Seminar Paper 'Blockchain Economics and Radical Markets'

# Cryptocurrencies, Rational Choice, and Organized Crime

Are cryptocurrencies a suitable monetary transfer system for criminal organizations?

*Sara Maria Engeler*
*University of Heidelberg*
*M. Sc. Economics*
*Summer Semester 2021*
*sara.engeler@stud.uni-heidelberg.de*

supervised by
Dr. Stefano Balietti

31.07.2021

# Contents

# List of Abbreviations

| | |
|---|---|
| AML | Anti-Money Laundering |
| CPU | Central Processing Unit |
| DCE | Detection Contolled Estimation |
| FATF | Financial Action Task Force on Money Laundering |
| FBI | Federal Bureau of Investigation |
| FinCEN | Financial Crimes Enforcement Network |
| FIU | Financial Intelligence Unit |
| GDP | Gross Domestic Product |
| ICO | Initial Coin Offerings |
| IOCTA | Internet Organized Crime Assessment |
| IP | Internet Protocol |
| KYC | Know-Your-Customer |
| NCA | Network Cluster Analysis |
| OECD | Organization for Economic Cooperation and Development |
| SLM | Smart Local Moving Algorithm |
| STR | Suspicious Transaction Records |
| TOR | 'The Onion Router' |
| U.S. | United States of America |
| UN | United Nations |

**Abstract**

Cryptocurrencies hold potential as a fast, secure, and decentralized monetary transfer system that is independent of governmental emission. They also received broader public attention due to price volatilities and misuse for illicit activities such as hacks, ransomware attacks, drug trafficking, and money laundering. Within a rational choice framework, this paper discusses if cryptocurrencies are a suitable money substitute for large international money laundering transfers of criminal organizations. Blockchain technology provides cryptocurrencies with inherent properties (e.g. *decentralization*, *pseudo-anonymity*, and a *lack of regulation*) that keep the probability of detection, the costs to offenders in terms of punishment, and the transaction costs small. Comparing these three components for traditional offshore money laundering and crypto-laundering, criminological, economic, and informatics literature proofs that '[...]*cash is still king*' (Weber and Kruisbergen, 2019, p. 352) due to availability of full transaction records, improved statistical detection methods, and advancing legislation for cryptocurrencies.

# 1 Introduction

Cryptocurrencies and especially Bitcoin attracted the public focus in the former years due to its application of blockchain technology as a private, virtual currency. They ensure a fast, privacy-protecting, and transparent opportunity to transfer large amounts of money across borders while being independent of any central institution. Cryptocurrencies also received attention because of price volatilities and 'bubble-like behavior' (Baur et al., 2018, p. 178), vast growth potential, and trading bans in several countries including China. As Baur et al. (2018) point out, bitcoin is mainly used as a 'speculative asset' rather than a decentralized peer-to-peer payment system. If cryptocurrencies such as Bitcoin are rarely used as a payment system by ordinary people then who is using them as money transfer schemes?

Bitcoin is still the cryptocurrency with the largest market share and was created in 2009 after the financial crisis as a result of a lack of trust in traditional financial institutions

(Barone and Masciandaro, 2019). The idea was to establish a private, virtual currency that does not rely on the issuing of a central bank as a third party but instead relies heavily on the integrity of its miners and thereby establishing trust (Nakamoto, 2008; Trautman, 2014). Cryptocurrencies establish transparency by publishing the complete transaction history while remaining the privacy of their users through encrypting the transaction information using cryptography. Bitcoins proof-of-work system is based on Central Processing Unit (CPU) power as the key to solving the cryptographic 'puzzles' to avoid past problems such as Internet Protocol (IP) address hoarding that leads to concentration of power (Nakamoto, 2008). While this application of blockchain technology holds potential as a alternative payment system it also got high energy consumption and technological prerequisites which limits availability to the broader public. At the same time, cryptocurrencies possess characteristics such as increased *anonymity* and *decentralization* which makes them prone to criminal activities (Smith and Kumar, 2018). Differing legislation on whether they need to be defined as assets, property, payment system (Kethineni and Cao, 2020), or income (Trautman, 2014) fails to cover them by existing legislation for illicit activities such as Anti-Money Laundering (AML) laws (Kethineni and Cao, 2020). In 2013, the Federal Bureau of Investigation (FBI) shuts down the most prominent darknet website 'Silk Road' at the time where users could buy illegal goods such as drugs, weapons, and child pornography (U.S. Department of Justice, 2020). 'Silk Road' as an early adopter relied on Bitcoin as a payment system, whereas the follow-up websites such as AlphaBay rather used cryptocurrencies like Monero with enhanced anonymity. Other illicit activities such as money laundering of criminal proceeds are moved onto the blockchain as well (Chainalysis, 2021). Ali et al. (2015) emphazise the decrease in risk of criminal transactions by moving them from the street to the internet, whereas Soudijn (2019) points out that traditional small-scope crimes are still carried out in cash, while larger illicit transactions for syndicated could be favorable on the blockchain.

The rational choice model of Becker (1968) models differing costs and benefits, as well as risk preferences of individuals and proofs that it can be profitable to undertake criminal rather than legal activities. The probability of detection is a key determinant for legisla-

tors to prevent individuals or organizations from engaging in criminal activities. While it is the goal of legislators to increase this probability then it must be of interest to criminals to keep it as small as possible. The model can in an aggregative sense be applied to criminal 'industries' (Becker, 1968, p. 170) and hence, to criminal organizations.

Cash has so far been the preferred payment medium for street crime, but cryptocurrencies are close substitutes and could replace cash (Hendrickson and Luther, 2021). Traditional international money laundering relies on costly financial intermediaries and founding offshore and letterbox companies (Ferwerda et al., 2020). By comparing the properties of traditional payment systems and cryptocurrencies, this paper is trying to answer the question: do cryptocurrencies reduce the probability of detection, the costs to offender, and the transaction costs such that it is rational for criminal organizations to use them as international money transfer systems?

In section 2, the rational choice model of Becker (1968) is introduced and applied to crypto-crime markets. The crime-favoring properties of cryptocurrencies are discussed in section 3. Section 4 contains a comparison of international money laundering as the base for organized crime and crypto-laundering as the emerging alternative. This comparison is based on the discussion of differing probabilities of detection, costs to offenders, and transaction costs within the rational choice model framework. The paper provides empirical approximations of these parameters using criminological, economic, and informatics literature as well as newspaper articles. Finally, section 5 concludes and proposes policy implications.

# 2 Crime and Punishment: A Rational Choice Model

Becker (1968) introduces in his paper 'Crime and Punishment' Becker (1968) a rational choice model for crime, in which he formalizes the damages and benefits to society of committing criminal activities and proposes corresponding levels of regulation. An individual committs an illegal activity whenever the expected utility of a criminal activity is larger than its legal activity counterpart ($EU(crime) > EU(legal\ activity)$). The inequality does not only depend on behavioral as well as differences in risk preferences but also on

differences in benefits and costs to that individual (Becker, 1968).

Becker (1968) establishes the damage side to society using the amount of harm $H_i = H_i(O_i)$ as a function of offenses $O_i$ with $i$ as a subscript for the criminal activity. $H_i' = \frac{dH_i}{dO_i} > 0$ as well as $H_i'' = \frac{d^2H_i}{dO_i^2} > 0$. This means that the amount of harm to society is increasing with each additional crime commited and the second order condition entails that with increasing levels of crime the harm worsens. The social gain to offender is given by $G_i = G_i(O_i)$ with $G_i' = \frac{dG_i}{dO_i} > 0$ and $G_i'' = \frac{d^2G_i}{dO_i^2} < 0$. Hence, the gain to offender from commiting a crime still increases with additional crimes but underproportionally to the harm that society faces. The net damages to society are therefore $D(O) = H(0) - G(O)$ which is an increasing function in the activity level and its second order property is assumed to be $D'' = H'' - G'' > 0$. Diminishing returns to illegal activities could pressure individuals to collaborate to achieve higher levels of $O$ and form a syndicate. Organized crime would in turn increase the harm to society disproportionally and hence require higher levels of regulation. Applying $O_i$ to crypto-crime markets, Chainalysis (2021) lists in the 'Crypto Crime Report' of 2021 money laundering, ransomware, darknet markets, scams, stolen funds, and terrorism financing as the main criminal activities (in decreasing order of criminal market share).

The cost of apprehension $A = g(m, r, c)$ on the regulative side includes $m$ for manpower, $r$ for materials, $c$ for capital and $g(.)$ as a function of the 'state of the art' (Becker, 1968) incorporating the development of forensic techniques like statistical learning methods. The costs of conviction $C(A) = C(pO)$ with $p$ being the probability of conviction that offenders face. The market offense function aggregates over all individuals that commit offenses is given by $O = O(p, f, u)$ with $f(.)$ as the costs to offender and $u$ being other influences on individuals favoring to commit a crime (Becker, 1968). Therefore, the level of crypto-crimes depends strongly on the probability of conviction and the costs to offender. This paper discusses and tries to quantify these two model components and transaction costs using estimates of economic, forensic, and informatics literature on money laundering and crypto-laundering. The optimal regulation depends on $f' \equiv bf$ with $b$ being a transformational coefficient relaying $f(.)$ to $f'(.)$ by considering the costs to the offender

in terms of their punishment. Becker (1968) suggests $b \cong 0$ for benign punishments such as fines and $b > 1$ for more severe punishments such as parole and imprisonment. If the harm to society is large while the costs to offender are essentially zero due to undetermined legislation, then the level of offenses increases. Since crypto-crime faced nearly no regulation in the early years (Trautman, 2014) this coefficient can be assumed to be close to zero starting in 2009 and slowly converging towards 1. In the former case, the elasticity of offenses is equal to zero while in the latter case, a lower elasticity results in more offenses both for an increase in $f(.)$ and $p$ (Becker, 1968). Collusion for individuals to a criminal 'syndicate' (Becker, 1968, p.207) in a diseconomy such as a criminal market to achieve monopoly pricing on the elastic part of the demand curve for criminal goods or services. Organized crime is also favorable for criminal markets with elastic marginal cost curves (Becker, 1968). The money transfer market for large international movements of criminal funds received a shock when cryptocurrencies emerged because the marginal costs are the costs per transfer and hence can be assumed as the transaction costs. If cryptocurrencies can lower the probability of conviction $p$, the costs to offender $f(.)$, and the marginal costs in terms of transaction costs, then rational criminals should switch to the substitute.

# 3 Cryptocurrencies as Money Transfer Systems

Cryptocurrencies rely on a decentralized ledger system where multiple 'nodes' validate a transaction instead of an individual or a central organization. Instead, cryptocurrencies are private, virtual currencies and payment schemes at the same time using blockchain technology. Each user of the blockchain got a virtual wallet that entails its 'address', a private and a public key, and a sequence of past transactions (Smith and Kumar, 2018). If a user makes a transaction, a network of 'miners' (the ledger) validates it by creating a hash that contains the encrypted information about the transaction. Several hashes form a block and several blocks add up to a blockchain. The miners creating the hashes get rewarded in units of the cryptocurrency. In the case of Bitcoin, the supply of coins is limited from above to avoid inflationary effects (Nakamoto, 2008).

## 3.1 Properties of Cryptocurrencies

Blockchain technology got inherent properties for cryptocurrencies which can keep the probability of conviction low, the costs to offender, and transactions costs low. Therefore, these properties make cryptocurrencies a profitable target for rational criminals.

Firstly, there is *decentralization* that goes hand in hand with a lack of governmental monitoring and regulation (Smith and Kumar, 2018). Each computer operated by a miner represents a node in the peer-to-peer network for validating a transaction that becomes part of the blockchain. Even though the full transaction history is visible for all users, the information is not transparent because the hashes within the blocks are encrypted. Once a transaction is validated by the miners, it becomes a lasting part of the blockchain and a second property arises, namely *transaction non-reversibility* (Nakamoto, 2008). It ensures the '*integrity of the blockchain*' (Smith and Kumar, 2018, p. 1549) by providing the full transaction history to all blockchain users and establishing trust. A downside to the otherwise transparent and democratic process is that this integrity relies on the miners that are assumed to be '*honest*' (Trautman, 2014, p. 107). A third and most important property is anonymity or more accurate *pseudo-anonymity*. Due to cryptography, the hashes encrypt the transaction information with a 26 to 35 character representation and thereby compressing the information (Foley et al., 2019). In combination with *transaction non-reversibility*, criminal organizations would be able to ensure the transfer of large sums of money across borders without information being directly linked to their identity and without costly financial intermediaries. Therefore, *cross-border transition* of cryptocurrencies are a fourth property that makes them comparable to SEPA or debit cards for fiat money. Only a small accounting fee rewards the miners as part of the transaction costs (Baur et al., 2018; Smith and Kumar, 2018).

The *decentralization* assures that no central authority monitors or regulates the transaction. That is favorable for illicit activities and laundering of criminal proceeds. As pointed out by Hendrickson and Luther (2021), with the increasing redundancy of cash transactions people switch to substitutes. If in the past large transactions for criminal activities were often handled in cash, then cryptocurrencies support anonymity and the techno-

logical framework to replace it as a money transfer system. Additionally, large amounts of cash are not easy to move with untraceable serial numbers, they leave a 'paper trail' (Hendrickson and Luther, 2021, p. 3) and need 'physically present' (Hendrickson and Luther, 2021, p. 2) parties. This has become increasingly difficult with the ban of the 500 Euro bill (Hendrickson and Luther, 2021). Cryptocurrencies avoid these problems. Both cryptocurrency and cash provide quasi-anonymous exchange (Hendrickson and Luther, 2021) but for a cash transfer, law enforcement would need to be present for detection. For cryptocurrencies, the transaction details are encrypted and only thoroughly traceable through IP-addresses but there exist a record of all past transactions (Hendrickson and Luther, 2021) as it exists for credit and debit cards. Additionally, criminals can use obfuscating technologies that cover their transaction path and provide enhanced anonymity (Böhme et al., 2015; Foley et al., 2019)).

## 3.2 Obfuscation of Transactions

There are several possibilities to enhance the most appealing property of the blockchain technology: *pseudo-anonymity*. Due to the availability of the blockchain transaction records the mailing address could potentially be tracked if the public key is known (Böhme et al., 2015). This was the case for the 'Silk Road' seizure in 2013 when the FBI tracked the personal mail address of 'Silk Road' founder Ross Ulbricht. The website used a mixer technology named 'The Onion Router' (TOR) but the FBI was able to track the IP address and arrested Ulbricht (Trautman, 2014). Cryptocurrencies such as Monero and ZCash incorporated anonymity concerns as part of their blockchain protocol (Foley et al., 2019). Monero applies a 'Ring Signature' which obscures public keys behind other public keys and is an important medium of exchange among criminals (Kethineni and Cao, 2020). After the shutdown of 'Silk Road' in 2013, AlphaBay became the largest darknet platform and adapted Monero in 2016 (Foley et al., 2019). ZCash on the other hand applies a zero-knowledge proof that detaches the sender's address from the transaction but still reveals the destination (Ben-Sasson et al., 2014). The decrease of illicit transactions in recent years on the Bitcoin blockchain is partly rooted in the adaption of criminals to

these 'shadow coins' (Foley et al., 2019).

*Mixers*, *tumbling*, or *chain hopping* are other possibilities of enhancing anonymity and thereby decreasing the probability of detection for law enforcement (Cyphertrace, 2018). *Mixers* are addresses where transactions are pooled such that payments from person to person would be more difficult to trace back (Böhme et al., 2015). The timing of transaction is a possibility to detect the use of *mixers* but some *mixers* already incorporated that and diffuse the time stamp (Böhme et al., 2015). *tumbling* and *wash trades* disguise the users holding values of cryptocurrencies by sending their funds to a 'tumbler' in exchange for a transaction fee. The 'tumbler' readdresses the funds to another address of the sender (Foley et al., 2019). *Wash trades* work similarly but without the middleman. Finally, *chain hopping* is another layering technique where users convert their holdings in one cryptocurrency to another and thereby obscuring their transaction record.

These privacy-enhancing techniques could also serve as the opposite intention as they can be used to trace obscured payments such as Foley et al. (2019) did. This could increase the transformative coefficient $b$, thereby the costs to offender, and the corresponding probability of conviction. Legal users could also use the techniques to avoid hacking risks but they got reduced incentives for their application.

# 4 Money and Crypto Laundering

Money laundering is the foundation for organized crime because the proceeds from illicit activities need integration into the real economy such that the funds appear to be legal (Ferwerda et al., 2020). There are three steps of embedding currencies as well as illegal funds which are placement, layering, and integration (Reuter and Truman, 2004; Chainalysis, 2019). Here is a simplified example of the embedding process: firstly, the funds are placed via a transaction into the blockchain; secondly, the funds are being moved to create long transactions chains to 'layer' the origins and make the funds appear legitimate; thirdly, the integration into the real world economy could take place via a cryptocurrency exchange for a real-world currency.

In a more advanced dynamic setting, Barone and Masciandaro (2019) compare in a theo-

retical framework the implementation of usury contracts and Initial Coin Offerings (ICO) offering of cryptocurrencies for money laundering. They assume that 'washed' illegal proceeds are partly consumed, while the remainders are reinvested in the illegal sector, and hence, large parts of the criminal funds need to be laundered. For illustration, laundered funds can be seen as the expense side of a criminal balance sheet with proceeds of gambling, fraud, weapon sales, drug, sex, and human trafficking on the income side.

## 4.1 Detecting Crypto Crimes and Crypto Laundering

Regulation and law enforcement struggle with the detection of cryptocurrency-related crimes due to the blockchain properties. But anomalies in the transaction chains leave behind traceable patterns. Ron and Shamir (2013) analyzed the transaction graph of Bitcoin and were able to perform a Union-find algorithm to assign users to one or more addresses. The algorithm clusters addresses to obtain user-level data through transitivity by tracing patterns across transactions. Based on this study, Foley et al. (2019) predict the number of Bitcoin users and the transaction volume of illicit transactions for the darknet market using a Network Cluster Analysis (NCA) and Detection Contolled Estimation (DCE) as classification tools. They identify two communities - 'illegal' and 'legal' users - using three approaches. Firstly, Foley et al. (2019) identify the seized users from records, secondly they detect other users depositing escrow funds in 'hot wallets' that were already involved in illegal activities, and thirdly, they search for posted bitcoin addresses in darknet forums. With NCA, Foley et al. (2019) classify the Bitcoin addresses by tracking the transactions between users and clustering them into the two communities. This is the first part of the Smart Local Moving Algorithm (SLM) algorithm. In an iterative procedure, they detect the users that transacted rarely with illegal users and those that were identified as belonging to the legal community whereas they transacted frequently with illegal users and reassign them (Foley et al., 2019). The DCE classification mechanism is similar but it sorts users into the two communities based on their characteristics (involvement in *tumbling* and *wash trades*). In a second step, Foley et al. (2019) resort falsely identified illegal and legal users into the other community and keep the detected illegal users as a

lower-bound estimation. The midpoint estimates between the two classification tools are that 26.17 percent of Bitcoin users are involved in illicit darknet activities that account for 46.17 percent of overall transactions. This is a far larger share than for the descriptive statistics which amounts to 5.86 percent of overall Bitcoin users after applying the Union-find algorithm. Firstly, these results prove potential illegal users could be detected when applying user identification techniques but that the network of illegal users is roughly even 22.4 percent larger than the users identified through seizures, 'hot wallets', and darknet websites. Secondly, the applied statistical learning techniques can track users despite and potentially because of obfuscating technologies.

Demant et al. (2018) apply predictive classification tools to explore the transformative potential of crypto markets for darknet drug trafficking. Their findings suggest that criminal organizations exploit this potential only for certain geographic areas and specific types of drugs (Demant et al., 2018). Besides these patterns, drug buyers rely mainly on domestic and intraregional drug routes (Demant et al., 2018) to reduce the probability of detection. This would increase larger transaction volumes for organized drug supply and therefore, other money transaction systems are preferred (Demant et al., 2018). Another possibility of their findings could be that larger transaction volumes for organized international transfers for geographically dispersed drugs are split into several smaller transfers to diffuse suspicion of miners. The resale could take place face-to-face from the dealer to the final consumer at a local level which is in line with findings from Europol (2018). The availability of the technological infrastructure and the know-how might be limited on the final consumer side which are two inhibiting factors for cryptocurrency adoption on street markets (Demant et al., 2018). Relatively small transfers can easily be conducted in cash in this setting. For larger transfers on the supply side for drug trafficking, cryptocurrencies might be of greater interest as well as the associated money laundering of these funds.

## 4.2 International Money Laundering

Ferwerda et al. (2020) divides between domestic and international money laundering. The former involves money being embedded into an existing business such as the original laundromats of Al Capone. The latter includes banks and other financial institutions as intermediaries and offshore companies to transfer the illicit funds internationally (Ferwerda et al., 2020). The advantage with crypto-laundering would be that no costly financial intermediaries would be involved which lowers the transaction costs only to the mining fees and hence should favor the use of cryptocurrency payment schemes for large syndicates. Ferwerda et al. (2020) determine with the help of a gravity model the international money-laundering flows depending on country characteristics (geographical and cultural proximity) as pull factors in a cost-benefit analysis for organized crime. They regress in the first step factors such as corruption, conflicts, language, or geographical distance to determine the shares of illicit flows between countries. In a second step, Ferwerda et al. (2020) simulate in multiple rounds the international flows based on these shares to determine which countries are likely to have attractive features for money laundering to another country. These features lower the costs to offenders and exploitation of these structures could help law enforcement to decrease it through international cooperation.
Estimating the actual extend of money laundering is challenging because its goal is to hide the criminal roots (Ferwerda et al., 2020). Therefore, statistical procedures have been developed to detect large money laundering cases such as in Badal-Valero et al. (2018). The authors examine police data in Spain for companies with suspicious operations and use Benford's distribution law for biased frequencies of small digits on the accounting records of these companies. They apply several statistical learning methods as classification tools to identify the criminal companies in their sample (Badal-Valero et al., 2018). According to international AML-standards, Suspicious Transaction Records (STR) need to be filed by financial intermediaries to the Financial Intelligence Unit of each state such as the Financial Action Task Force on Money Laundering (FATF) for the Organization for Economic Cooperation and Development (OECD) countries (Ferwerda et al., 2020). Similar to Badal-Valero et al. (2018), Ferwerda et al. (2020) used the same

type of data for the Netherlands and evaluate these as '[...]*the best available proxy for money laundering transactions*' (Ferwerda et al., 2020, p. 4). The algorithms would be able to identify up to 95 percent of the 26 cases where the companies were fraudulent with certainty (Badal-Valero et al., 2018). These account for 4 percent of overall companies with suspicious operation records. Both studies show that with working institutions and improving detection and statistical learning methods as well as a better understanding of profitable money laundering environments, traditional international money laundering becomes increasingly risky due to a higher probability of detection too.

Quantifying global money laundering and the associated cost components are complex challenges that involve a lot of uncertainty due to a lack of data. Walker and Unger (2009) estimated again with a gravity model the global money-laundering flows for the early 2000s. The United Nations (UN) estimates the share of flows around the globe within a range of 2 to 5 percent of the worldwide Gross Domestic Product (GDP) - which amounts to a volume of 1.6 to 4 trillion U.S. Dollar per year (Weeks-Brown, 2018; Lennon, 2021). Chainalysis (2021) quantifies the volume of overall illicit transactions in 2019 to 21 billion and in 2020 to only 10 billion U.S. Dollar. This accounts for a share of 1.3 and 0.625 percent for the lower bound worldwide illicit funds of 1.6 trillion and an even smaller share of 0.525 and 0.25 percent for the upper bound of 4 trillion U.S. Dollars for both years. Taking into account the predictive results of Foley et al. (2019) then the estimated volume of illegal activities amounts to roughly 430 billion U.S. Dollars which accounts for 26.875 and 10.75 percent of ill-gotten funds that need to be laundered. The latter back-of-the-envelope calculation is a quite sizeable effect and could indicate a trend for cryptocurrencies as payment schemes in organized crime. Nonetheless, the head of Europol, Rob Wainwright, expects around 3 to 4 percent of the continental illicit proceeds to be laundered through cryptocurrencies (Economist, 2018).

## 4.3 Probability of Conviction and Transaction Costs

The British news agency Thomson Reuters refers to Chainalysis and Cyphertrace as '[...] *both industry-leading blockchain forensics companies — hold some of the largest datasets*

*on crypto-crime and blockchain metadata in the world.*' (Marinnan, 2021). In the following, the data of these two companies is applied to assess the potential of cryptocurrencies for criminal market transactions.

The overall share of illicit transactions in cryptocurrencies for the year 2020 is set at 0.34 percent by Chainalysis (2021) and at 0.5 percent by Cyphertrace (2021). Both companies register a vast decrease in the recent years 2019 and 2020. In the early days of cryptocurrencies, Chainalysis (2019) indicates the illicit transaction share from 7 percent in 2012, Cyphertrace (2018) over a six-fold increase in 2015 and 2016, followed by a three-fold increase in 2017 and 2018 and a final drop in the trend for the last two years. This development is in line with Cyphertrace (2018) findings that criminals are early adopters of new technologies.

Blockchain technology relies on addresses rather than 'true' identities and therefore one individual can potentially be linked to multiple addresses. For simplicity, it is assumed that one 'user' is identical with one 'address' because Foley et al. (2019) use the Union-find algorithm by Ron and Shamir (2013) to merge transaction into user-level data. The illegal user identification of Foley et al. (2019) consists of three approaches as mentioned above. Only the first approach includes the actually seized users through tracing them back to their Bitcoin addresses for the years 2011 until 2017. Foley et al. (2019) identify a seized user sample of 1,016 illegal users through sources such as newspapers and U.S. court records *Seized users*. To determine the population of illegal users is a far more difficult empirical challenge because of the secret nature of criminal activities. Foley et al. (2019) determine the remainder of illegal users through identification of 'hot wallets' (*Black market users*) and darknet forums (*Forum users*) which adds up to an overall sample size of 6,223,359 observed illegal users which would determine the ratio of seized to actual illegal users to 0.016. Hence, the probability of detection $p$ for the predictive results would essentially be zero. After applying the NCA and the DCE, the midpoint estimate for illegal users amounts to 27,810,000 which gives a ratio of 0.004. Since the estimates of Foley et al. (2019) are predictive results, they should be carefully interpreted as a *lower bound* for $p$.

The transaction fee for mining where empirical estimates approximate it around 0.1 percent of transaction volume (Möser and Böhme, 2014). Additionally, when undertaking the currency exchange for converting cryptocurrencies a fee of around 0.2 to 2 percent is charged as a commission (Böhme et al., 2015). These costs could be higher for currency exchanges that take the risk of exchanging potentially illegal proceeds. Including the costs of obscuring for *mixers*, *tumblers* and *chain hopping* which vary from 1 to 3 percent of transaction value (Cyphertrace, 2018; Böhme et al., 2015). This gives a lower-bound percentage of 1.3 to an upper-bound 5.1 of the overall transaction volume as variable cost approximation for $f(.)$. A more distinguished cost discussion would include fixed costs for technological infrastructure (e.g. holding a wallet or provision of power for mining and mining farms). For international money laundering off the blockchain, the technological costs are ranged between 5 to 15 percent of the transaction volume (Reuter and Truman, 2004). This range mirrors a high uncertainty because there are no valid estimates of transaction costs. Comparably the range for cryptocurrency transfers is lower than for traditional international money laundering. Another interesting thought is the creation of mining pools for criminal organizations. Cryptocurrencies like Bitcoin apply a proof-of-work system where the highest CPU power solves the 'mining puzzle'. It could be cost-effective for large syndicates to develop mining pools to validate illegal transactions by minting those and hence saving parts of the transaction fees as well as lowering suspicion for large transaction volumes. Of course, this is just speculative and not a part of the discussion here.

Rational criminals should hence switch more frequently to cryptocurrency transfers for large bross-border transactions due to the comparably small transaction costs and the relatively low probability of detection. There are several possible explanations why this is still not fully the case even though cryptocurrencies were increasingly involved in illicit transactions until 2018. The first is that the technical infrastructure and availability of cryptocurrencies are still not ubiquitous (Demant et al., 2018). A second explanation is that traditional money laundering schemes such as cash are convenient and that technical innovation lags behind its adaptation within criminal markets (Soudijn, 2019). Addi-

tionally, the forensic and statistical learning techniques are enhanced (Ron and Shamir, 2013; Foley et al., 2019) such that the full availability of the transaction records could increase the probability of detection by reducing anonymity even in the presence of obfuscating technologies. Another important aspect of anonymity is the lack of cryptocurrency regulation which is discussed in the following section.

## 4.4 Regulative Uncertainties and Costs to Offender

It is complex to classify new technologies under existing regulations and laws. Felonies such as tax evasion as an example are a challenge in regulating cryptocurrencies because legislation differs between countries (Trautman, 2014). In Germany for example, holdings of cryptocurrencies are taxed as financial assets while mining cryptocurrencies is categorized as income generation (Trautman, 2014). A lot of times, informational asymmetries can be held accountable for that time lag in legislation and be taken advantage of from the criminal side - from cavalier white-collar crimes such as tax evasion to severe ones like drug trades and money laundering. Nonetheless, a decreasing trend for the use of cryptocurrencies in illicit activities is detected (Chainalysis, 2021; Cyphertrace, 2021) as regulation becomes more rigid in recent years. On the one hand, Böhme et al. (2015) state that law enforcement should become easier because blockchain technology stores by construction every transaction ever made. On the other hand, there are different obstacles such as obfuscating technologies or loopholes in the protocol to undermine effective regulation.

The definition and classification of cryptocurrencies play a central role in regulation because both imply either the coverage of international AML regulations or not. As stated in Trautman (2014), a legal definition for virtual currencies did not exist in the U.S. until 2013. Virtual currencies and therefore cryptocurrencies do not fulfill the basic monetary properties, hence have no legal tender status and are no target of monetary policies (Baur et al., 2018). Identifying them as assets, income, payment scheme, or currency can lead to coverage of AML-regulation or not. In the U.S., money transmitter laws require payment schemes to have a license and they need to register to the Financial Crimes Enforce-

ment Network (FinCEN)) to comply with money laundering statutes from 2014 onwards (Trautman, 2014). Around the same time, cybercrime statutes became increasingly strict as well. Mining creates taxable income and needs to comply with income tax laws, while trading cryptocurrencies classifies as capital asset holdings (Trautman, 2014). The main challenge to regulation is that state law has to be in line with federal law which in turn needs to comply with international cooperations (Trautman, 2014). In 2011, the law enforcement agency of the European Union, Europol, established the Internet Organized Crime Assessment (IOCTA) by the European Cybercrime Centre that captures crypto under cybercrimes. From the provider side, Know-Your-Customer (KYC) protocols are proposed for payment schemes such as cryptocurrencies to ensure user identification and limitation of criminal activities (Trautman, 2014; Böhme et al., 2015; Smith and Kumar, 2018). For the legislative side, AML-compliance and monitoring are identified as the key determinants to increase the probability of detection (Ali et al., 2015; Trautman, 2014). Shedding light on the regulative challenges of cryptocurrencies is important because they are decreasing the probability of conviction and the costs to offenders when being undetermined. An increase in manpower $m$ through e.g. Europol and the 'state of the art' function $f(.)$ through forensic machine learning techniques increases the costs of apprehension $A = pO$. The costs to offender increase with regulative coverage because criminals can only be held accountable for money laundering if they violated existing AML statutes. This leads to a shift in the transformative coefficient $b$ towards 1. The costs to offender are also increasing with an enhanced probability of conviction because the criminal can only be punished after conviction. 'Silk Road' founder Ross Ulbricht received a life sentence because of illegal weapon trade, drug, and human trafficking among others. His costs include his lifetime earnings in terms of opportunity costs and therefore his $b$ coefficient is equal to 1 even though his probability of conviction was low a priori.

# 5 Conclusion

Blockchain technology has been an important technological development in recent years with cryptocurrencies as an innovative application as a money transfer system. Their

inherent properties such as *decentralization*, *transaction non-reversibility*, and *pseudo-anonymity* make them suitable for large and discrete cross-border transactions and therefore of interest for criminal organizations who try to minimize risks and costs. Due to these properties and a lack of regulation in the early years of cryptocurrencies the probability of detection remained low. Also, the transaction costs are lower than for traditional international money laundering because no financial intermediaries and offshore companies need to be involved. Until today, no valid quantitative approximation of these costs exists because the secret nature of criminal activities leaves no incentive to do so. The costs to offender are potentially quite high depending on the timing and location of the sentence.

According to Soudijn '[...] *cash is still king*' (Weber and Kruisbergen, 2019, p. 352) for money laundering illicit funds of criminal organization (Europol, 2015; Soudijn, 2019). But according to the network analysis results of Foley et al. (2019), it is apparent that Bitcoin as the cryptocurrency with the largest market share already accounts for approximately one-quarter of the worldwide funds that need to be laundered due to their criminal background. And there are privacy coins like Monero or ZCash that ensure increased levels of privacy that have already replaced Bitcoin as their payment scheme due to a lower probability of detection.

Why is it then that organized crime did not switch their financial affairs fully to the blockchain? Firstly, even though transaction costs might be lower for cryptocurrencies than for cash or complex bank transfers through shell corporations, fixed costs for the technical infrastructure and the know-how are probably high. Secondly, the supplier side for illegal activities might have already switched to cryptocurrency transfers, whereas the resale of illicit goods and services still proceeds in cash. These effects are difficult to disentangle because estimates for criminal proceeds are usually provided as overall measures. Thirdly, if the costs of conviction are severe even though potentially not more severe than for 'off-the-chain' organized crime.

Several approaches in the economic and criminological literature attempted to estimate money laundering flows (Badal-Valero et al., 2018; Walker and Unger, 2009; Ferwerda

et al., 2020). More recently, these estimates exist for illicit transfers of cryptocurrencies as well (Foley et al., 2019). The provision of the full transaction history on the blockchain could still make it easier for statistical learning methods to detect criminal patterns despite obfuscating technologies (Foley et al., 2019) and could in turn bear potential for applications to traditional international money laundering. In combination with KYC-protocols for cryptocurrencies and AML-regulation coverage could close regulative gaps on the policy side to increase the probability of conviction.

# References


Ali, S. T., Clarke, D. and McCorry, P. (2015), 'Bitcoin: Perils of an Unregulated P2P Currency'.

**URL:** *https://doi.org/10.1007/978-3-319-26096-9-30*

Badal-Valero, E., Alvarez-Jareno, J. A. and Pavía, J. M. (2018), 'Combining Belford's Law and Machine Learning to Detect Money Laundering. An Actual Spanish Court Case.', *Forensic Science International* **282**, 24–34.

Barone, R. and Masciandaro, D. (2019), 'Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques', *European Journal of Law and Economics* **47**, 233–254.

Baur, D., Hong, K. and Lee, A. D. (2018), 'Bitcoin: Medium of Exchange or Speculative Asset?', *Journal of International Financial Markets, Institutions and Money* **54**, 177–189.

Becker, G. S. (1968), 'Crime and Punishment: An Economic Approach', *Journal of Political Economy* **76**(2), 169–217.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M. (2014), Zerocash: Decentralized Anonymous Payments from Bitcoin. Proceedings of the 2014 IEEE Symposium on Security and Privacy.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015), 'Bitcoin: Economics, Technology, and Governance', *The Journal of Economic Perspectives* **29**(2), 213–238.

Chainalysis (2019), 'Crypto Crime Report 2019'.

**URL:** *https://blog.chainalysis.com/2019-cryptocrime-review*

Chainalysis (2021), 'Crypto Crime Report 2021'.

**URL:** *https://go.chainalysis.com/2021-Crypto-Crime-Report.htm*

Cyphertrace (2018), 'Cryptocurrency Anti-Money Laundering Report 2018 Q2'.

**URL:** *https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report.htm*

Cyphertrace (2021), 'Cryptocurrency Anti-Money Laundering Report Febuary 2021'.

**URL:** *https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/*

Demant, J., Munksgaard, R., Décary-Hétu, D. and Aldridge, J. (2018), 'Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime', *International Criminal Justice Review* **28**(3), 255–274.

Economist, T. (2018), 'Crypto Money-Laundering. Will Crypto Help the Money Launderers of the Future?', *The Economist* .

**URL:** *https://www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering*

Europol (2015), 'Why is Cash Still King?'.

**URL:** *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*

Europol (2018), 'Internet Organized Crime Assessment (IOCTA) 2018'.

**URL:** *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*

Ferwerda, J., van Saase, A., Unger, B. and Getzner, M. (2020), 'Estimating Money Laundering Flows with a Gravity Model-Based Simulation', *Nature Scientific Reports* **10**(1), 1–11.

Foley, S., Karlsen, J. R. and Putnins, T. J. (2019), 'Sex, Drugs and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', *The Review of Financial Studies* **32**(5), 1798–1853.

Hendrickson, J. R. and Luther, W. J. (2021), 'Cash, Crime and Cryptocurrencies'.
**URL:** *https://doi.org/10.1016/j.qref.2021.01.004*

Kethineni, S. and Cao, Y. (2020), 'The Rise in Popularity of Cryptocurrency and Associated Criminal Activity', *International Criminal Justice Review* **30**(3), 325–344.

Lennon, H. (2021), 'The False Narrative Of Bitcoin's Role In Illicit Activity', *Forbes Magazine* .
**URL:** *https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=2401033432f*

Marinnan, P. (2021), 'Crypto-Crime and Caveats'.
**URL:** *https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/crypto-crime-caveats/*

Möser, M. and Böhme, R. (2014), Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. Proceedings of the 2nd Workshop on Bitcoin Research 2014.

Nakamoto, S. (2008), 'Bitcoin: A Peer-to-Peer Electronic Cash System'.
**URL:** *http:/bitcoin.org/bitcoin.pdf*

Reuter, P. and Truman, E. M. (2004), *Chasing Dirty Money: Progress on Anti-Money Laundering*, Institute for International Economics.

Ron, D. and Shamir, A. (2013), 'Quantitative Analysis of the Full Bitcoin Transaction Graph'.
**URL:** *http://arimoto.lolipop.jp/584.pdf*

Smith, C. and Kumar, A. (2018), 'Crypto-Currencies - an introduction into not-so-funny moneys', *Journal of Economic Surveys* **32**(5), 1531–1559.

Soudijn, M. R. J. (2019), 'Using Police Reports to Monitor Money Laundering Developments. Continuity and Change in 12 Years of Dutch Money Laundering Crime Pattern Analysis', *European Journal on Criminal Policy and Research* pp. 83–97.

Trautman, L. (2014), 'Virtual Currencies; Bitcoin and What Now After Liberty Reserve, Silk Road and MT GTOX ', *Richmond Journal of Law and Technology* **20**(4), 1–108.

U.S. Department of Justice (2020), 'Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency enforcement framework'.
**URL:** *https://www.justice.gov/cryptoreport*

Walker, J. and Unger, U. (2009), 'Measuring Global Money Laundering: 'the walker gravity model", *Review of Law and Economics* **5**, 821–853.

Weber, J. and Kruisbergen, E. W. (2019), 'Crimina Markets: The dark web, money laundering and counterstrategies', *Trends in Organized Crime* **22**, 346–356.

Weeks-Brown, R. (2018), 'Cleaning UP. Countries are Advancing Efforts to Stop Criminals from Laundering their Trillions', *IMF Finance and Development* **55**(4).