁰⁷ See e.g., Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System* 15–17 (2013).

¹⁰⁸ Privacy tokens are especially analyzed under traceability.

¹⁰⁹ Or even conceal their location to seemingly not belong to any jurisdiction at all (see FANUSIE & ROBINSON, *supra* note 39, at 11.). This does not hinder agencies in jurisdictions which convict all criminals that cause damage in their countries to prosecute them, but it poses difficulties regarding international competences, analyzed under internationality.

¹¹⁰ See Irwin & Dawson, *supra* note 40, at 124; *United States v. Galarza*, No. 18-mj-146 (RMM), 2019 WL 2028710, at 2 (D.D.C. May 8, 2019) (Howell, C.J.) (explaining Tor-based web browsers); “Tor” is available for free at <<https://www.torproject.org/>> and is an open-source software for enabling anonymous communication.

¹¹¹ See Irwin & Turner, *supra* note 38, at 297, 303.

¹¹² See Irwin & Dawson, *supra* note 40, at 125.

second is how difficult it is to circumvent the privacy restrictions.

The first question needs to be answered individually for every payment and asset token. People trying to obfuscate their illicit means choose the payment and asset tokens as well as wallets and exchange services that suit their privacy interests best.¹¹³ For instance, they may avoid tokens with high KYC-processes and those falling under stringent security law and in countries with high legal restrictions. There are tokens requiring considerably less information than most traditional financial instruments.¹¹⁴ Nonetheless, authorities can obtain additional information for tokens similarly to how they would for traditional financial instruments. For both means, how much information the money launderer discloses depends on the precautions she or he takes.

Regarding the possibilities to circumvent the identification requirements, the fact that most accounts are created online and not in person simplifies a possible falsification of personal documents.¹¹⁵ However, identification processes are improving and certain financial instruments already allow for online authentication. Thus, the falsification is quite similar to traditional falsification of identities.

The authentication process strongly influences the probability to be convicted for money laundering p . If anti-money laundering regulation is enforced through the exchange services and at ICOs, the authentication level will be similar to the one provided by other financial intermediaries.¹¹⁶

Through the optional privacy-enhancing mechanisms described above, privacy levels rise in comparison to traditional instruments.¹¹⁷ This has a tremendous effect on the probability of being convicted of money laundering. If the person laundering the funds cannot be associated at all with the transaction involving those funds and no extra information is provided, the prosecution is impossible and p is reduced.

In the case of politically exposed persons, who are usually required to provide additional information about their identity and transactions,¹¹⁸ the capacity to establish accounts pseudonymously lowers their probabilities of conviction p .

Furthermore, z also decreases using payment and asset tokens with a strong emphasis on privacy. If the money launderer is identified, the funds can be traced to the illicit actor of the predicate crime. Without identification, a link between the funds in the money laundering process and the predicate crime might appear, but no person can be convicted as she or he is not

¹¹³ See Irwin & Milad, *supra* note 40, at 407, 412.

¹¹⁴ For example Monero.

¹¹⁵ See De Koker, *supra* note 54, at 329, 339; see Tang & Ai, *supra* note 75, at 349, 350.

¹¹⁶ Apart from the possible differences arising from the online registration.

¹¹⁷ See Irwin & Dawson, *supra* note 40, at 122.

¹¹⁸ See FATF, *supra* note 36, at 14 Recomm. 12.

identifiable.

Finally, the higher privacy can be obtained cheaper in payment and asset tokens than through the falsification of documents with traditional money laundering instruments. Thus, the direct costs of the money laundering process and therefore the aggregate transaction costs tc are reduced.

The expected utility of the money launderer increases through the usage of payment and asset tokens if she or he uses certain privacy mechanisms and takes the needed precautions.¹¹⁹

3. Acceptability

Acceptability refers to the acceptance on the interfaces between the analyzed money-laundering product and the values exchanged for this product at the time of purchase and disposal. To be able to launder funds with a certain money laundering mean, the acquisition of the values must first be feasible. Liquidating the values may then be an intermediate step to further obfuscate the origin. Lastly, for the funds to be ready for use in the legal economy, the values need to be accepted by the people of the economic world.¹²⁰ This is the final state as well as the goal of money laundering.

Thus, the acceptability of payment and asset tokens in the market is crucial for their utility as money laundering instruments. The interface where conventional values are exchanged for the acquisition of payment and asset tokens allows for high acceptability. If the proceeds stem from a crime resulting in payment or asset tokens—for example, a transaction on a black market or a ransom paid in tokens—no transformation at all is undergone.¹²¹ In a case where the proceeds are in the form of a more traditional value, this value is usually easily exchanged for payment or asset tokens in token exchanges,¹²² using privacy exchanges or exchanges in unregulated economies. These low barriers to entry make the acceptability of fiat or similar values for tokens very high.¹²³

On the other end, exchanging tokens for traditional values also leads to some level of acceptability. Certain payment tokens can be used to purchase a multitude of goods and services.¹²⁴ Furthermore, exchanging payment tokens for fiat money (especially for cash) via cryptocurrency exchanges also

¹¹⁹ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8–9.

¹²⁰ See KLIPPL, *supra* note 53, at 2.

¹²¹ See Laura Shin, *How Widespread Is Money Laundering in Crypto?*, UNCHAINED (July 17, 2018), <https://unchainedpodcast.com/how-widespread-is-money-laundering-in-crypto-ep-72/> (last visited Jul. 29, 2020).

¹²² See Irwin & Milad, *supra* note 40, at 413.

¹²³ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

¹²⁴ Especially beneficial for money laundering purposes are the provided possibilities to acquire gift cards and luxury goods directly for the payment token.

supports the money laundering process.¹²⁵ Asset tokens are partly harder to exchange directly for cash, but depending on their liquidity they can be traded for payment tokens on an intra-crypto trade market and then be cashed out. These intra-crypto trade markets are growing, where different payment tokens and certain asset tokens can be exchanged for each other to further obfuscate the origins of the money.¹²⁶ But even though the market capitalization for payment and asset tokens is increasing,¹²⁷ in comparison to traditional financial means it is limited.¹²⁸ Therefore, these proceeds are more difficult to exchange for other financial means as well as goods and services in the traditional economy, and their acceptability is lower.¹²⁹ Even if their acceptability increases, it is not to be expected that it will reach the level of acceptability of traditional financial instruments.¹³⁰

However, what significantly reduces the acceptability of payment and asset tokens is their combination with suspicious activities. Examples of such activities include the purchase of tokens on an exchange or an ICO missing KYC controls, connections of the tokens to the black market or other traceable crimes,¹³¹ and payment tokens originating from a mixer as well as the tokens being privacy tokens or arising from an exchange with privacy tokens. As soon as centralized exchanges and legitimate counterparties become aware of such incidents, they are cautious to exchange the tokens. Next to the general skepticism behind payment and asset tokens, a further reason for this caution is that they might get punished for violating anti-money laundering duties, or that it will be impossible to exchange them at a later point with more skeptical parties recognizing the risks. Furthermore, financial institutions in general are hesitant to provide accounts for companies with high money laundering risk, as they fear sanctions for facilitating money laundering. The difficulties in opening bank accounts increase if companies operate with the crypto-world. For criminals that use their own exchanges or companies to wash their dirty payment or asset tokens, the possibilities to open a bank account are thus limited.

On the other hand, if the money laundering proceeds in the form of tokens are to be used in the dark market, the acceptability of payment tokens in particular is higher than regular fiat¹³² as a high proportion of the dark market

¹²⁵ See TEICHMANN, *supra* note 87.

¹²⁶ See Irwin & Milad, *supra* note 40, at 413.

¹²⁷ See Irwin & Dawson, *supra* note 40; Müller & Ong, *supra* note 84, at 201–202.

¹²⁸ See Müller & Ong, *supra* note 84, at 201–202.

¹²⁹ See Müller, Reutlinger & Kaiser, *supra* note 84; see BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

¹³⁰ BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

¹³¹ As they often can be traced on the public ledger, analyzed under traceability.

¹³² See TEICHMANN, *supra* note 87, at 516. This usage is particularly important if the

operates with payment tokens.¹³³

Entry into the crypto-world and the wide acceptance of fiat in exchange for tokens are comparable to regular money laundering means. Therefore, neither influences the expected utility of the money launderer.

Exit, however, has a tremendous influence, with significant differences depending on the further usage of the values. For an exit through legitimate counterparties, the acceptability depends on the apparent legitimacy of the funds.

For non-suspicious transactions with legitimate counterparties, the tokens can be exchanged for goods, services as well as fiat and financial products but suffer from low market capitalization. The funds might need to be exchanged into a certain form before being used further, raising costs through multiple transactions. If one wants to exchange the means directly and there only exist a few counterparties, the imperfect market leads to the money launderer having to pay excessively for the exchange. Both effects increase the direct costs and thus the transaction costs tc . Moreover, the opportunities to further obfuscate the means are reduced, leading possibly to a reduction in obfuscation of the money laundering and predicate crime. This increases the chances for authorities to raise suspicion and the probabilities of being convicted of the money laundering and predicate crime p and z increase.

For suspicious transactions with legitimate counterparties, their lacking acceptability leads to the need to transform the payment and asset tokens in such a way that they can no longer be connected to the crime, which can be very costly or even impossible, as analyzed before under traceability. Interestingly, completely missing acceptability leads to transaction costs tc being equal or even higher than the net proceeds laundered y . This is the case if the values are trapped in the crypto-world with no possibilities to exit it. In this case, the utility of the money launderer would be negative even in the best scenario. This same scenario could occur for criminals operating their own crypto exchanges or launching ICOs to launder their funds if they are incapable of opening a bank account.

In total, both scenarios of exiting the crypto-world through a transaction with legitimate counterparties decrease the expected utility of the money launderer because of limited acceptability.¹³⁴

Lastly, for the further use in the black market, the acceptability, especially for payment tokens, is very high. To acquire a product from the black market, it costs less to pay directly in payment tokens than first needing to exchange

proceeds are destined for further criminal actions. Examples hereof could be further cyber-crimes with the purchases of hacking tools, malware or fake accounts, or purchases for terrorist activities such as weapons or explosives; see Irwin & Dawson, *supra* note 40, at 110.

¹³³ See Irwin & Dawson, *supra* note 40, at 110.

¹³⁴ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 8.

traditional money laundering instruments into them. This reduces the direct costs and thus the transaction costs tc of the money laundering act. The source of the values is insignificant for illicit transactions in the dark market,¹³⁵ and privacy tokens are even preferred.

Thus, for transactions with illicit counterparties, the expected utility is increased through the high acceptability of tokens, especially of payment tokens.

4. Liquidity

Liquidity defines the level to which an asset can be traded quickly for its intrinsic value.¹³⁶ Often liquidity is described as the possibility to convert assets rapidly into cash, the most liquid asset.¹³⁷ High liquidity is required to layer illicit funds as fast as possible in the money laundering process without suffering excessive losses.¹³⁸ This renders the monitoring and prosecution more difficult for the investigative authorities. At the same time, it reduces costs otherwise arising through illiquidity.

Because of the smaller market capitalization, the liquidity of payment tokens is often lower than that of traditional financial instruments.¹³⁹ There are also possible complex legal regulations applied to the transfers of the payment and asset tokens. Among these legal complexities is the lack of legal certainty regarding the ownership of tokens on a blockchain in most jurisdictions. For example, it is not clear who is the owner of a Bitcoin¹⁴⁰ until there is a clear legal basis for the allocation and transfer of ownership.¹⁴¹ Therefore, countries like Switzerland and the Principality of Liechtenstein are

¹³⁵ The question poses itself if in these cases money laundering actually takes place.

¹³⁶ See James Chen, *Liquidity*, INVESTOPEDIA (May 1, 2019), <https://www.investopedia.com/terms/l/liquidity.asp> (last visited Jul. 29, 2020).

¹³⁷ See Aldo Soprano, *Liquidity Risk in the Financial Crisis* 5–6 (2015).

¹³⁸ See THIERRY FOUCAULT, MARCO PAGANO & AILSA ROELL, *MARKET LIQUIDITY: THEORY, EVIDENCE, AND POLICY* 6 (2013).

¹³⁹ See Simon Trimbom, Mingyang Li & Wolfgang Härdle, *Investing with Cryptocurrencies – A Liquidity constrained Investment Approach* 2–3, 9 (SFB 649, Working Paper No. 2017-014, 2017) (discussing the liquidity of cryptocurrencies as well as their effects when included in an investment portfolio). This is particularly true for rather unknown payment tokens, where it can be difficult to find buyers or sellers timely or the market might even freeze completely (see TEICHMANN, *supra* note 87.). For payment tokens such as Bitcoin and Ethereum, the liquidity is comparable to traditional financial instruments with high liquidity.

¹⁴⁰ See *supra* note 1.

¹⁴¹ See e.g. Chason *supra* note 4, at 135; See also Seth Litwack, *Bitcoin: Currency or Fool's Gold: A Comparative Analysis of the Legal Classification of Bitcoin*, 29 TEMP. INT'L & COMP. L.J. 309, 313 (2015); Federal Council of Switzerland, *Legal Basis for Distributed Ledger Technology and Blockchain in Switzerland*, Report, Dec. 14, 2018, 44–46, available at <https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilungen.msg-id-73398.html> (last visited Jul. 29, 2020).

introducing legal codes dealing with distributed ledger technology and the allocation or transfer of tokens in such a distributed ledger technology system.¹⁴² As long as there is no legal certainty about the allocation of property rights of tokens in a distributed ledger, this makes it more difficult to trade the assets and thereby launder them. However, the same problem makes it more difficult for authorities to prosecute money laundering activities if the authorities cannot tie a suspect to a money paper trail. Whether the first or last effect is predominant ultimately influences the liquidity and the outcome of how much money is laundered.

Apart from the possible legal uncertainty, the liquidity of asset tokens is higher because of the ease in how they are traded in comparison to the underlying values. Asset tokens represent an underlying asset such as a commodity or realty. These assets can be difficult to trade through traditional means as conducting a valuation is costly and prices are subject to the preferences of the buyers and sellers.

Through asset tokens, however, the value is split into unitized and standardized tokens, which are traded individually. Furthermore, asset tokens are bought online, which makes them more liquid than if a counterparty needs to be found at auctions through brokers or real estate agents. This favors trade and increases liquidity.¹⁴³

Thus, the liquidity of the instruments increases when asset tokens are used instead of similar money laundering instruments. If the money launderer wants to exploit the advantages of commodity-based money laundering, the liquidity level increases by using asset tokens. This lowers the chances of getting convicted of money laundering and the predicate offense p and z , as the transaction time is reduced and the transactions can be settled online, needing less alarming contact to the real world. Additionally, the transaction costs tc are lowered because of the cheaper transfer of the property through the asset tokens and the lower opportunity costs. In this case, the expected utility is increased.

For payment tokens and asset tokens representing very liquid values, such as traditional financial instruments, the liquidity might be reduced or stay constant relative to traditional money laundering means. This depends on the

¹⁴² The Swiss National Council has approved the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology on July 19, 2020. Now the Swiss Council of States has to approve it as well. All legislative materials are available at <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20190074> (last visited Jul. 29, 2020). A translation of the Blockchain Act of the Principality of Liechtenstein is available at <https://impuls-liechtenstein.li/en/blockchain-act-liechtenstein/> (last visited Jul. 29, 2020).

¹⁴³ These improvements only exist in comparison to illiquid assets. Examples are real estate or companies outside a stock exchange. It does not apply to assets with a liquid market, such as gold, diamonds, or shares of a listed company.

market size of the respective token. If it stays constant, no effect on the expected utility is caused. If the liquidity is lower, the reverse effects of the ones described above appear.¹⁴⁴

5. Volatility

Volatility and uncertainty about future prices increase the risk of investment.¹⁴⁵ It requires constant attention without a full guarantee of not losing the investment value in a sudden downturn. As for illicit assets, even while moving at a fast speed, a sudden decrease in price can result in substantial losses. Furthermore, if the proceeds need to be changed rapidly from one source to another, waiting for the price to recover is often not possible. To obfuscate the assets further, the convertibility of values at a fast pace is essential for money launderers.

Payment tokens have proven to be highly volatile investments. As they are not backed by fiat, there is no underlying asset and the market alone decides the value of payment tokens.¹⁴⁶ This volatility will likely continue in the future. For payment tokens with a fixed upper quantity cap,¹⁴⁷ a deflationary spiral might occur.¹⁴⁸ This could lead to the fluctuation diminishing and either resulting in a constantly increasing price, or the payment tokens being deemed valueless as nobody would be willing to trade them anymore knowing their value will increase.¹⁴⁹ Even under a “quantity cap” regime, there can be inflation in cryptocurrencies. Investors can invest in other type of cryptocurrencies or crypto asset classes. It is also possible to create “hard-fork” of a cryptocurrency and thereby copy it. With this “copy” of the cryptocurrency, it is possible to create more coins even if these coins are labelled differently than the original coin. Consequently, with such a “hard-fork” copy, it is

¹⁴⁴ Increase in p , z and tc and thus decrease in expected utility.

¹⁴⁵ See Giacomo Luciani, *Price and Revenue Volatility: What Policy Options and Role for the State?*, 17 GLOBAL GOVERNANCE 213, 214 (2011) (evaluating the role of the state for stabilizing price volatilities caused by exports).

¹⁴⁶ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 9; see Vandezande, *supra* note 104, at 342.

¹⁴⁷ See Irwin & Milad, *supra* note 40.

¹⁴⁸ See Vandezande, *supra* note 104, at 343; Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, at 177 (2012).

¹⁴⁹ Interestingly to note, research has provided insights that payment tokens are completely uncorrelated to established asset classes. Thus, in combination with many different asset classes, the diversification of the money laundering portfolio could even provide to be useful to minimize risks of volatility. However, the research was only conducted over 5 years, which does not provide enough evidence to further consider this development here. See ANKENBRAND, *supra* note 127, at 26–29.

possible to create more coins from an economic point of view.¹⁵⁰

Asset tokens, on the other hand, are backed with an asset such as real estate, art, valuable metals or shares of a company. Thus, the volatility of asset tokens is directly correlated with the normal market development of these products.¹⁵¹ However, as new technology is often used for speculation purposes at the beginning, the overpricing and bursting of blockchain bubbles have been and might further be the result of speculation.¹⁵² This has taken place before with some assets based on the distributed ledger technology—the ICO hype, for example.

The uncertainty driven by volatility of payment and asset tokens has an impact on the direct cost of the crime, through which the expected utility is changed. The extent to which volatility affects the expected utility varies depending on the level of risk preference of the criminal. The uncertainty is likely to cause higher losses for those who cannot wait for price recovery. And to speculate effectively in volatile markets is very time-consuming.

For payment tokens, the overall effect is an increase in the direct costs and thus in the transaction costs tc .¹⁵³ This lowers the expected utility of the money launderer. For asset tokens, the effect depends on the further development of these products in the market. If the prices behave similar to the price development of the underlying assets, no significant effect with regards to the transaction costs tc and the total change in expected utility will not be noticeable.

6. Risk

Risk is defined as the uncertainty about potential profits and losses combined with an incomplete control over the outcomes of decisions.¹⁵⁴ In distinction from volatility, the risk aspect in this case is evaluated as the likelihood of a loss of the assets themselves instead of a loss of the market price.¹⁵⁵ The overall risk of losing one's assets has a substantial impact on the expected utility of any investor as well as money launderers.¹⁵⁶

¹⁵⁰ See KATHARINA PISTOR, *THE CODE OF CAPITAL, HOW THE LAW CREATES WEALTH AND INEQUALITY*, 199–200 (2019).

¹⁵¹ See e.g. Thomas Ankenbrand & Denis Bieri, *Assessment of cryptocurrencies as an asset class by their characteristics*, 15 INV. MGMT. & FIN. INNOVATIONS, 177 (2018).

¹⁵² See Tushi Mathur, *The Theory Behind a Bubble Burst* (June 17, 2020), available at <https://ssrn.com/abstract=3629319> (last visited July 29, 2020), at 6.

¹⁵³ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 9.

¹⁵⁴ See ALLAN M. MALZ, *FINANCIAL RISK MANAGEMENT: MODELS, HISTORY, AND INSTITUTIONS* 34 (2011).

¹⁵⁵ Obviously, the two might interrelate.

¹⁵⁶ Risk preferences may differ. The assumption made is of the money launderer not

In our model, risks can be differentiated on the basis of origin, leading to four possible risk categories: bankruptcy, fraud, attack, and loss.

First, bankruptcy risk is the likelihood that an enterprise fails to meet its debt obligations. This risk always exists in enterprises. In the crypto world in particular, there are high chances of bankruptcy for startups after ICOs.¹⁵⁷ This increases the risk of investment in comparison to traditional instruments. As a result, asset tokens backed by underlying shares are very prone to bankruptcy risks. On the other hand, assets such as commodities and realty cannot become bankrupt and therefore carry no bankruptcy risk, which means asset tokens backed by this type of underlying assets also carry no bankruptcy risk.

Second, the risk of fraud refers to the likelihood that a fraud occurs, leading to a complete loss of value. Common in traditional money laundering instruments,¹⁵⁸ the risk also exists in payment and asset tokens. A fraud is committed when the provider issues asset tokens without any underlying value or payment tokens which cannot be used once the provider has cashed in. In addition, services such as wallet providers, exchange services and mixers can decide to close their business while keeping all payment or assets¹⁵⁹ stored in it at that moment.¹⁶⁰ This is called going offline and possible for custodial services, as they possess the private key on behalf of the beneficial owner.¹⁶¹ Because there is no way to recover from these frauds, the complete value is lost.¹⁶²

Third, there is a risk originating from outsider attacks.¹⁶³ There are different types of attacks, some affecting the money launderer and others not.¹⁶⁴ For example, a majority attack only concerns the money launderer if the transactions deleted involve her or him and thus her or his values are stolen,

wanting to lose all values, see Rafaella Barone & Donato Masciandaro, *Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques*, 47 EUR. J. L. & ECON. 1, 19 (2019) (discussing the differences between money laundering through usury and via ICO).

¹⁵⁷ See *id.* at 19. HUGO BENEDETTI & LEONARD KOSTOVETSKY, DIGITAL TULIPS? RETURNS TO INVESTORS IN INITIAL COIN OFFERINGS 5 (2018) state that the probability that a new company will survive 120 days after the ICO is 44.2%. The bankruptcy risk might also be especially because many start-up companies in the technology sector have an immature business plan which cannot survive on the market. Many of the companies were also fraudulent; see Paola Cerchiello, Paolo Tasca, & Anca Mirela Toma, *ICO success drivers: a textual and statistical analysis*, 21 J. ALT. INV. 13, 14 (2019).

¹⁵⁸ See TEICHMANN, *supra* note 68, at 34, 36–38, 43.

¹⁵⁹ See Irwin & Milad, *supra* note 40, at 413.

¹⁶⁰ See MÖSER, BÖHME & BREUKER, *supra* note 37, at 10.

¹⁶¹ See Garner, *supra* note 90.

¹⁶² See Vandezande, *supra* note 104, at 342.

¹⁶³ For an economic approach to why majority attacks are fatal to Bitcoin and similar cryptocurrencies with increasing growth, see ERIC BUDISH, THE ECONOMIC LIMITS OF BITCOIN AND THE BLOCKCHAIN, 5–6 (2018).

¹⁶⁴ See *id.*; see MÖSER, BÖHME & BREUKER, *supra* note 37, at 10.

or if the attacker blocks her or his transactions from being processed. Cryptocurrencies cannot be stolen by creating new transactions. Depending on the form of attack, the money launderer's tokens are stolen or they simply underlie a loss in worth because of volatility and decreasing market prices.

Fourth, the risk of loss of the underlying values arise as a result of a loss of the private key,¹⁶⁵ especially in the case of non-custodial assets. With traditional financial instruments, there usually remains a possibility to recover values if a password or key is lost. To mitigate this risk in payment and asset tokens, money launderers can secure their values through technical precautions.¹⁶⁶

Regarding the expected utility of the money launderer, the transaction costs tc are affected by these risks. The variable y encompassing the net proceeds laundered is not changed, as the initial amount the money launderer tries to launder is not altered. Instead, the risks affect the transaction costs tc , which are defined as the aggregate transaction costs of the money laundering process, as ultimately losing (a part of) the funds is simply a prohibitively high cost of laundering the values, which can in the end even surpass the initial amount of funds to be laundered y . If the company becomes bankrupt, the payment or asset tokens are stolen, or the private key is lost, the values are lost. As these risks are not certain, the loss through a bankruptcy or an attack should be weighted by the probability of this event to occur. This probability, while tends to be particularly high at an early development stage of the products, must be considered on a case-by-case basis.

7. Fees

Fees for the usage of money laundering are technical transaction costs and part of the direct, certain costs.¹⁶⁷ Logically, the cheaper the technical transaction costs of the money laundering technique, the better for the money launderer. They largely influence the expected utility, as an important approach to successfully obscure funds is the layering of as many transactions as possible. Fees are charged for the ownership of an account or wallet, transmitting transactions, exchanging values, and advisory services among other things. They can be flat or variable fees based on the specific underlying value.

Across traditional money laundering instruments, the fee rates vary tremendously. The same applies to the payment and asset tokens subset. Thus, an inter-category comparison is difficult to make. However, if the fees for the

¹⁶⁵ See Irwin & Milad, *supra* note 40, at 412–13.

¹⁶⁶ See *id.* at 413.

¹⁶⁷ See Masciandaro, *supra* note 26, at 227.

whole life cycle of a money laundering instrument¹⁶⁸ are considered, in most cases payment and asset tokens are the cheapest option.¹⁶⁹

The lower fees reduce the direct, certain costs and thus the aggregate transaction costs *tc*. This increases the expected utility of the money launderer.

8. Novelty

Money laundering is a constant sprint between criminals and authorities. Criminals are usually early adopters of new technology.¹⁷⁰ Regulators and investigative authorities, on the other hand, are often slow and need plenty of time to adapt to new developments, leaving opportunities for money launderers to be in action.

Currently, regulators in many countries are implementing better frameworks to criminalize token-based money laundering. But to render the frameworks effective, law enforcement needs improvement. It encompasses modern technologies and software, assistance from specialists such as cybercrime experts and data scientists, and standardized policies and procedures across legislations.¹⁷¹ Most countries lack institutions capable of prosecuting token-based money laundering.¹⁷² Thus, at the very moment, newer forms of payment and asset tokens pose an advantage for money launderers from the novelty aspect. However, this issue will diminish as soon as authorities gain experience in enforcing the rules against blockchain-based law violations or money laundering.¹⁷³ For example, in Switzerland, the Swiss Financial Markets Authority (FINMA), the public prosecutors of the 26 cantons, and the Office of the Attorney General of Switzerland have a mandate for enforcing

¹⁶⁸ From acquiring the money laundering instrument, to transferring the values and re-obtaining another instrument with the proceeds.

¹⁶⁹ See BRENIG, ACCORSI & MÜLLER, *supra* note 52, at 10–11. Possible exceptions could be cash in small amounts and over short distances, or wire transfers if compared to payment/asset tokens with high fees. Clearly more expensive is money laundering through front businesses, acquisition of real estate and most money transmitting services.

¹⁷⁰ See FANUSIE & ROBINSON, *supra* note 39, at 1.

¹⁷¹ See MÜLLER, *supra* note 63, at 156; TEICHMANN, *supra* note 87, at 516; Irwin & Turner, *supra* note 38, at 304.

¹⁷² See *e.g.* Order Granting Defendant's Motion to Dismiss the Information, *State v. Espinoza*, No. F14–2923, at 7 (Fla. Cir. Ct. dismissed July 22, 2016) where the court dismissed a money laundering charge; see Peck *supra* note, at 220–221 (arguing that the court in the *Espinoza* case wrongly dismissed the charges of money laundering because of flawed analyses of the relevant statutes and a wrong understanding of cryptocurrencies).

¹⁷³ See *e.g.* Steven David Brown, *Cryptocurrency and Criminality: The Bitcoin Opportunity*, 89 POLICE J. 327, at 333 (2016).

the law violations related to blockchain-based assets.¹⁷⁴

While the advantage of the novelty aspect is only true in the short term, the probability to be convicted for money laundering p as well as the probability to be linked back to the predicate crime z are reduced in comparison to well-known methods of money laundering. This increases the expected utility of the money launderer, an effect which will, however, be reduced as law enforcement mechanisms improve.¹⁷⁵

¹⁷⁴ See e.g. art. 22 to 28 of the SCHWEIZERISCHE STRAFPROZESSORDNUNG [StPO], CODE DE PROCÉDURE PÉNALE SUISSE [CPP], CODICE DI DIRITTO PROCESSUALE PENALE SVIZZERO [CPP] [SWISS CRIMINAL PROCEDURE CODE, CRIMPC] Oct. 5, 2007, SR 312.0, (Switz.); art. 1 and 3 of the BUNDESGESETZ ÜBER DIE EIDGENÖSSISCHE FINANZMARKTAUFSICHT [FINMAG], LOI SUR L'AUTORITÉ FÉDÉRALE DE SURVEILLANCE DES MARCHÉS FINANCIERS [LFINMA], LEGGE FEDERALE CONCERNENTE L'AUTORITÀ FEDERALE DI VIGILANZA SUI MERCATI FINANZIARI [LFINMA] [FEDERAL ACT ON THE SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY, FINANCIAL MARKET SUPERVISION ACT, FINMASA] Jun. 22, 2007, SR 956.1, (Switz.); see also e.g. Decision of the Swiss Federal Supreme Court, 6B_99/2019, 6B_148/2019, Apr. 18, 2019, Consideration 2.3.2 (Switz.); Decision of the Swiss Federal Administrative Court, B-5769/2017, Jan. 21, 2019 (Switz.) and Decision of the Swiss Federal Administrative Court, B-6413/2017, Jan. 21, 2019 (Switz.).

¹⁷⁵ As analyzed under traceability, it is furthermore dangerous to rely too heavily on the weaknesses of investigative authorities at the moment, as they might prosecute criminals subsequently.

C. Discussion

Table 1: Effects of using tokens for money laundering instead of traditional financial means

Aspect	Sub-Aspect	Effect of the Aspect	p	z	tc	f _{ML}	f _C	U
Inherent Factors								
Traceability	With no privacy enhancing mechanisms	↑	↑	↑	–	–	–	↓
	With privacy enhancing mechanisms	↓	↓	↓	↑	–	–	↑
Rapidity		↑	↓	↓	↓	–	–	↑
Internationality and portability		↑	↓	↓	↓	–	–	↑
Irrevocability of Transactions		↑	–	–	↓	–	–	↑
Value Constraint		↓	↓	–	↓	–	–	↑

External Factors								
Administration	Transaction operation	↓	↓	↓	↓	↓	↓	↑
	Initial purchase/ final disposal	–	–	–	–	–	–	–
Authentication	With AML duties	–	–	–	–	–	–	–
	With privacy-enhancing mechanisms	↓	↓	↓	↓	–	–	↑
Acceptability		↓	↑	↑	↑	–	–	↓
Liquidity	Of payment tokens and asset tokens with underlying liquid values	–	–	–	–	–	–	–
	Of asset tokens with underlying illiquid values	↑	↓	↓	↓	–	–	↑
Volatility	Of payment tokens	↑	–	–	↑	–	–	↓
	Of asset tokens	–	–	–	–	–	–	–
Risk		↑	–	–	↑	–	–	↓
Fees		↓	–	–	↓	–	–	↑
Novelty		↑	↓	↓	–	–	–	↑

Legend:

↑: Increase of the variable through laundering money with payment and asset token instead of traditional financial means

↓: Decrease of the variable through laundering money with payment and asset token instead of traditional financial means

–: No difference between laundering money with payment and asset token or with of traditional financial means

While the theoretical model and analysis capture the direction of the change in the expected utility caused by each analyzed aspect, they are not sufficient in determining the magnitude of each change to provide a quantifiable combined impact of all analyzed aspects on the expected utility. There may also be interrelations among the analyzed aspects that are not captured in the model. However, the theoretical framework may be used to identify which aspects individually provide positive incentives to use payment and asset tokens for money laundering instead of traditional financial instruments.

Regarding the probabilities of conviction of money laundering and the predicate crime p and z , we identify that value constraint (only for p), rapidity, internationality and portability as well as novelty reduce the chances of conviction in comparison to traditional financial instruments. Irrevocability of transactions, risk and fees have no impact in comparison to traditional means of money laundering. Only the acceptability of tokens increases the probabilities of conviction in every case. Regarding traceability, administration, authentication and liquidity, the outcomes vary, depending on the state of the token in the money laundering process for the administration aspect and on the token's characteristics for the other three aspects. For the latter, the money launderer can choose tokens and processes with the most favorable characteristics.¹⁷⁶ By doing so, only the acceptability aspect of tokens increases the probabilities of conviction. If the increase of p and z due to the lack of acceptability does not outweigh the effects of the decrease due to the eight aspects for p and seven aspects for z , the probabilities of conviction are reduced through the use of payment and asset tokens for money laundering.

The transaction costs are reduced as a result of rapidity, internationality and portability, irrevocability of transactions, value constraint and fees in comparison to traditional money laundering means. Only novelty produces no effect. Acceptability and risk increase transaction costs. For the rest of the aspects (apart from administration), the money launderer can choose which characteristics of tokens suit her or his interest best. Only for traceability the choice is limited, as choosing tokens without privacy-enhancing mechanisms leads to a higher chance of conviction. For this aspect, it is probably favorable to choose privacy-enhancing mechanisms even if they are more expensive. Thus, eight aspects reduce the transaction costs, while only two increase them.

Regarding the expected utility of the money launderer, it is increased through rapidity, internationality and portability, irrevocability of transactions, value constraint, fees and novelty. Only the acceptability and risk aspects reduce the expected utility in every case. Traceability, administration, authentication, liquidity and volatility all provide possibilities to select a

¹⁷⁶ For the example of traceability, choosing a token with privacy enhancing mechanisms.

method that either increases the expected utility or leaves it indistinguishable from that of traditional money laundering methods. Combining the effects of these aspects, it is likely that using payment and asset tokens with the right characteristics can increase the expected utility of the money launderer if the effects of acceptability and risk are not prominent enough to outweigh the others.

Changes or lack thereof in the expected utility resulted from an introduction of a money laundering instrument in comparison to others provide evidence for whether or not such an instrument would be a method of choice for money laundering. An increase in the expected utility as a consequence of the use of payment and asset tokens means that this method is more favorable compared to traditional methods. Thus, people that would already launder money with previous methods may switch to payment and asset token-based money laundering or at least include it in their portfolio. Some people whose expected utility of money laundering is not positive under the traditional methods might start laundering money with payment and asset tokens¹⁷⁷ if the increase is large enough to bring up the expected utility to a positive value.

IV. CONCLUSION

The purpose of this paper is to establish whether money launderers would choose payment and asset tokens as a money laundering method. To identify the preferences of money launderers, the paper employs the expected utility function of criminals from the economics of crime. This model provides a framework for comparing the expected utility of traditional money laundering instruments to the expected utility of payment and asset tokens as money laundering means.

Thirteen different aspects relevant to the money laundering processes within the categories of inherent and external factors are evaluated. Payment and asset tokens are analyzed in relation to those aspects to understand their impact on the expected utility through changes in the variables of the function in comparison to traditional money laundering methods. This allows the analysis to conclude whether each aspect increases or decreases the expected utility of the money launderer.

The results discussed above indicate that the majority of the aspects of payment and asset tokens possess various characteristics that provide more incentives for their usage as money laundering instruments in comparison to traditional means. If the impacts of the acceptability and risk of payment and asset tokens do not exceed the other eleven aspects, and the money launderer chooses the tokens with the most suitable characteristics for money

¹⁷⁷ We are aware of this provocative conclusion but would like to highlight that it is stringent regarding the model of the economics of crime.

laundering, and consequently the expected utility of the money launderer is increased with the use of payment and asset tokens. Thus, it can be concluded that a rational money launderer would choose payment and asset tokens for the money laundering process.

Research providing more insights, especially empirical ones, is necessary to confirm these theoretical conclusions. Further aspects and information on the interrelation among different aspects may be included for a robust analysis that could provide a full picture of the impact of on money laundering decision-making. With changes in technology or the environment of payment and asset tokens, a re-evaluation and new analysis of the aspects will be needed as changes in technology will impact the inherent factors and changes in the environment of tokens will affect the external factors.

At this stage of research, this paper has identified different aspects that theoretically facilitate or hinder money laundering using payment and asset tokens. It provides a first elaborated analysis, concluding that payment and asset tokens are suitable for money laundering.