IMPLICATIONS OF CRYPTOCURRENCIES IN MONEY LAUNDERING

Edouard VAN DEN HEUVEL[a], Darby WESSELINK[a], Mario BOOT[a], Marc VORNETRAN[a] and Zijian WANG[a]

[a] *Graduate School of Informatics*
Faculty of Science
University of Amsterdam

Abstract. Money laundering has a new vehicle: cryptocurrencies. Reportedly, regulations in countries worldwide are sought to prevent money laundering related to cryptocurrencies. However, a lack of literature on the topic restrains the pace of developing such efforts. This qualitative research based on a grounded theory methodology aims to provide insights for future research. Four interviews with field experts from various backgrounds are conducted. By combining the interviews with literature, implications of cryptocurrencies in money laundering are concluded.

Keywords. Money laundering, Cryptocurrency, Bitcoin

1. Introduction

1.1. Background, relevancy and problem statement

Innovations in cryptocurrencies provide criminals with new possibilities for money laundering, but there is a shortage of insights on the exact relationship. This motivates the aim of this qualitative investigation: providing insights on the extent to which cryptocurrencies are used for money laundering. The investigation focuses on the fields of criminology, law enforcement and information systems. Money laundering as a criminal activity has the primary focus together with cryptocurrency as a laundering vehicle. The investigation is relevant because of the implications this phenomenon has for research directives and resource allocation.

Within the relatively short existence of cryptocurrencies (CCs), there are 170 money laundering (ML) cases in the past 6 months in Japan alone (Kyodo, 2017). On the other side of the world, some of the European governments are planning a crackdown on Bitcoin in response to growing speculations of the use of the digital currency for ML and tax evasion purposes (Kollewe, 2017). The founder of Liberty Reserve, a CC used by cybercriminals, was pleaded guilty for laundering more than 250 million dollars 'through his digital currency business' (The U.S Department of Justice, 2016).

1.2. Research questions

Given that newly developed cryptocurrencies are a vehicle for money laundering, the following main research question has been chosen: **to what extent are cryptocurrencies used for money laundering?**

To assist achieving the goal of the research, the following sub-questions are proposed:

1. What is the scope of the influence of CCs in ML?
2. How can CCs be exploited for ML?
3. Who are the stakeholders in detecting ML activities using CCs?

1.3. Transactional mechanisms of cryptocurrency

Prior to the research, a fundamental understanding of the transaction mechanism of CCs is reached as a common starting point. Figure 1 demonstrates the mechanism of CC transactions.

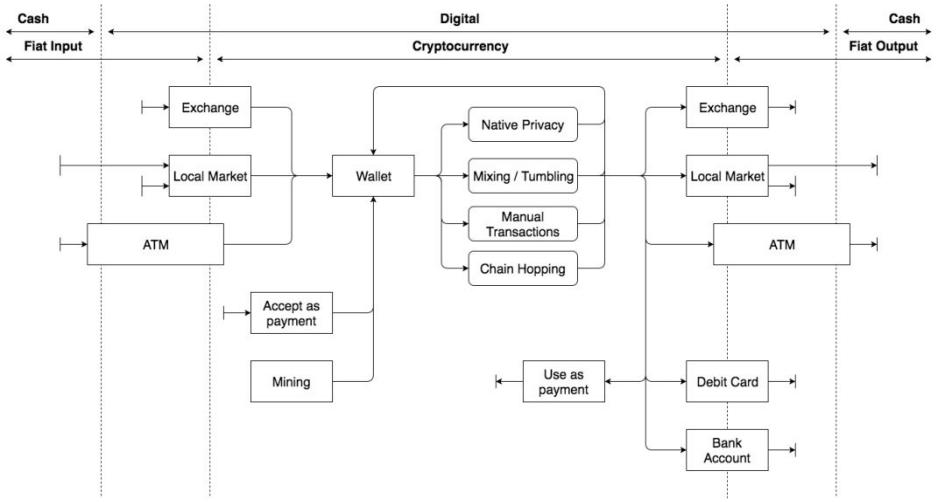

Figure 1 - Transaction model of cryptocurrencies

Various types of exchanges put money into the CC system, including: exchanges, local peer-to-peer trading markets and automated teller machines (ATMs) There, a number of services are available for manipulation and transformation. Converting CC back to regular currencies can be achieved using the same services as in the input. Notably, special debit cards and bank accounts can be funded using CCs.

1.4. Structure

The structure of the report follows the research cycle of the grounded theory method. Based on existing literature, chapter 2 explains the core concepts blockchain, Bitcoin and ML. Research methodology follows in chapter 3. Chapter 4 illustrates the design of interviews, as well as data collection. Chapter 5 presents the essential findings, followed by the conclusions in chapter 6. In chapter 7, the study's limitations and implications are discussed.

2. Theoretical base

The initial literature review creates a foundation of basic concepts related to the theme. ML is the core topic to be investigated, while blockchain is the backbone of all CCs. In addition, an instance of the most value-increasing cryptocurrency, Bitcoin, is explained.

2.1. Money laundering

Due to the long-standing history of illegal activity, the term 'money laundering' has been defined through multiple endeavors. This report adopts a simplified definition of ML: *a criminal activity that forges the illegal source of money to appear as a legitimate one*. This definition is based on Schneider (2008), Masciandaro (1999), Low (2017) and interviews.

2.2. The Blockchain and Bitcoin

The blockchain technology is the enabling technology behind CCs. The blockchain is an incremental ledger based on information consistency as approved by all involved nodes (Zohar, 2015). The technology is simple in logic, easy to implement yet resistant against illicit manipulation. It is regarded as a revolutionary invention which can be compared to the internet.

Bitcoin is knowingly the first application of the blockchain technology, which enables peers to transfer money online anonymously. It is introduced after the global financial crisis in 2008 with an aim of creating an electronic financial system based on proof-of-work instead of trust. It is revolutionary since the role of central banks, governments and other third parties is excluded from transactions. This exclusion provides privacy to users and prevents double spending (Nakamoto, 2008).

3. Methodology

This research is explorative as it aims to achieve a preliminary understanding of the relatively unknown phenomenon of ML activities using CCs. A grounded theory methodology is chosen to unearth theory filling the previously described gap. Insights derived from literature combined with expert interviews are input for the grounded theory method. The interviews are described further in the next chapter. Literature on ML approaches and police reports are considered as well. The research is conducted in Amsterdam, the Netherlands, over a period of seven weeks. The flowchart of Bitsch (2005) in Figure 2 demonstrates the procedure of the research.

Conclusions are drawn based on a triangulation of interviews and literature. Datasets containing statistical data about aforementioned topics were not accessible for this investigation due to time and resource constraints. A lack of statistical data, a need for insights and access to experts and literature validates the justification for this interpretivist analysis.

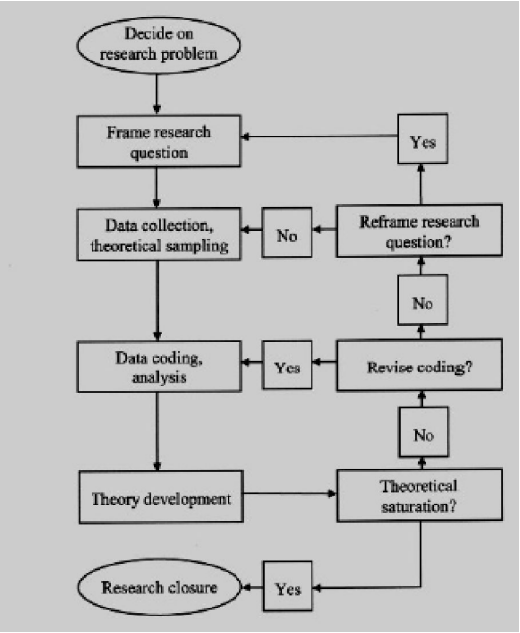

Figure 2 - Grounded Theory Flowchart (Bitsch, 2005)

4. Interviews

4.1. Sampling

Convenience and snowball sampling fits the time- and resource constraints of this study. The research team reached out to academic scholars working on the intersection of ML and CCs. A preliminary understanding of the domains in scope (criminology, law enforcement, and information systems) served as starting point for manually searching candidates via internet search engines. From the 19 candidates, 4 agreed to be interviewed, and the interviews were conducted in 3 weeks. The first interviewee provided contacts for two other interviewees. Table 1 summarizes the title, organization and background of the interviewees.

For each domain in scope one interviewee has been interviewed, and interviewees are selected based on knowledgeability and trustworthiness. Therefore, a basic level of saturation is achieved. Triangulation with literature review and description of limitations compensates for interviewee bias, which is further described in chapter 7.

A peculiar interview was held with interviewee 4 who acts as real-life money launderer. One of the members from the research team possessed a trust relationship with interviewee 4. This relationship, together with mutual consent and complete anonymity lays a foundation for considering this interview as partially credible and trustworthy.

Interviewee	Title & Organization	Background
I.1	Lecturer on Financial Investigation at a law enforcement agency	Has been conducting research on financial investigations related to blockchain and CCs.
I.2	Senior Researcher on Cybercrime at a crime research agency	Director for a research group on cybercrime; has collaborated in cryptocurrency crime investigations; holds a PhD in cybercriminal networks.
I.3	Strategist at a cryptocurrency exchange	Has been involved in growth of a legal cryptocurrency exchange organization since the founding of the organization. Works with international criminology organizations and other law/compliance related companies.
I.4	Not applicable	Money launderer and narcotics trader. Has been laundering 50.000-100.000 euro in past 5 years.

Table 1 - Interviewee summary

4.2. Structure of interviews

With interviewee approval, transcriptions were made from sound recordings. The semi-structured and face to face interviews took place in the work offices of the interviewee. Except for I.4 who was met in a public restaurant. A standardized list of questions (see Appendix III) was developed to reduce interview variance. The number of interviewers ranged between 1 and 2 due to planning constraints. All interviewers are from the research team who conducts this study. No standard list of probing and prompting remarks was used.

4.3. Data collection

Interview content is coded, meaning that the text is analyzed by looking for indicators to themes. Main attention is given to a number of coding categories:

- Highlights
- Interviewee background
- Legal context
- Privacy
- ML (connected with CC)
- Inter-interviewee (dis)agreement
- Law enforcement
- Scope
- Stakeholders
- Other

Inter-reviewer consistency is achieved by discussing coding results among reviewers. A common understanding of interview content is obtained by agreeing on the findings in the interviews.

The following summaries of statements are consistently present in all interviews:

1. The blockchain has a wide range of potential applications and ML via CCs is just one of the use cases.

2. CCs offer advantageous features to criminals which increase along with CC maturity, but the exact scope and size is unknown.

3. Criminals do use CCs in the process of ML, however the majority of criminals relies on traditional schemes of activity.

4. Regulation for CCs is lacking.

5. Bitcoin transactions are traceable, but Monero's transactions are not.

6. Trust in personal relationships and in used practices and systems is vital to criminals.

The following statements are subject to debate:

1. No complete consistency among interviewers that criminals are reluctant to adopt CCs for ML. I.2, I.3 and I.4 confirm reluctancy while I.1 believes that CCs are very popular among criminals.

2. I.1 and I.2 state that reverse burden of proof may speed up financial cyber crime convictions.

The following statements are made by one interviewee:

1. I.3: Anti-ML analysis tools are used to identify outliers of transactions

2. I.3: A number of CC companies are actively focusing on preserving industry reputation and brand imago, by ensuring compliance with financial regulations.

3. I.2: A website called LocalBitcoins.com and CC ATMs are prone to involvement in ML schemes.

5. Findings

To answer the research question, collected data is analyzed structurally in terms of sub questions. Newly-gained insights from the interviews - the 3-Step Model of Money Laundry, Monero, and the role of trust - are researched by further literature review.

5.1. Scope of influence

The influence of ML via CCs is cross-domain and cross-border by nature. Both private and public sector are involved and these activities have implications for the fields of criminology, law enforcement and information systems. All of the micro-, meso- and macro levels are touched. Both existing literature and interviewees are aligned on this influence. I.2 suggests that CCs dissolve social barriers in international money movement.

It is agreed that the exact scope is unknown. The precise influence cannot be quantified on a detailed level due to the absence of information. Yet, the cases of Liberty Reserve and MtGox (Trautman, 2014; Decker and Wattenhofer, 2014) give an indication of the scope's size and significance.

5.2. Exploitation of cryptocurrencies for money laundering

To grasp an understanding of the exploitation of CCs in ML, the 3-Step Model of ML is recommended. When the transaction model in figure 1 is mapped onto the 3-step model, a potential money laundering scheme emerges. Interviewees 1 & 2 argue that CCs are used most often for the purpose of 'placement'. A possible weak point for laundering money this way is the phase of 'integration", because financial institutions might require justifications for transferring money to the "white" world.

Figure 3 - 3-Step model for ML (Renner, 2017)

However, based on the interviews with I.2, I.3 and I.4, it can be concluded that the role of CCs in ML is relatively small. Criminals are reluctant to adopt CCs which might be explained by the uncertainty of the future of the field. The MtGox case indicates potential system errors and Bitcoin has been called by others as a potential "tulip mania" (Zohar, 2015). Reluctance to adopt can be explained by criminal's need for trust. I.2 and I.4 emphasize this need for trust.

Some so-called "altcoins" offer criminals features that are potentially more advantageous for criminals, while harder to investigate, compared to Bitcoin. The potential advantage that Monero and Zcash are untraceable by design (Ben-Sasson, et al., 2014) is confirmed by all interviewees. The exact role and implications of these CCs for ML are hardly covered - not in academic literature and not in legislation. Search queries "Monero" and "Zcash" on academic literature search engines and Rechtspraak.nl (the Dutch database of court ruling documentation) delivered no results specific to ML.

5.3. Stakeholders

Governments and law enforcement agencies are stakeholders in the public domain as confirmed by I.1, I.2, I.3 and a report from the Dutch Ministry of Justice and Security (Ministerie van Justitie, 2016). Appendix I outlines a detailed list of stakeholders.The same sources are aligned on the involvement of CC companies in the private domain such banks, CC exchanges and merchants. However, some CC companies tend to comply already with existing laws out of social responsibility and self-interest, as indicated by I.3. Parties may benefit from CCs for socially acceptable and legal purposes.

In the public-private domain, trade associations might play a role in preserving industry reputation and compliance as indicated by I.3. Criminals are an obvious stakeholder. Infiltration into existing networks and analysis of convicted cases helps in determining the implications of their actions.

Lastly, as indicated by I.2, a number of relatively new type of organizations are subject to involvement. ATMs where cash money can be transformed into cryptocurrencies via ATMs have come into existence and might be used for ML schemes. Also LocalBitcoins.com is prone to ML activity.

5.4. Additional findings

The role of trust was brought up by I.2 and was confirmed by I.4. It is essential to I.4 that he can trust personal relationships and systems. He prefers to stick to traditional schemes of activities with persons that he is familiar with, above adopting a relatively unknown system.

Moreover, to help with the understanding of legal procedure of ML, the six step model of ML prosecution (see Appendix II) is proposed by the Supreme Court of the Netherlands (De Hoge Raad). The model is applied to identify ML related crimes (Ministerie van Veiligheid en Justitie, 2015).

6. Conclusion

This qualitative undertaking leads to implications for the fields of criminology, law enforcement and information systems. Implications are reached via a grounded theory methodology with literature investigation and in-depth interviews. This chapter positions the research question answers while next chapter discusses the limitations.

It is evident that CCs are exploited for ML purposes. Compared to the global size of crime and financial involvement, the role of CCs is relatively small in ML. However, the exact scope is not and cannot be precisely defined. Mainly the interviewees state a lack of regulation, which is confirmed by an absence of literature on regulation. Criminals may be reluctant to adopt CCs due to a lack of trust stemming from the infancy of the field. Full privacy CCs such as Monero and Zcash might provide criminals bigger benefits than Bitcoin, and are well suited for the placement step of the 3-step ML model. Stakeholders in scope are in the public, private, and public-private domain. Micro-, meso- and macro level stakeholders should be involved in the domains of criminology, law enforcement and information systems.

This research has several useful implications for the broader community. It provides scientists and decision makers with insights on the actual relationship between ML and CCs. These insights lead to opportunities to set research directions and resource allocation. Close attention should be paid to how CCs evolve and mainly Monero and Zcash are relevant to ML. Blockchain analysis tools are a field under heavy development and provide both investigators and law enforcement with powerful tools to analyse, detect and potentially prevent ML. CC exchanges should be regulated more tightly on a global level by one or more authorities which possess decision power to enforce regulations.

7. Discussion

With regards to the interviews, full data saturation on all levels is not reached because of a relatively low number of interviews. However, time and resource constraints as well as interviewee credibility justify this level of saturation. Bias can be recognized in most interviewees due self-interest from the respondents. Especially the money launderer is likely to prefer downplaying his actions over revealing true knowledge. Interviews are replicable because a standardized question list was used, but a standard prompt and probing list would strengthen replicability. No respondent validation took place which reduces conclusion validity.

In general the chosen method is considered as appropriate because of three reasons: (1) the infancy of the field, (2) the need for insights which can guide future research and resource allocation, and (3) the availability of described sources. The generalizability of conclusions is bound by temporal and spatial considerations due to the background of interviewees and nature of the literature. Appropriateness of the chosen method combined with the credibility of interviewees and literature strengthen this study's validity.

Acknowledgements

Special thanks are given to the interviewees for their participation. The supportive coaching from professors at the University of Amsterdam steered this investigation towards a coherent whole.

Bibliography

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., et al. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *2014 IEEE Symposium on Security and Privacy* (pp. 459-474). IEEE.

Bitsch, V. (2005). Qualitative Research : A Grounded Theory Example and Evaluation Criteria. *Journal of Agribusiness*, 75-91.

Decker, C., Wattenhofer, R. (2014, September). Bitcoin transaction malleability and MtGox. In *European Symposium on Research in Computer Security* (pp. 313-326). Springer, Cham.

Kollewe, J. (2017, December 4). *Bitcoin: UK and EU plan crackdown amid crime and tax evasion fears*. Retrieved December 6, 2017, from The Guardian: https://www.theguardian.com/technology/2017/dec/04/bitcoin-uk-eu-plan-cryptocurrency-price-traders-anonymity

Kyodo, J. (2017, November 30th). *170 money-laundering cases in Japan involved cryptocurrency in six months since April*. Retrieved December 6, 2017, from The Japan Times: https://www.japantimes.co.jp/news/2017/11/30/national/crime-legal/police-say-170-cryptocurrency-laundering-cases-suspected-six-months-april/#.Wigi9bOnGHs

Low, J. (2017, March 12). *Money Laundering*. Retrieved December 6, 2017, from Anti-money laundering and countering the financing of terrorism: https://aml-cft.net/library/money-laundering/

Masciandaro, D. (1999). Money laundering: the economics of regulation. *European Journal of Law and Economics*, 225-240.

Ministerie van Veiligheid en Justitie. (2015). *Misdaadgeld, witwassen en.* Den Haag: Boom Juridische uitgevers.

Ministerie van Veiligheid en Justitie. (2016). *Cybercrime en Witwassen.* Den Haag: Boom Juridische uitgevers. Retrieved December 11, 2017 from Ministerie van Veiligheid en Justitie: https://www.wodc.nl/onderzoeksdatabase/2540-criminele-dienstverlening-op-internet.aspx

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

Renner, P. (2017). *What is Money Laundering? The Three Stages in Money Laundering….* Retrieved December 9, 2017, from KYCMap: http://kycmap.com/what-is-money-laundering/

Schneider, F. (2008). *Money laundering and financial means of organized crime: some preliminary empirical findings.* Global Business and Economics Review.

The U.S Department of Justice. (2016, January 29). *Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business*. Retrieved December 7, 2017, from The United States, Department of Justice: https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital

Trautman, L. (2013). Virtual Currencies: Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox. *Richmond Journal of Law and Technology*, 2014.

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM, 58*(9). 104-113.