Spring 5-29-2015

Economic Analysis of Cryptocurrency Backed Money Laundering

Christian Brenig
University of Freiburg, christian.brenig@iig.uni-freiburg.de

Rafael Accorsi
University of Freiburg, rafael.accorsi@iig.uni-freiburg.de

Günter Müller
University of Freiburg, guenter.mueller@iig.uni-freiburg.de

Recommended Citation

Brenig, Christian; Accorsi, Rafael; and Müller, Günter, "Economic Analysis of Cryptocurrency Backed Money Laundering" (2015). *ECIS 2015 Completed Research Papers.* Paper 20.
ISBN 978-3-00-050284-2
http://aisel.aisnet.org/ecis2015_cr/20

ECONOMIC ANALYSIS OF CRYPTOCURRENCY BACKED MONEY LAUNDERING

Complete Research

Brenig, Christian, University of Freiburg, Freiburg, Germany, brenig@iig.uni-freiburg.de

Accorsi, Rafael, University of Freiburg, Freiburg, Germany, accorsi@iig.uni-freiburg.de

Müller, Günter, University of Freiburg, Freiburg, Germany, mueller@iig.uni-freiburg.de

Abstract

This paper reports on our research towards an economic analysis of money laundering schemes utilizing cryptocurrencies, which are convertible decentralized virtual currencies based on cryptographic operations. They gain ground as means to offer enterprises and its customers new payment methods, investing opportunities and some are even intended as substitutes for centrally controlled government-issued fiat currencies. Our starting point is the observation that their increasing popularity attracts the attention of practitioners and scholars, particularly because of raising anti-money laundering concerns. Consequently, work has already been conducted in this area, mainly focusing on implications on anti-money laundering efforts. However, we argue that the potential benefits for criminal individuals are an important, yet neglected factor in the dissemination of cryptocurrencies as money laundering instrument. Addressing this issue, the paper firstly presents the structure of the money laundering process and introduces prevailing anti money-laundering controls. This forms the basis for the subsequent analysis of contextual and transactional factors with respect to their influence on the incentives of criminals to utilize cryptocurrencies for money laundering. This aims at providing an answer to the open question, whether cryptocurrencies constitute a driver for money laundering.

Keywords: Cryptocurrencies, Bitcoin, Money Laundering, Anti-Money Laundering, Economic Incentives.

1 Introduction

Profits resulting from illegal activities committed by criminal networks such as drug or human trafficking, smuggling and illicit gambling pose a serious threat to economic systems as well as public safety. They provide e.g. the financial resources for criminals and terrorists to operate and expand their business, undermine the legitimate private sector and financial markets and diminish tax revenues (McDowell and Novis 2011). Money laundering (ML) describes the process by which the illegal sources of profits are disguised to obscure the link between the funds and the original criminal activity (IMF 2014). While the origin of the term lies in the US Mafia's activities to "launder" illegal money via cash-intensive washing salons (Schneider and Windischbauer 2008), nowadays it has to be understood in a much broader context. The emergence of complex financial instruments and global networking through technical developments and increased use of the Internet offers hitherto unknown pathways to conduct ML (ECB 2012). Therefore it is not surprising that around USD 1.6 trillion funds from illicit sources were laundered in 2009, which amounts up to 2,6% of the global GDP (UNODC 2011). These numbers emphasize the severity of the problem, but should be treated cautiously due to the absence of precise statistics.

The process of ML is characterized by asymmetric information between criminals and law enforcement. Criminal individuals thereby aim at obfuscating the origin of illicit funds through utilizing various channels, while coincidently institutions obliged to be compliant with anti-money laundering (AML) regulation employ controls to reduce these information asymmetries. The tendency of criminals to abuse information and communication technology and virtual environments has become problematic for law enforcement in this context (McCusker 2007; Stokes 2012). Some of today's commonly mentioned ML instruments presently are virtual currencies. While virtual currencies solely valued within a specific company or limited virtual community have long been existent in the form of bonus points or loyalty rewards, newer developments allow them to be converted into traditional currencies and transferred across national borders (Dilley et al. 2013). Since 2008, when a whitepaper introduced Bitcoin as the world's first practicable decentralized virtual currency (Nakamoto 2008), a plethora of similar currencies based on cryptographic techniques (e.g. Litecoin, Peercoin) appeared. Today, the Bitcoin economy alone is larger than the economies of some nations (Brito and Castillo 2013). And the market cap of the largest representatives amounts to roughly US$5 billion total value in circulation (CoinMarketCap). This is because cryptocurrencies offer many benefits for honest individuals. They, for example, provide low transaction costs, may ensure privacy in online transactions or even act as a substitute for bank accounts in countries with immature financial systems. These certainly existing advantages are out of the scope of this paper but should be kept in mind. On the other side, characteristics such as decentralization and perceived transaction anonymity attracted the interest of criminal structures in adopting cryptocurrencies as financial instrument to conduct illegal activities including ML. The FBI recognizes the increasing attractiveness for criminals who avoid traditional financial systems to conduct global monetary transfers and motivates it with "difficulties detecting suspicious activity, identifying users, and obtaining transaction" (FBI 2012).

The suitability of cryptocurrencies for ML is eagerly discussed in related disciplines such as computer science (e.g. Meiklejohn et al. 2013), legal studies (e.g. Stockes 2012) and economics (e.g. Dostov and Shust 2014) lately. Although these works provide insights into, e.g., regulatory aspects, their embeddedness in the financial system and methods to derive implications from publicly available transaction data, the majority of studies focus on the challenges cryptocurrencies pose on AML efforts (Brezo and Bringa 2012). However, existing literature lacks in-depth analysis of the particular factors which provide the economic incentives for money launderers. Instead, it implicitly assumes that cryptocurrencies are attractive for money launderers because of their technical design features and the few publicly known money laundering incidents. But only if cryptocurrencies are perceived economically beneficial from a criminals' point of view, they may be qualified as a promising instrument to support the process of ML and consequently pose a real threat to AML efforts. Factors that have an effect on the execution of the ML process, and thereby influence the economic incentives of criminals, need to be identified and analyzed.

Contribution: This paper develops a conceptualization via which channels economic incentives are provided to use a monetary instrument for ML. In particular, it is focused on the ML process and AML controls. In light of their growing spread, cryptocurrencies are examined as a concrete example. Therefore, an analysis considering both contextual and transactional factors influencing the incentives of criminals is shown. It addresses the question whether, and if so why, cryptocurrencies represent a risk of being misused for ML. This aims at supporting academics and decision makers in understanding the underlying risks of cryptocurrencies for AML efforts, in order to derive suitable countermeasures. Our overarching objective, however, is to provide an incentive-oriented approach for the systematic evaluation and design of virtual currencies. The development of appropriate frameworks needs to integrate both the perspective of honest as well as criminal individuals.

The remainder of the paper is structured as follows: In Chapter 2, we give an overview of the ML process, categorize AML controls and elaborate through which channels economic incentives are provided. Based on this, Chapter 3 present our conceptualization for the analysis of ML related factors. We make a distinction between direct and indirect effects that the factors have on the execution of the

ML process. In Chapter 4, after an introduction to the design philosophy of cryptocurrencies, we identify and analyze contextual and transactional factors that provide economic incentives for criminals to utilize cryptocurrencies for ML compared to traditional financial instruments and services. We finish this paper with an overview over related challenges in Chapter 5 and our conclusion and outlook in Chapter 6.

2 Setting the Context: ML Process & AML Controls

The success of ML is crucial dependent on the existence of information asymmetries between money launderers and investigative authorities. ML activities share two key-characteristics: illegality and concealment (Masciandaro 1999). In order to reuse illegally acquired funds for legal activities without causing suspicion, they need to appear generated from legitimate sources. Therefore, money launderers' aim is to obfuscate the stream of cash in a way that prevents any connection to the underlying criminal activity (UNODC 2005). In economic terms, the transfer of potential purchasing power into actual purchasing power, to minimize incrimination risks (Masciandaro 1998). The process of establishing these information asymmetries is called "ML process" and is carried out by utilizing a "ML Instrument". Policies and procedures employed by investigative authorities to prevent, detect and investigate ML are called "AML controls". They aim at decreasing the information asymmetries between money launderers and investigative authorities. The more effective AML controls are, the more difficult it is for criminals to successfully execute the ML process and benefit from their offences due to an increasing risk of prosecution and conviction (Becker 1968). The interrelations between the actors and important elements in the context of ML are summarized in Figure 1.

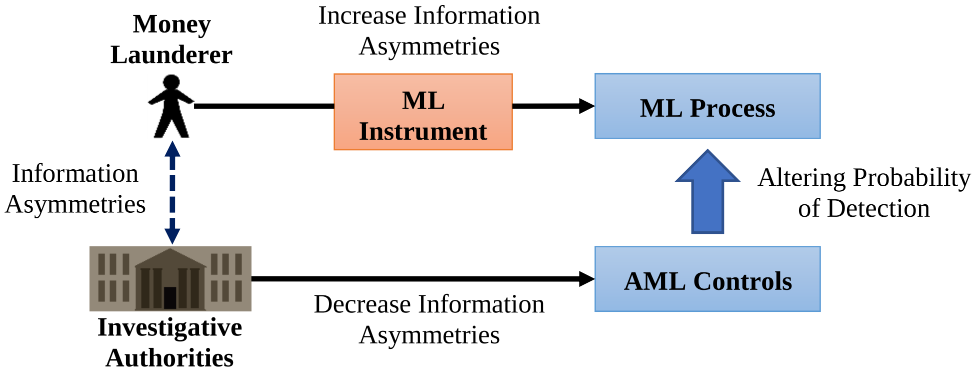
Money Launderer
Increase Information Asymmetries
ML Instrument
ML Process
Information Asymmetries
Altering Probability of Detection
AML Controls
Decrease Information Asymmetries
Investigative Authorities

Figure 1. Context of Money Laundering

Consequently, the economic incentives of a money launderer to utilize a ML instrument are conditional on: How well it is suited to establish a high degree of information asymmetry between the money launderer and investigative authorities, at the lowest possible expense of financial resources. This depends on the effects it has on the execution of the ML process and the available AML controls. For that reason, the general structure of the ML process and prevailing AML controls are introduced and their influence on the incentives is examined in the following. The results are used as input for the conceptualization of the subsequent analysis of cryptocurrency backed ML.

2.1 Money Laundering Process

There will always be a criminal agent or a criminal organization having committed a predicate offence (i.e. a transaction which generated and accumulated illicit funds) such as drug trafficking, kidnapping, arms smuggling, extortion or financial crime occurred before the process execution (UNODC 1988). In the majority of all illegal transactions cash is exchanged for the payment of illegal goods and services. This can be attributed to the properties of cash, which allow for anonymous and irrevocable transactions (with respect to third parties not involved in the transaction) without leaving eminent traces for investigative authorities (Schneider and Windischbauer 2008; Vilasenor et al. 2011). As depicted in Figure 2, the process of ML itself consists of three stages: placement, layering and integration (Reuter and Truman 2004).

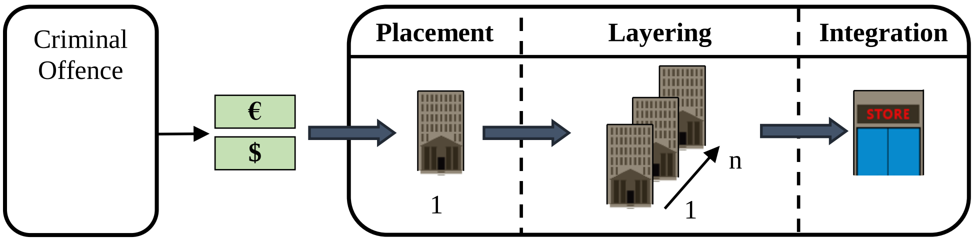

Figure 2. Money Laundering Process

In the initial *placement stage* illicitly obtained funds are introduced into the financial system in a form or a place that is less suspicious to public authorities and convenient to make them more liquid.

In the subsequent *layering stage* the funds usually get passed through many institutions and jurisdictions using multiple complex financial transactions in order to obfuscate their illegal origin. They are channeled through the purchase and sale of investment instruments such as bonds, stocks and cheques or they are simply transferred between a series of accounts at various banks, particularly to those jurisdictions with lax AML regimes (Bauer and Ulmann 2001).

Finally, the *integration stage* integrates ill-gotten proceeds into the legal economy, where they appear to be legitimate, through financial or commercial operations.

From an economic perspective, the ML process consists of a series of transactions between individuals, third parties, accounts and jurisdictions. Positive incentives for criminals to utilize an instrument for ML are provided, when it is relatively advantageous compared to alternatives that allow for the transfer of funds (Mantel and McHugh 2001).

2.2 Anti-Money Laundering Controls

The economic incentives of money launderers for utilizing a ML instrument are also conditional on the available measures and procedures to detect suspicious transactions and individuals. Depending on the effectiveness of the implemented controls, the probability of being detected while laundering money is altered. This risk imposes costs on criminals and therefore negatively influences their economic incentives for utilizing a ML instrument (Masciandaro 1998; Geiger and Wuensch 2007; Ferwerda 2009). Rational criminals generally have three alternatives to mitigate the risk. They can implement more sophisticated laundering schemes (e.g. involving additional jurisdictions, transactions, parties), which generally imply higher costs while reducing risk. If available, money launderers also have the alternative to utilize a different, less risky instrument. The third option, which constitutes the ultimate objective of AML controls, is that criminals refrain from laundering money. That is the case when the costs for laundering money undetected are greater than its valuation (Masciandaro 1999). The conclusion is that the effectiveness of the implemented control mechanisms is negatively correlated with the attractiveness of an instrument for money launderers. Consequently, if no controls are implemented or it is possible to circumvent them with little effort, positive economic incentives to utilize an instrument for ML are provided.

In order to enable the analysis of how the factors of cryptocurrencies influence the effectiveness of controls (and thus the economic incentives of money launderers), an overview of prevailing AML controls is given. The main driver behind AML investment decisions are regulatory requirements which oblige financial institutions and certain non-financial businesses to comply with AML legislation

(KMPG 2014). In order to be compliant, they have to implement preventive measures to identify and assess customers or transactions and report suspicious activities to law enforcement, which is considered "to be a crucial tool in the investigation and prosecution of money laundering offences" (Bauer and Ullmann 2001). The global standard are the recommendations published by the Financial Action Task Force on Money Laundering (FATF). As international standard-setting body, the FATF established AML measures that should be adopted by financial institutions and designated non-financial businesses (FATF 2012). A central element of the overall framework is the shift from a rule-based towards a risk-based approach countering ML. Risk management becomes increasingly important because solely relying on rules (i.e. if characteristics of a transaction meet conditions specified in the rule, then a specified action is taken) produces insufficient reports. In the European Union financial institutions are obliged to report cash transactions in excess of EUR 15.000 (EU 2005). Criminals are also aware of such thresholds and simply execute transactions just below those boundaries ("structuring") (Reuter and Truman 2004; Takats 2011). A risk-based approach is, in contrast, flexible and a reasonable designed risk management process enables to focus on customers and transactions that pose the highest risk for ML. Appropriate controls should be selected on basis of the risk assessment so that resources are allocated in the most efficient ways.

Controls are based on the so called Know-Your-Customer (KYC) principle and can be categorized whether they are performed a priori, during or a posteriori the business relationship of an individual with a financial institution or a non-financial business. In general, every AML strategy consists of multiple building blocks: a priori collection and analysis of personal data to derive implications regarding the expected risk of ML imposed by potential customers, collection and analysis of actual transaction data to detect suspicious activities and enrichment of customer profiles during the business relationship. This is complemented by a posteriori record keeping to provide audit trails for investigative purposes (see Table 1). It is important to determine how the implementation and application of prevailing controls is influenced by the factors of cryptocurrencies to identify the ML risks imposed.

Timepoint	Controls
A Priori	**Customer Identification Procedures** • Identify and verify the identity of each customer/beneficial owner • Develop customer profiles containing personal data • Exclude certain potential customers
During	**Ongoing Account & Transaction Monitoring** • Understanding of regular and reasonable activities • Detection of unusual activity patterns • Updating of customer profiles
A Posteriori	**Record Keeping** • Provide audit trails

Table 1. Overview of Anti-Money Laundering Controls

3 Conceptualization: Provision of Incentives

Figure 3 illustrates the conceptualization for our analysis, which refers to our discussion of the ML process and AML controls in the previous sections. It is based on the economic incentives of criminals to utilize a ML instrument. We identify contextual and transactional factors that have effects on the execution of the ML process. We draw a distinction between direct and indirect effects. The direct impact of contextual and transactional factors on the conducting of transactions is defined as direct effects. They influence the efficiency and effectiveness of the ML process by making the process execution, for example, more cost-efficient, time-efficient or the system more robust against disturbances.

Given that the ML process basically consists of a series of transactions, they affect honest individuals in conducting legal transactions as well as money launderers. Furthermore, money launderers also have to take indirect effects into account. They have an indirect impact on the execution of the ML process. Indirect effects influence the effectiveness of AML controls, which in turn alter the probability of being caught while laundering money. The direct and indirect effects of contextual and transactional factors on the execution of the ML process provide positive or negative economic incentives, which eventually influences criminals in their decision to utilize an instrument for ML.

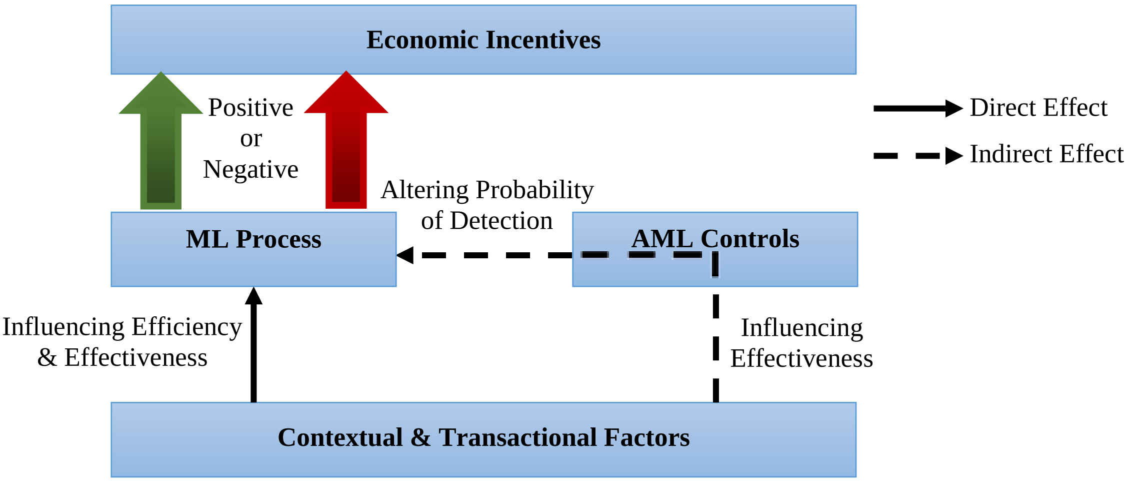
Economic Incentives
Positive or Negative
Direct Effect
Indirect Effect
Altering Probability of Detection
ML Process
AML Controls
Influencing Efficiency & Effectiveness
Influencing Effectiveness
Contextual & Transactional Factors

Figure 3. Conceptualization of the Analysis

4 Incentives to Utilize Cryptocurrencies for Money Laundering

As a first step to assess the risks posed by cryptocurrencies as possible ML instrument for AML, this chapter focuses on the incentives of criminals to utilize cryptocurrencies for ML. The first step is to present a brief introduction of the design philosophy behind cryptocurrencies, which is necessary to provide an understanding about their specific characteristics. Subsequently, a comparative analysis based on our conceptualization of the economic incentives of criminals to utilize a ML instrument is conducted (see Figure 3). In order to facilitate ML, cryptocurrencies must be perceived relatively advantageous to other potential ML instruments (Mantel and McHugh 2001). Therefore, we compare cryptocurrencies with traditional financial instruments and services as benchmark. Traditional financial instruments and services are the most important instruments for ML (Reuter and Truman 2004; UNODC 2013). Generally, a financial service involves the transaction of a financial instrument or money within the financial system using financial institutions. For our purposes, we consider currently used means of payment backed by conventional currencies. They allow for the transfer of funds between accounts supported by financial institutions. We deliberately choose such a broad definition to include a wide range of potential ML instruments (e.g. Credit Card, Online Money Transfer or PayPal) with common factors.

4.1 Design Philosophy behind Cryptocurrencies

Cryptocurrencies are internet-based payment systems with which two parties can carry out transactions over the internet. They are not tied to any fiat currency designated and issued by a central authority. Instead they possess their own unit of account (e.g. BTC for Bitcoin), while the respective value is determined by supply and demand and trust in the system (Velde 2013; Descôteaux 2014). They fall within in the notion of virtual currencies, which according to (ECB 2012) are, “a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community”. While there are virtual currencies around for some time (e.g. e-Gold, Liberty Reserve), the distinctive feature of cryptocurrencies is their decentralized nature without a centralized repository and no single administration (FATF 2014). Bitcoin’s success since its launch resulted in a number of alternative currencies such as Litecoin or Peercoin. They differ in their design such as the expected time to confirm transactions, maximum number of coins, used hash algorithm and transaction fees, to name a few differences (Bitcoin Wiki 2014). But for the purpose of our analysis in the context of ML those differences are of no significance, therefore we consistently use the term “cryptocurrencies” to consider all concrete implementations.

The concept of cryptocurrencies is based on the use of advanced encryption techniques alias cryptography. An intuitive way to understand the mechanisms is to think of a publicly accessible log file. This so log file records information about every accounts’ balance at a certain time and if somebody transfers funds, it is broadcasted to and accepted by all participants of the system (Peck 2012). The technical realization is based on a distributed peer-to-peer network. Individual computers act as nodes and bundle previously unrecorded transactions into blocks. They entail information regarding when a transaction between whom of which amount took place and are also linked to previous blocks before publishing. A hash value is then applied to record the transactions using cryptographic hash functions. The resulting public block-chain includes timestamps of all transactions ever conducted (Nakamoto 2008). Unlike physical money, digital files can be duplicated and hence it is possible to spend virtual money twice. In e-commerce this is traditionally prevented with an intermediary (e.g. PayPal, credit card company) verifying whether a transaction is valid or not (Chircu et al. 2000; Baddeley 2004). The block-chain provides awareness to the receiver of money that it has not been spent before and in this way solves the problem of *double-spending* (Möser et al. 2013).

The nodes transforming data into hash values and adding it to the block-chain are called miners. They compete against each other to find a hash value which meets certain requirements imposed by the protocol. In particular, the challenge is to find a sequence of data that produces a certain pattern when the hash algorithm is applied to it (Brito and Castillo 2013). That process requires a lot computing power, and hence, the miner who finds a solution to this mathematical problem first is rewarded with transaction fees paid by the senders of funds and an amount of newly generated money (until a certain threshold specified in the protocol is reached). The winning miner broadcasts a summary of all previously unrecorded transactions in a block to the other nodes in network, which validate and incorporate it into the block-chain and start working on the next block (Reid and Harrigan 2013). In addition to preventing *double-spending* such a proof of work principle also establishes scarcity, an important property of every virtual currency (Becker et al. 2013).

Accounts get tied to individuals via an asymmetric key encryption scheme. They are not really accounts in the traditional understanding, because funds “can be transferred and stored without using centralized storage or settlement institutions” (Dostov and Shust 2014). For the sake of simplicity we call them accounts, having in mind that they are in fact pairs of private and public keys. Account numbers are public keys and *ownership* is established by knowing the corresponding private key. Individuals can generate multiple of such key pairs, which allow them to handle more than one account simultaneously. To this end, individuals are not required to disclose personal information such as their names or addresses (Möser et al. 2013).

4.2 Comparative Analysis of Money Laundering Related Factors

The identification of the conceptual and transactional factors took place in a two-step process. Firstly, we reviewed literature of transnational organizations responsible for AML (i.e. UNODC and FATF) considering the risks of ML through financial instruments and services. This included general literature as well as literature specifically targeted at virtual currencies. It was complemented by the sparsely available academic literature about ML. We have thus been able to understand potential vulnerabilities of financial instruments and services, which are exploited by money launderers. Vulnerabilities are the result of certain design features (e.g. anonymity, irrevocable transactions, decentralization) and their implications (e.g. wide acceptance, borderless nature). Secondly, we searched for academic and the vast, fragmented online literature addressing the extent to which cryptocurrencies exhibit these vulnerabilities. In doing so, we identified contextual and transactional factors, which are now analyzed according to our conceptualization of how incentives for money launderers are provided.

Acceptability: A growing number of merchants are offering cryptocurrencies as payment method for both real and digital goods and services. Thus users are not necessarily required to exchange them for fiat currencies. Products and services range from clothing, electronics, groceries or travel services to games and online dating sites. One prominent example is the computer technology specialist Dell, who made the switch towards cryptocurrencies (Dell 2014). Furthermore, Ebay's payment unit PayPal allows digital goods merchants to accept Bitcoin payments (Paypal 2014). The purchase of commodities and services is a common way for money launderers to enjoy their illegal profits without necessarily drawing attention of government agencies. However, cryptocurrencies compared to traditional financial instruments and services currently are not nearly as widely accepted (Srinivas et al. 2014). From a money launderers' perspective, this limits the channels to convert, move and integrate illicit funds. One important aspect is that limited market size reduces the extent to which large amounts of illicit value can be moved and restricts the utility of cryptocurrencies for smaller scale illicit activities (AUSTRAC 2012). Therefore, we argue that limited acceptance currently has a direct effect on the execution of the ML process, providing negative incentives for money launderers to rely on cryptocurrencies. Even though this may evolve in the future, it is unlikely that they will gain greater acceptance than traditional financial instruments and services, which interact with a wide range of economic sectors (Dostov and Shust 2014).

Administration: Despite the fact that intermediaries are not required to process transactions, there is also no central oversight body authorized to control the supply of cryptocurrencies and prevent certain individuals from account creation. This task is executed by the decentralized peer-to-peer network which, moreover, makes it impossible for law enforcing agencies to confiscate accounts containing ill-gotten funds due to the lack of a central repository (FATF 2014). The accessibility of accounts is restricted to individuals knowing the corresponding private key. This is in contrast to financial institutions, with their ability to grant access to authorities for investigative purposes. It has an indirect effect, providing positive economic incentives for money launderers. High risk individuals, who are excluded from traditional financial instruments and services in AML regimes with effective customer identification procedures, need other channels to move illicit funds. Because of these low barriers to entry, cryptocurrencies are a particularly suitable instrument and they even permit to create several accounts without any restrictions including funding limits (UNODC 2014). The lack of a central authority prevents the applicability of a priori AML controls. This has an indirect effect on the execution of the ML process, providing positive incentives.

Authentication Level: Although the block-chain contains a public record of every transaction processed in the network, there is no identifying information of involved parties (Peck 2012; Velde 2013). Accountability is realized via asymmetric encryption, which allows for pseudonymously authentication. Following the privacy-terminology of (Pfitzmann and Hansen 2010): "A pseudonym is an identifier of a subject other than the subject's real names". Therefore, without access to identifying information from outside the system connecting public keys with subjects, it is impossible to identify particular individuals (Reid and Harrigan 2013). Additionally, multiple accounts can be opened by criminals to hide the true value of deposits. Pseudonymous authentication in connection with publicly accessible transaction histories is a double-edged sword with regard to the feasibility of AML controls. It prevents any successful customer identification procedures, as long as individuals don't interact with actors outside the network that collect personal identifying information (e.g. exchanges, online retailers). This is also addressed in the FATF recommendations, which explicitly require countries to give special attention to the risks arising from new or developing technologies that might facilitate transactions without disclosing personal identification (FATF 2012). Today no AML software is available to monitor and report suspicious transaction patterns (FATF 2014). Hence, the pseudonymous nature of cryptocurrencies has an indirect effect, providing positive incentives. At the same time, however, the public record allows to trace any transaction that has ever occurred. If a pseudonym is being associated with an individual, it is possible to identify suspicious activities in the transaction history (Möser et al. 2013). That calls for new AML controls based on the analysis and enrichment of transaction graphs (Meiklejohn et al. 2013; Ober et al. 2013; Reid and Harrigan 2013). Depending on their effectiveness, such controls may provide negative incentives for criminals to utilize cryptocurrencies for ML in the future.

Price Volatility: There exists a wide range of funding sources and withdrawal destinations for cryptocurrencies including: bank transfer, cash, other cryptocurrencies, payment cards or PayPal (ECB 2012; UNODC 2014). Cash acquired when committing predicate offences needs to be converted for cryptocurrencies and placed into the network through this channels. Money launderers will prefer funding sources that permit anonymous funding, like cash or third-party funding through exchangers that do not properly identify the funding source (FATF 2014). The same holds in the opposite direction, in order to convert funds back into fiat currency after or while layering. Unlike financial instruments and services, cryptocurrencies are not backed by fiat currencies. Consequently, the exchange rates between cryptocurrencies and fiat currencies fluctuate over time. All cryptocurrencies suffer from a high level of price volatility, what is likely to discourage individuals to utilize them for transactions (Rogojanu and Badea 2014; EPRS 2014). Funds may diminish in value during the layering stage, which requires money launderers to monitor the market continuously. This effort has to be added to the costs for the execution of the ML process and is of particular relevance for money launderers that may desire the flexibility to store their funds in cryptocurrencies. Hence, volatility has a direct effect on the execution of the ML process, providing negative economic incentives for money launderers.

Flexibility: It is possible to transfer cryptocurrencies globally, nearly instantaneously, with very low transaction fees. Accounts are not tied to any financial institution and the network processing transactions and transferring funds is a complex interconnected infrastructure. Several entities are involved, spread across different countries and one only needs an internet-supported device to participate. Since each node of the peer-to-peer network processes every transaction, and the difficulty of the mathematical problem to complete and publish blocks scales with the available computing capacity, the network only collapses when every node is disconnected (Nakamoto 2008). Thus, there is no single point of failure, which makes the system robust against disturbances (Bryans 2014). With financial instruments and services, the failure of a service provider negatively influences the processing of transactions. Flexibility has a direct effect, providing positive incentives to utilize cryptocurrencies compared to traditional financial instruments and services. Furthermore, it is essentially impervious for AML efforts to interrupt the ML process due to the systems flexibility. Therefore, flexibility also has an indirect effect, providing positive incentives for money launderers (Hochstein 2014).

Irrevocability: Irrevocability of transactions is a property cryptocurrencies have in common with cash (besides interaction without necessary identification). Once confirmed, the protocol does not offer any functionality of having transferred funds charged back unless the receiver issues a new transaction (Hurlburt and Bojanova 2014). That is the opposite of financial instruments and services, where it is possible to revoke transactions. Therefore, just like merchants offering legal goods or services, criminals benefit from this kind of fraud protection when committing predicate offences (Meiklejohn et al. 2013; UNODC 2014). They profit even more, because no rational criminal would take legal action against someone involved in an illegal financial transaction, due to the risk of being prosecuted likewise. Irrevocability has a direct effect, decreasing the risk of payment fraud when offering illegal products and services, providing positive incentives for money launderers. Beyond that, irrevocability also has an indirect effect, providing positive incentives. Funds are outside of control of any authority after the completion of a transaction. It is impossible for law enforcement to reverse the transaction a posteriori (Shasky Calvery 2013).

Payment Processing: Until the invention of cryptocurrencies online transactions required a trusted third party intermediary to verify payments and ensure that digital money could not be spent twice (double-spending problem). As mentioned, prevailing AML controls are based on transaction and user data being reported to law enforcement by these intermediaries (FATF 2013). This situation can be modeled as agency problem, where the intermediary acts as agent on behalf the government and has an informal advantage. Incentives for monitoring and transaction reporting are provided by means of fines for false negatives (i.e. not reporting of transactions which are identified to be suspicious ex-post) (Takats 2011). Unlike traditional financial instruments and services, cryptocurrencies do away with the need of interaction with third parties to process transactions by distributing the ledger among all users of the peer-to-peer network and offering irrevocable transactions (Brito and Castillo 2013). This has an indirect effect on the execution of the ML process, providing positive incentives for criminals to utilize cryptocurrencies for ML. This is because current controls and their enforcement depend on agents implementing them (EBA 2014).

Portability: Cryptocurrencies offer the opportunity to move large amounts of funds across national borders seamlessly without restrictions. The only requisite for this is an internet-supported device which grants access to the peer-to-peer network. ML is a transnational process in most cases, because the source of funds can be veiled more efficiently, when multiple jurisdictions are involved (Stessens 2000; Schott 2006). Practical experience indicates the particular difficulties when it comes to transaction monitoring across several jurisdictions, even when solely traditional financial instruments and services are involved (KPMG 2014). It requires cooperation between authorities (with potentially diverging interests) on a global scale in order to develop a consistent approach, whilst it has traditionally been carried out in a localized manner (Dilley et al. 2013). National borders nevertheless constitute a danger of being discovered, it be whether while smuggling large sums of cash through border controls or be it because of increasing reporting obligations of transnational capital flows (Basel Committee on Banking Supervision 2014). This suggests the conclusion that the borderless international transferability of cryptocurrencies through global operating networks complicates monitoring of suspicious transactions. Thus, portability has an indirect effect on the execution of the ML process, providing positive incentives for money launderers. But portability has also a direct effect, providing positive incentives, because funds may be easily accessed from any remote location.

Rapidity: Scholars have long acknowledged the link between advances in information and communication technology and increasingly transnationally interconnected financial systems (Zagaris and MacDonald 1992). One of the results of this globalization is the tendency towards instantaneous payment solutions. Rapidity is the speed with which transactions can occur. Cryptocurrency transactions are usually conducted in real time, which renders ongoing account and transaction monitoring very difficult and the suspension of suspicious transactions impossible. Another particular risk associated with near instantaneous transactions over the internet is, that they build up an extensive audit trail in a short space of time, requiring additional resources for near-time analysis (Philippsohn 2001). This complicates the timely monitoring, investigation of suspicious transactions and also the freezing of funds (UNODC 2014). Rapidity has an indirect effect on the execution of the ML process, providing positive incentives for money launderers. Furthermore, instantaneous transaction processing increases the time-efficiency of the ML process (FED 2013). This is why rapidity also has an indirect effect, providing positive incentives for money launderers.

Transaction Costs: The transaction costs of traditional financial instruments and services vary as a function of transaction value and charges policy of the respective service provider. They include for example currency conversion fees, effort for authorization through the intermediary or interchange fees. An overseas money transfer with Western Union, for example, incurs on average round about 10% of the monetary value transferred as transaction costs (Western Union 2014). Cryptocurrencies serve as inexpensive funds-transfer systems potentially driving savings for merchants and users (Nathan et al. 2014). Because the distributed peer-to-peer network enables transfers directly between accounts, the only transaction costs of cryptocurrencies are the operating costs for authorization and verification of payments (FATF 2014). These costs are negligible at the moment, but may rise as operations scale up (Houy 2014; Kashaloglu 2014). Nevertheless, for our analysis we assume that the cost advantages will remain in the future. Costs associated with ML activities are transaction costs and have to be considered when choosing the instruments used. As stated by (Masciandaro 1999) transaction costs for ML are the aggregated costs due to AML activities and the technical costs related to the specific ML instrument. In general, illicitly acquired funds require to go through multiple transactions and parties across different jurisdictions, aiming at reducing the risk of being discovered and prosecuted to an acceptable level. The lower the costs for conducting these transactions are, the higher the revenue of ML. For that reason, the cost advantage of cryptocurrencies over traditional financial instruments and services allows for a more cost-efficient ML process. It has a direct effect, providing positive incentives for money launderers (FED 2013; EBA 2014).

Instrument Factors		Financial Instruments & Services	Cryptocurrencies	Effect Provides (+/-) Incentives for ML	
				Direct Effect	Indirect Effect
Contextual	Acceptability	Widely Accepted	Limited Acceptance	-	
	Administration	Designated & Issued by a Central Authority	Decentralized Mining & Storing		+
	Authentication Level	Identified Authentication	Pseudonymous Authentication		+
	Price Volatility	Relatively Stable	High Volatility	-	
Transactional	Flexibility	Transactions Depending on Service Provider	No Central Point of Failure	+	+
	Irrevocability	Revocable Transactions	Irrevocable Transactions	+	+
	Payment Processing	Based on Intermediaries	No Intermediaries Required		+
	Portability	Increasing Transnational AML Efforts	International Transferability	+	+
	Rapidity	Up to Several Days	Instantaneous Transactions	+	+
	Transaction Costs	Varying Fees & Charges	Low or not Existent Transaction Costs	+	
Examples		Credit Card, Online Money Transfer, Wire Transfer, PayPal, Other Monetary Instruments	Bitcoin, Litecoin, Peercoin		

Table 2. Comparative Analysis

4.3 Results of the Comparative Analysis

Table 2 provides an overview of the main findings from the preceding comparative analysis. It is structured according to our differentiation, whether the identified contextual and transactional factors have a direct or indirect effect on the execution of the ML process and how they provide incentives for criminals (either positively or negatively). Without revising the respective factors explicitly, it can be summarized that the vast majority of them may provide positive incentives for criminals to utilize cryptocurrencies for ML. We identify limited acceptance and high price volatility of cryptocurrencies as the only factors considered to provide negative incentives. The distribution between direct and indirect effects is fairly even. Five factors directly increase the efficiency and effectiveness of the ML process compared to conventional financial instruments and services. Additionally, this result supports the claim that cryptocurrencies provide positive economic incentives for honest individuals. Seven properties facilitate ML by limiting the applicability of prevailing AML controls. It confirms our assumption that both the direct and the indirect effects on the ML process shape the incentives of criminals. The results do indicate that cryptocurrencies can be a driver for ML, but not to which extent the respective factors facilitate it. This implies that we do not yet consider dependencies between and the importance of the individual factors.

5 Related Challenges

The preceding analysis aimed at providing a better understanding about the economic incentives of criminal individuals to misuse cryptocurrencies for ML, based on their specific properties. We have identified that cryptocurrencies may indeed constitute an attractive instrument for money launderers from an economic point of view. However, as the analysis indicates, already evolving technological developments and regulatory approaches may affect the economic incentives. We are aware that this requires a view that integrates findings from the disciplines of economics, computer sciences, legal studies as well as law enforcement authorities.

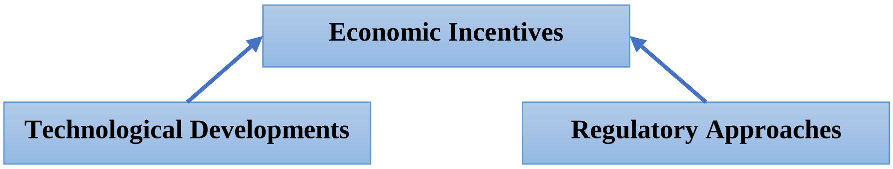

Figure 4. Related Challenges

Current research on ML with cryptocurrencies in computer sciences concentrates mainly on statistical analysis and data mining to enable traceable transactions. As briefly mentioned above, pseudonymity is only guaranteed as long as an individuals public key cannot be linked to his true identity (Möser et al. 2013). In particular, it is necessary to systematically evaluate available approaches to utilize context information based on the structure of the network inferred from the block-chain (e.g. transactions including amounts transferred over time) and the integration of data from outside the system (e.g. voluntary disclosures of identifying information in social networks). Some promising work has already been conducted in this area (Meiklejohn et al. 2013; Ober et al. 2013; Reid and Harrigan 2013). Nevertheless, it remains unclear to what extent those approaches are appropriate to monitor transactions timely and indicate suspicions for ML. Especially when taking into account recent developments of mixing services or currencies, which aim at providing untraceable transactions (e.g. Ben-Sasson et al. 2014; Bonneau et al. 2014; Ruffing et al. 2014). The success of appropriate tools could imply a paradigm shift in AML controls, where monitoring of actual transactions gains more relevance compared to ex-ante customer identification procedures. This would clearly influence the economic incentives of money launderers, too. If it becomes possible for law enforcement to link transactions to identities with a certain degree of precision, the probability of identifying suspicious transactions increases. That imposes additional costs on criminals, since they either need to implement more sophisticated laundering schemes or accept the higher risk of prosecution and conviction. Additionally, possible privacy violations have to be considered due to derivations from the permanent public availability of transaction data (Androulaki et al. 2013).

The regulatory perspective is also highly relevant, because cryptocurrencies are currently hardly regulated and not closely supervised or overseen by any public authority (ECB 2012). As pointed above, prevailing AML controls are implemented at the level of financial institutions and designated non-financial businesses (FATF 2012; EBA 2013). One starting point for the regulation of cryptocurrencies may be exchanges for client information that the exchanger collects (FATF 2014). The U.S. FinCEN follows this approach and stated that administrators and exchangers of cryptocurrencies are money exchangers under existing regulations (FinCEN 2013). However, a large number of issues remain open. The rapidly evolving nature of technology and business models with changing market roles and participants providing services causes uncertainty regarding how regulation should be carried out in practice and needs to be addressed (FATF 2014). Another challenge lies in tailoring regulation under consideration of the specific properties of cryptocurrencies (e.g. actors will be allocated in one jurisdiction and operate in another one). Furthermore, a level of regulation should be identified that minimizes ML risks by creating negative incentives for criminal individuals. At the same time, overregulation must be avoided. Only then it could be ensured that honest individuals do not hesitate from using cryptocurrencies.

6 Conclusion & Outlook

Against the background of a growing propagation of the cryptocurrencies' ecosystem, we have to address the challenges it imposes for financial systems in general and especially for AML programs around the globe. This research provides a first step towards an economic analysis of ML utilizing cryptocurrencies. In particular, this paper focuses on the economic incentives of criminals to utilize cryptocurrencies as ML instrument. Only if cryptocurrencies are perceived as beneficial from a criminals' point of view, and for that reason are used as ML instrument, they represent a risk for combating ML. After setting the context, we introduced the ML process, gave an overview of AML controls and conceptualized our analysis. As the first study, we distinguished between direct effects (i.e. the direct impact our derived factors might have on the process execution) and indirect effects (i.e. the indirect impact on the process execution by changing the effectiveness of prevailing AML controls), which allowed us to state whether the identified factors provide positive or negative economic incentives for ML. This formed the theoretical foundation for the comparative analysis. In order to assess the risks posed by cryptocurrencies for AML, we identified and analyzed contextual and transactional factors that facilitate ML from the perspective of criminal individuals to reveal their incentives. This was done against the benchmark case of utilizing conventional financial instruments and services. Based on this explorative analysis it can be concluded that the presented properties might indeed encourage the exploitation of cryptocurrencies by money launderers. Afterwards, we also provided a brief overview of related challenges that might impact the economic incentives of money launderers.

Clearly, this analysis constitutes only an initial step towards the examination of cryptocurrency backed money laundering. Additional research needs to be conducted in light of the interconnections with current research in other disciplines such as computer sciences and legal studies, because their results may impact the economic incentives of money launderers to utilize cryptocurrencies. The identified contextual and transactional factors need to get further specified and evaluated in future work. There may also be other factors which have remained unconsidered. We intend to cooperate with investigative authorities and financial institutions in order to derive realistic ML schemes with cryptocurrencies. In the future, we are going to examine appropriate and effective tools, including a variety of risk mitigation processes to address the identified risks. The analysis of ML is one part of our overarching incentive-oriented approach towards the evaluation and design of virtual currencies. The ongoing development of a holistic framework requires the perspective of honest as well as dishonest individuals, because every financial instrument is also potentially misused by criminals. Although they are presently the most prominent example in the context of virtual currencies, cryptocurrencies are not the first type of digital money and it is likely that they won't be the last. It is even conceivable that governments will issue their own digital money, due to the high maintenance costs for monetary systems (i.e. printing and distribution of banknotes) and new arising business opportunities for economies. Therefore, we will extend our analysis to honest individuals, combine the results, elaborate if there are inevitable trade-offs and use the results to derive requirements for future digital forms of money.

References

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer T. and Capkun, S. (2013): “Evaluating User Privacy in Bitcoin.” In: *Financial Cryptography and Data Security.* Ed. by D. Hutchison, T. Kanade and J. Kittler, Springer Berlin Heidelberg, Berlin, Heidelberg, 34-51.

AUSTRAC (2012). *Typologies and Case Studies Report 2012*. Australian Transaction Reports and Analysis Centre.

Baddely, M. (2004). “Using E-Cash in the New Economy: An Economic Analysis of Micropayment Systems”. *Journal of Electronic Commerce Research* 5 (4), 239-253.

Basel Committee on Banking Supervision (2014). *Sound management of risks related to money laundering and financing of terrorism.* Jan. 2014. Bank for International Settlements, Basel.

Bauer, P. and Ullmann R. (2001). “Understanding the Wash Cycle”. *Economic Perspectives* 6 (2), 19-23.

Becker, G. (1968). “Crime and Punishment: An Economic Approach. *The Journal of Political Economy* 76 (2), 169-217.

Becker, J., Breuker, D., Heide T., Holler J., Rauer, H. P. and Böhme, R. (2013). “Can we Afford Intergrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency.” In: *The Economics off Information Security and Privacy.* Ed. by R. Böhme, Springer Berlin Heidelberg, Berlin, Heidelberg, 135-156.

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M. (2014). “Zerocash: Decentralized anonymous payments from Bitcoin.” In: *IEEE Symposium on Security and Privacy*. IEEE.

Bitcoin Wiki. *Comparison of Cryptocurrencies.* URL: https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies. (visited on 09/19/2014).

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A. and Felten, E.W. (2014). “Mixcoin: Anonymity for Bitcoin with accountable mixes.” In *Financial Cryptography and Data Security. March 2014.*, Springer Berlin Heidelberg, 486-504.

Brezo F. and Bringas, P. G. (2012). “Issues and Risks Associated with Cryptocurrencies such as Bitcoin.” In: *SOTICY 2012: The second international conference on social eco-informatics. October 21-26, Venice, Italy.* Ed. by L. Berntzen and P. Dini. IARIA, [S. 1], 20-26.

Brito, J. and Castillo, A. (2013). *Bitcoin: A Primer for Policymakers.* Mercatus Center at George Mason University

Bryans, D. (2014). “Bitcoin and Money Laundering: Mining for an Effective Solution.” *Indian Law Journal* 89 (Iss. 1), Article 13, 441-472.

Chircu, A., Davis G. and Kauffmann, R. (2000). “Trust, Expertise, and E-Commerce Intermediary Adoption.” *AMCIS 2000 Proceedings, Paper 405,* 710-716.

CoinMarketCap. *Crypto-Currency Market Capitalizations.* URL: http:// http://coinmarketcap.com/ (visited on 03/16/2015).

Dell. *Dell now accepts bitcoin*. URL: http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing (visited on 09/21/2014).

Descôteaux, D. (2014). *How should Bitcoin be regulated?: Economic Note.* Montreal Economic Institute.

Dilley, B., Dawson, N. and Schutze, J. (2013). *Virtually Unregulated: Countering Virtual Currency Money Laundering in the 21st Century*.

Dostov V. and Shust, P. (2014). "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators? *Journal of Financial Crime* 21 (3), 249-263.

EBA (2013). *EBA warns consumers on virtual currencies* European Banking Authority. URL: http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies (visited on 10/07/2014).

EBA (2014). *EBA Opinion on 'virtual currencies'.* EBA/Op/2014/08. European Banking Authority. URL: http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (visited on 03/16/2015).

ECB (2012). *Virtual currency schemes.* European Central Bank. Frankfurt-on-Main. URL: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (visited on 03/16/2015).

EPRS (2014). *"Bitcoin: market, economics and regulation"* Briefing. European Parliamentary Research Service. URL: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI%282014%29140793_REV1_EN.pdf (visited on 03/16/2015).

EU (2005). "DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005: on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing." *Official Journal of the European Union* (L 309/17).

FATF (2012). *The FATF Recommendations - International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.* Financial Action Task Force. URL: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (visited on 03/16/2015).

FATF (2013). *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.* Financial Action Task Force. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/aml_cft_measures_and_financial_inclusion_2013.pdf (visited on 03/16/2015).

FATF (2014). *Virtual Currencies Key Definitions and Potential AML/CFT Risks: FATF Report*. Financial Action Task Force. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (visited on 03/16/2015).

FBI (2012). *(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Federal Bureau of Investigation: Cyber Intelligence Section and Criminal Intelligence Section.

FED (2013) *Payment System Improvement - Public Consultation Paper*. Federal Reserve Financial Services. URL: https://fedpaymentsimprovement.org/wp-content/uploads/2013/09/Payment_System_Improvement-Public_Consultation_Paper.pdf (visited on 03/16/2015).

Ferwerda, J. (2009). "The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime?" *Review of Law & Economics* 5 (2), 903-329.

FinCEN (2013). *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.* FIN-2013-G001. Department of the Treasury – Financial Crimes Enforcement Network. URL: http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (visited on 03/16/2015).

Geiger, H. and Wuensch, O. (2007). "The fight against money laundering: An economic analysis of a cost-benefit paradoxon." *Journal of Money Laundering Control* 10 (1), 91–105.

Hochstein, M. (2014). “Why Bitcoin Matters for Bankers.” *American Banker Magazine, 124(2), 18*. URL: http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html. (visited on 11/6/2014).

Houy, N. (2014). *The Economics of Bitcoin Transaction Fees: Working Paper*. Université de Lyon.

Hurlburt, G. F. and Bojanova, I. (2014). “Bitcoin: Benefit or Curse?.” *IT Professional* 16 (3), 10–15.

IMF (2014). *The IMF and the Fight Against Money Laundering and the Financing of Terrorism*. URL: http://www.imf.org/external/np/exr/facts/pdf/aml.pdf.

Kashaloglu, K. (2014). “Near Zero Bitcoin Transaction Fees Cannot Last Forever.” In: *The International Conference on Digital Security and and Forensics (DigitalSec2014)*, The Society of Infor-Digital mation and Wireless Communication, 91–99.

KPMG (2014). *Global Anti-Money Laundering Survey – 2014*. URL: http://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf (visited on 16/03/2015).

Mantel, B. and McHugh, T. (2001). Competition and Innovation in the Consumer e-Payments Market? Considering the Demand, Supply, and Public Policy Issues. *Federal Reserve Bank of Chicago Public Policy Working Paper No. EPS-2001-4.*

Masciandaro, D. (1998). “Money Laundering Regulation: The Micro Economics.” *Journal of Money Laundering Control* 2 (1), 49–58.

Masciandaro, D. (1999). “Money Laundering: the Economics of Regulation.” *European Journal of Law and Economics* 7 (3), 225–240.

McCusker, R. (2007). “Transnational organised cyber crime: distinguishing threat from reality.” *Crime, Law and Social Change* 46 (4-5), 257–273.

McDowell, J. and Novis, G. (2001). “The Consequences of Money Laundering and Financial Crime.” *Economic Perspectives* 6 (2), 6–10.

Meiklejohn, S., Pomarole, M. and Jordan, G. Levchenko, K., McCoy, D., Voelker, G. M. and Savage, S (2013). “A fistful of bitcoins: characterizing payments among men with no names.” In: *IMC'13 Proceedings of the 2013 conference on Internet measurement conference.* Ed. by K. Papagiannaki, K. Gummadi and C. Partridge, 127–140.

Möser, M., Böhme, R. and Breuker, D. (2013). “An inquiry into money laundering tools in the Bitcoin ecosystem.” In: *2013 eCrime Researchers Summit (eCRS)*, pp. 1–14.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System. Consulted, 1*(2012), 28.

Nathan, A., Currie, J., Ursua, J., Wilson, D. and Leaf, R. (2014). *Top of Mind: All About Bitcoin*.

Ober, M., Katzenbeisser, S. and Hamacher, K. (2013). “Structure and Anonymity of the Bitcoin Transaction Graph.” *Future Internet* 5 (2), 237–250.

PayPal (2014). *PayPal Payments Hub*. URL: https://www.paypal.com/webapps/mpp/paymentshub. (visited on 10/15/2014).

Peck, M. E. (2012). “The cryptoanarchists' answer to cash.” *IEEE Spectrum* 49 (6), 50–56.

Pfitzmann, A. and Hansen, M. (2010). *Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology: Version 0.34*.

Philippsohn, S. (2001). “Money Laundering on the Internet.” *Computers & Security* 20 (6), 485–490.

Reid, F. and Harrigan, M. (2013). “An Analysis of Anonymity in the Bitcoin System.” In: *Security and Privacy in Social Networks*. Ed. by Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony and A, Pentland, Springer New York, New York, NY, pp. 197–223.

Reuter, P. and Truman, E. M. (2004). *Chasing dirty money: Progress on anti-money laundering*. Institute for International Economics, Washington, DC.

Rogojanu, A. and Badea, L. (2014). “The issue of competing currencies. Case study – Bitcoin.” *Theoretical and Applied Economics* 21(1), 103-114.

Ruffing, T., Moreno-Sanchez, P. and Kate, A. (2014). “CoinShuffle: Practical decentralized coin mixing for Bitcoin.” In *Computer Security-ESORICS 2014*. Springer International Publishing, 345-364.

Schneider, F. and Windischbauer, U. (2008). “Money laundering: some facts.” *European Journal of Law and Economics* 26 (3), 387–404.

Schott, P. A. (2006). *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, Second edition*. World Bank Publications.

Shasky Calvery, J. (2013). *Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury: Before the United States Senate Committee on Homeland Security and Government Affairs*.

Srinivas, V., Piscini, E., Dillion, D. and Zagone, R. (2014). *Bitcoin: The new gold rush?*. Deloitte Center for Financial Services.

Stessens, G. (2000). *Money laundering: A new international law enforcement model*. Cambridge University Press, Cambridge, New York.

Stokes, R. (2012). “Virtual money laundering: the case of Bitcoin and the Linden dollar.” *Information & Communications Technology Law* 21 (3), 221–236.

Takats, E. (2011). “A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement.” *Journal of Law, Economics, and Organization* 27 (1), 32–78.

UNODC (1988). *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*. URL: http://www.unodc.org/pdf/convention_1988_en.pdf (visited on 03/16/2015).

UNODC (2005). *Model legislation Model legislation on money laundering and financing of terrorism*. URL: https://www.imf.org/external/np/leg/amlcft/eng/pdf/amlml05.pdf (visited on 03/16/2015).

UNODC (2011). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes*. URL: http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf (visited on 03/16/2015).

UNODC (2013). *Risk of Money Laundering through Financial and Commercial Instruments*, Bogota, D.C. URL: http://www.imolin.org/pdf/Risk_of_Money_Laundering_Version_2.pdf visited on 03/16/2015).

UNODC (2014). *Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies*. United Nations Office on Drugs and Crime. URL: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf (visited on 03/16/2015).

Velde, F. (2013). “Bitcoin: A primer.” *Federal Reserve Bank of Chicago Essays on Issues* (317).

Villasenor, J., Monk, C. and Bronk, C. (2011). *Shadow Figures: Tracking Illicit Financial Transactions in the Murky Word of Digital Correncies, Peer-to-Peer Networks, and Mobile Device Payments*. The Brookings Institution and the James A. Baker III Institute for Public Policy URL:

http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf.

Western Union (2014). *Fees for Western Union Services*. URL:https://www.westernunion.com/us/en/price-estimator/start.html. (visited on 10/29/2014).

Zagaris, B. and MacDonald, S. B. (1992). “Money laundering, financial fraud, and technology the perils of an instantaneous economy.” *The George Washington Journal of International Law and Economics* 26 (1), 61–107.