

How to combat money laundering in Bitcoin?

An institutional and game theoretic approach to anti-
money laundering prevention measures aimed at Bitcoin

David Bååth
Felix Zellhorn

Handledare: Göran Hägg
Examinator: Peter Andersson

Titel:

How to combat money laundering in Bitcoin?
An institutional and game theoretic approach to anti-money laundering prevention measures aimed at Bitcoin.

Författare:

David Bååth
Felix Zellhorn

Handledare:

Göran Hägg

Publikationstyp:

Masteruppsats i Nationalekonomi
Internationella Civilekonomprogrammet
Avancerad Nivå, 30 Högskolepoäng
Vårterminen 2016
ISRN-nummer:
Linköpings Universitet
Institutionen för ekonomisk och industriell utveckling (IEI)
www.liu.se

Abstract

Money laundering is a growing issue which has in later years emigrated more and more to the digital sphere of Bitcoin. Its pseudonymous nature and unrigorous legal definition has made regulation a difficult challenge. This thesis provides a unique take on the Bitcoin money laundering problematique by using incentive structures in place of forced restrictions. The goal is to create, validate and analyze a game theoretic incentive model which aims to combat money laundering by increasing the transaction costs for money laundering Bitcoin users without affecting the transaction costs for the honest users. The results prove the model to be feasible, leading to the conclusion that its real-world application has the potential to combat money laundering in Bitcoin to a significant degree.

Acknowledgements

We would like to thank our supervisor Göran Hägg, for his dedication and help throughout the entire process of writing this thesis. His inspiration and constructive criticism helped us to continuously increase the quality of this paper.

We would also like to express our gratitude toward Jonathan Jogenfors who provided us with all the technological expertise we needed to grasp the concept of Bitcoin. Furthermore, we would also like to thank him for inspiring us to choose this particular topic.

Furthermore, we would like to thank all interview respondents, without their qualified answers we would not have been able to be complete this thesis. Lastly, we thank our seminary group for their competent feedback throughout the process of writing this thesis.

David and Felix Zellhorn
Linköping, May 26 2016

Table of Contents

1. Introduction	1
1.1 Background & Problem Discussion.....	1
1.2 Purpose	2
1.3 Research questions	3
1.4 Execution	3
1.5 Restrictions	3
1.6 Research Contributions	4
2. Reference frame	5
2.1 The Definition of Transaction Costs.....	5
2.2 The Problem with Money Laundering	5
2.3 The Bitcoin System.....	8
2.3.1 A brief history.....	8
2.3.2 Bitcoin transactions.....	8
2.3.3 The blockchain.....	9
2.3.4 The creation of bitcoins	10
2.4 Bitcoin's Role in Money Laundering.....	10
2.5 Whom to Regulate?	12
2.6 Anti-Money Laundering Regulation in Bitcoin Today.....	14
3 Method.....	16
3.1 Scientific Approach.....	16
3.2 Data Collection	17
3.2.1 Interviews.....	17
3.2.2 Interview sample	17
3.2.3 Interview preparation.....	21
3.2.4 Interview execution	22
3.2.5 Secondary sources	22

3.2.6 Reference Guide	23
3.3 Ethical Statements	23
3.4 Criticism	24
3.4.1 Reliability	24
3.4.2 Validity.....	24
3.4.3 Source criticism	24
3.4.4 Method criticism	26
4 The Bååth-Zellhorn Model.....	27
4.1 Illustrating the Problem	27
4.1.1 Assumptions of preferences	29
4.2 Solving the Problem	31
4.2.1 Explanation of actions and strategies	32
4.2.2 Assumption of preferences	33
4.2.3 Playing the game	34
4.2.4 General concepts of the <i>separation game</i>	35
4.3 Confirming the Solution.....	37
4.4 Criticism on the Model.....	38
5 Empirical Evidence, Results and Analysis.....	40
5.1 Incentives.....	40
5.1.1 Presentation of the empirical findings	40
5.1.2 Empirical findings analyzed and applied to the model	41
5.2 Practicality.....	44
5.2.1 Presentation of the empirical findings.....	44
5.2.2 Empirical findings analyzed and applied to the model	46
5.3 Technicality	48
5.3.1 Presentation of the empirical evidence.....	48
5.3.2 Empirical findings analyzed and applied to the model	49

5.4 Interpreting the Results	50
6 Discussion	52
7 Conclusion.....	55
Sources.....	56
8 Appendix.....	62
8.1 Extensive Games.....	62
8.2 Signaling Games.....	64
8.3 Repetitive Games	66
8.4 Interview Questions	70
8.5 Interview Guides Sent to Bitcoin Traders.....	76

Table of Figures and Formulas

Figure 1 - The suboptimal equilibrium game	28
Figure 2 - The optimal equilibrium game.....	30
Figure 3 - The separation game	32
Figure 4 - The general separation game	35
Figure 5 - The long-run stability game	38
Figure 6 - The extensive game	63
Figure 7 - The signaling equilibrium game.....	65
Figure 8 - The prisoner's dilemma game.....	67
Figure 9 - The infinitely repeated prisoner's dilemma game	69
Formula 1 - The general formula	68
Formula 2 - The concrete formula.....	68

Conceptual Definitions

Bitcoin	The system/network.
bitcoin	Units of currency.
Bitcoin traders	Financial institutions that offer the service to exchange bitcoin for fiat-currency (or gold) and vice-versa.
Bitcoin users	Individuals using bitcoin as a payment method.
Block	A digital ledger that permanently registers transactions made in Bitcoin. A block is a history of all transactions not yet registered in precedent blocks. ¹
Blockchain	Is a publicly distributed database over all transactions made in the Bitcoin system, connecting all computer (nodes) in use to enable bitcoin transactions. ²
Digital currency	An Internet-based medium of exchange that exhibits properties similar to physical currencies, but allows for instantaneous transactions and borderless transfer-of-ownership. ³
ECA	Economic Crime Authority (Ekobrottsmyndigheten) is a Swedish government agency organized under the Ministry of Justice, with the mandate to investigate and prosecute financial crimes. The agency primarily focus on serious economic crime, with a special emphasis on investigating crime in the financial market and recovering the proceeds of crime. ⁴

¹ D.L. Chuen, *Handbook Of Digital Currency. Bitcoin, Innovation, Financial instruments, And Big Data*, USA, Academic Press, 2015.

² D.L. Chuen.

³ P. Tasca, *Digital Currencies:Principles, Trends,Opportunities, and Risks*, 2015. Available from: SSRN, (accessed 10 May 2016).

⁴ Ekobrottsmyndigheten, [Om Oss](#), 3 March 2014, (accessed 10 May 2016)

Fiat currency	Currency distributed by a central bank, deciding its value and enabling its usage as a payment method for goods and services as long as individuals trust their central entity. ⁵
FIU	Financial Intelligence Unit (Finanspolisen) is a central national agency with the purpose to inform about and combat money laundering. The FIU follows its national laws, but is closely intertwined with the European laws to facilitate a cooperation between the European countries. ⁶
FSA	Financial Supervisory Authority (Finansinspektionen) is a Swedish government agency responsible for financial regulation in Sweden. It is responsible for the oversight, regulation and authorization of financial markets and their participants. ⁷
Miner	Agents on the market that mine.
Mining	Verification of transactions in the Bitcoin system through users solving mathematical problem. Users get rewarded bitcoins for solving these problems. ⁸
P2P network	Peer-to-Peer networks allow online users to connect their computers to each other without the usage of a central server. This kind of network is often used in file-sharing. ⁹

⁵ G. Mankiw, *Brief Principles of Macroeconomics - 7th edition*, USA, Cengage Learning, 2014.

⁶ Rikskriminalpolisen, [Årsrapport Finanspolisen 2009](#), 6 July 2010.

⁷ Finansinspektionen, [Vårt Uppdrag](#), (accessed 10 May 2016)

⁸ D.L. Chuen, *Handbook Of Digital Currency*.

⁹ M. Rouse, [What is Peer-to-Peer?](#), August 2014, (accessed 10 May 2016)

1. Introduction

1.1 Background & Problem Discussion

Money laundering is a transnational, institutional and regulatory problem that makes out the dark side of the financial world. In 1998 Michel Camdessus, Managing Director of the International Monetary Fund (IMF), roughly estimated that money laundering amounted to about 2-5% of global GDP, or \$800 billion-\$2 trillion US dollars.¹⁰ United Nation Office on Drugs and Crime (UNODC), in a report published in 2009, found a similar estimate that varied around the 3% mark and also found that “less than 1% of global illicit financial flows are currently seized and frozen”.¹¹ Through the eyes of a government this entails a loss of taxes, for companies it shows unfair competitive advantages and for consumers it signifies unjust behaviour. But from the perspective of transaction cost theory these numbers show something that is arguably even more severe: transaction costs are low in the criminal world as a consequence of the prevalent money laundering taking place, giving dishonest actors incentives to circumvent the law.¹² But before asking the question of how to combat money laundering, perhaps the first question should be: What is causing it?

One viable answer is embedded in the globalization and technological advancement that has shaped the world these past few decades. For all the good that open-borders and online-bank transfers have given us, it has also given criminals a whole new playing field in which to transfer and conceal illicitly gained money, allowing them to lower the transaction costs of crimes. Controlling the hundreds of billions of transnational transactions that take place yearly all over

¹⁰M. Camdessus, [Money Laundering: The Importance of International Countermeasures](#), [website], 1998 (accessed Web. 11 Apr. 2016.)

¹¹ T. Pietschmann, et al., [Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes](#), United Nations Office on Drugs and Crime (UNODC), [website], 2011, p.5 (accessed 12 March 2016)

¹² [Money Laundering Impacts Development](#), The World Bank, 2003. See section A-3. (accessed 26 April 2016)

the world has proved to be difficult to say the least. This challenge has been made potentially more difficult with the gaining momentum of a technology named Bitcoin.¹³

This decentralized, digital currency was created for the purpose of allowing people to transact money cheaply, globally and anonymously, within a framework that is self-regulatory, so that it does not have to rely on any third-party.¹⁴ Though these inherent attributes are appealing to the standard, law-abiding, Bitcoin user, they are invaluable for a less lawful user with the intent to conceal the true origin of the money. There is Anti-Money Laundering (AML) regulation in place today to combat this risk opened up by Bitcoin, but as it creates a barrier for the dishonest, it does the same for the non-money laundering users as well. And herein lies the problem. The high transaction costs imparted on the dishonest users through AML directives, are to some extent also affecting the honest users. Conversely, the low transaction costs enabled by Bitcoin are not only imparted on the honest users, but on the dishonest users as well. A balance between these transactional costs needs to be reached in order to effectively combat money laundering, while taking into account the differing incentives that will be at play in any regulation aimed at Bitcoin.¹⁵

1.2 Purpose

This thesis seeks to create, validate and analyze around a game theoretic incentive model which aims to combat money laundering by increasing the transaction costs significantly for the money launderer without imparting additional transaction costs on the honest user. The model will be built in three parts; a sequential game illustrating the potential pitfalls that any AML regulation has to overcome, a signaling game solving the posed problem and lastly a prisoner's dilemma game confirming its long-term sustainability.

¹³ [Number of Worldwide Non-Cash Transactions for North America, Europe, Mature APAC, Latin America, CEMEA and Emerging Asia in 2012, 2013 and 2014E](#), [website], 2015. (accessed April 12 2016).

¹⁴ S. Nakamoto, [Bitcoin: A Peer-to-Peer Electronic Cash System](#), [website], 2008. (accessed 28 March)

¹⁵ M. Yeandle et al, [Anti-money Laundering Requirements : Costs, Benefits And Perceptions](#), [website], 2005, (accessed 5 April 2016)

1.3 Research questions

Can an incentive model combat money laundering in Bitcoin?

Can such an incentive model be realistically implemented?

1.4 Execution

A game theoretic incentive model will be created with the purpose to combat money laundering and solve for the transaction cost problems that come with it. The feasibility of the model will be tested through the use of empirical data which will be collected through ten semi-structured interviews with state authorities, Bitcoin traders and various Bitcoin experts. This data will be complemented with secondary sources consisting of electronic articles and educational literature.

1.5 Restrictions

The tool used to put the problem of money laundering into an institutional perspective will be restricted to transaction cost theory. The creation of the model will be made up out of three theoretical components found in game theory, namely; sequential games, signaling games and infinitely repeated games.

Although technical information will be provided in the form of a short background on Bitcoin and a short overview of the technical feasibility of the model, an economic point of view will still be the focus of this thesis. Technical details will only be explained thoroughly enough to further the discussion from an economic standpoint and provide a good foundation for the analysis. The juridical information provided in this thesis follows the same logic, with the explanation of relevant law being in depth enough to allow a useful economic discussion.

Another restriction this thesis chooses to follow, is to combat money laundering in Bitcoin, without hindering the technological innovation of Bitcoin.

1.6 Research Contributions

Bitcoin is a relatively young phenomenon which is why many questions about it are yet unanswered, the topic of this research included. As far as is currently known, there is not yet a standardized incentive model that aims to combat money laundering. Answering this research question opens up for a wide variety of utility for Bitcoin and other cryptocurrencies. This paper distinguishes itself from previous work by answering how incentives need to be changed in order to counteract upon money laundering in Bitcoin. As well as providing practical solutions as to how these incentives need to be changed. This study is to be considered a pioneer work as in how AML regulations need to be adapted in order to solve the transaction cost problem caused by money laundering.

2. Reference frame

2.1 The Definition of Transaction Costs

Throughout the entire thesis, transaction costs are used as an analyzing tool to distinguish the different incentives of the players on the market. This thesis will lean its interpretation and usage of the term “transaction costs” on the work of Williamson, and Groenewegen, Spithoven and Van den Berg.¹⁶ In this thesis, transaction cost will be the collective term for any factor which obstructs, prevents or makes transactions between two parties more costly.

Several types of transaction costs will be presented, all based on their utility for the model and its analysis. These costs can be the trouble one has to go through to seek information about a desired product. Another transaction cost this thesis will include are integration costs, integration costs occur when anonymity is lost due to new regulations. The next transaction cost is called screening cost, which is the cost for someone to confirm that their business partner is reliable and legitimate. The cost of a diminished reputation is also defined as a transaction cost in this thesis.

This thesis further assumes that all actors on the market are rational and thus strive after minimizing their own transaction costs as much as possible.

2.2 The Problem with Money Laundering

A decrease in transaction costs leads to an increase in welfare, this knowledge was already brought to us by Smith and Ricardo with the theory of comparative advantages. Since then, many theories have been crafted to perfectionize the diminution of transaction costs in the

¹⁶ O. Williamson, *Markets and Hierarchies*: The Free Press, New York, 1975, J. Groenewegen, et al, ‘Institutional Economics: An Introduction’, Basingstoke, Palgrave Macmillan, 2010.

world.¹⁷ Money for example diminishes transaction costs greatly by being a storage for value as well as an exchange medium.¹⁸ Through globalization and a developing technology, money transfers can be made instantly and globally, from anywhere to anywhere, resulting in very low transaction costs for transfers of value.

There is however a downside to these diminished transaction costs, which comes in the form of illicit or politically unwanted transactions, facilitated through globalization and its technology. The low transaction costs of transfers are thus abused for the concealment of illicitly received funds, obtained through criminal activities; called money laundering. Laundering illicit money causes various problems to the governments, for example by financing terrorists, creating corrupt front companies or infiltrating politics.¹⁹

Money laundering is usually divided into three different stages; placement, layering and integration. Placement is the step where illicit funds of any kind are being introduced into the legal financial system without being revealed by legal authorities. Illicit money can be either primarily or secondarily deposited, with the former being the direct way of infiltration into legal accounts. This can be done either by dividing sums into smaller sub sums and by doing so avoiding restrictions of deposit limits, or by using corrupt employees of banks, using bribery to pass legal restrictions. Secondary deposits are hence an indirect way of infiltrating illicit money into a legal system, either by using a medium to convert the illicit money into assets, or by the use of third parties, this can be self-owned companies introducing black money into the legal banking system through their accounts. During the placement stage money launderers are most vulnerable to being discovered by legal authorities.²⁰

The second step, called layering, describes the phenomenon of transferring ill-gotten money around, to conceal the true origin of the funds, making them look legitimate. This is often done by fictional purchases of goods or fictional loans to other accomplices. Electronic transferring opened up for wide possibilities to do layering on an international scale, making it far easier to

¹⁷ J. Baeten and F. Den Butter, *Welfare gains by reducing transaction costs: Linking trade and innovation policy*, 2006.

¹⁸ H. Ekstedt *Money in Economic Theory*, Routledge, London, 2015.

¹⁹ [Money Laundering and Terrorist Financing: Definitions and Explanations](#), World Bank, [website], 2003. (accessed 17 February 2016).

²⁰ F. Schneider and U. Windischbauer, "Money Laundering Some Facts", *Economics of Security Working Paper 25*, 2008.

camouflage the true origin of the money. Dividing the total sum, then investing them into advanced foreign assets to exploit political inability of cooperation.²¹

The final stage of money laundering is integration where the illicit money goes back to its originator and if the launderer was successful, without traces of suspicion as to where the money came from, due to the previous phases. Often assets such as real estate or luxury goods are purchased with this money, to minimize the chance of raising suspicion.²²

To combat illicit transactions, governments have created regulations and anti-money laundering directives to increase the transaction costs of politically unwanted transactions, without distorting the gained welfare for regular transactions.²³ Several methods are in place to combat money laundering, one method that proved effective is the “know your customer” policy, henceforth referred to as KYC. As the name indicates, the KYC policy aims to facilitate the identification of customers of financial institutions, often in institutions which act as intermediaries between buyers and sellers, for example banks. For individual customers, legal independent identification is required, as well as information about residency (addresses, nationality etc.) and a valid photograph to facilitate identification. If the customer is a legal person, the legal status of the business needs to be validated as well as the authority of the signatories and beneficial owners.²⁴

With Bitcoin, a new technology got introduced to the market, opening up for new possibilities on a globalized transaction market. However unwanted transactions within the Bitcoin system occur and need to, once again, be regulated in an effective way.²⁵

²¹ Schneider and Windischbauer.

²² Schneider and Windischbauer.

²³ [International Monetary Fund: Anti-Money Laundering/Combating the Financing of Terrorism](#), [website], (accessed 4 May 2016).

²⁴ KYC, [Standard Chartered Bank](#), 2016 [website], (accessed 2 March 2016).

²⁵ Elena Scherschneva, interviewed by Felix Zellhorn and David Bååth, 2016, Wiener Neustadt, Linköping

2.3 The Bitcoin System

2.3.1 A brief history

In the aftermath of the financial collapse of 2008, in what is now known as the Great Recession, a vast amount of economic value was lost through a banking crisis that expedited a house market crisis, a trade crisis and a sovereign debt crisis. Amongst the financial loss of the individual, there was also a loss of trust in banks and the government policies governing them. It was out of this growing mistrust that Bitcoin emerged as an alternative payment method, a decentralized electronic currency which would be controlled by rigorous mathematical equations rather than a government entity. In early 2009 the system went online after the publication of a paper explaining the intricate system. It was created and published, by a person or group, using the pseudonym Satoshi Nakamoto who detailed a peer-to-peer network²⁶ which would generate "a system for electronic transactions without relying on trust"²⁷. As of February 2016 the total net value of Bitcoin was roughly \$5.7 Billion and had an overwhelming market share of cryptocurrency, namely 94.5%.²⁸

2.3.2 Bitcoin transactions

A bitcoin is an electronically created and digitally held currency which can be transacted by anyone who has a bitcoin wallet; a specialized piece of software downloadable as an app or computer program that connects the user to the Bitcoin network. Bitcoins can be obtained in three ways; (1) in exchange for fiat currency, such as dollars or euro, through the use of private channels or bitcoin traders, (2) in exchange for goods and services, or (3) through the process of "mining" (which will be explained in detail in section 2.3.3).²⁹

Every transaction with bitcoins starts out with one user specifying a certain amount of bitcoins to be transferred to another user in the system. The bitcoin wallet of the receiver then generates a unique code consisting of alphabetic and numeric characters, to which payments can be received, akin to that of a bank account number. The sender puts in bitcoins at this unique

²⁶ A network which allows online users to connect their computers to each other without the usage of a central server.

²⁷ S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, p.8.

²⁸ D.L. Chuen, *Handbook of Digital Currency*.

²⁹ M. Tsukerman, *The Block is Hot: a Survey of the State of Bitcoin Regulation and Suggestions for the Future*, Berkeley Technology Law Journal, Vol. 30, 2015. Available from: SSRN, (accessed 23 February 2016).

address and confirms the payment by using a private key only he knows, while the receiver is able to take the bitcoins out from this address by using their own private key. Although the identity of every Bitcoin user is shrouded in a random sequence of numbers and letters, anyone on the network can see every transaction made from that random sequence, making Bitcoin a pseudonymous network more than an anonymous one.³⁰

This system of transacting cryptocurrency would be impossible to maintain if not for the self-regulating mechanism lying at the core of Bitcoin; namely the blockchain.

2.3.3 The blockchain

This piece of technology works as a shared public ledger in which every confirmed transaction ever made within the system is stored and allows every user to track how much value each Bitcoin user has had at any point in time. With every new transaction the entire blockchain is checked to make sure a certain bitcoin has not already been spent, this helps to counteract the so called “double-spending problem” where any user could spend the same bitcoin twice by simply copying it. The blockchain is not maintained by a third-party, but by “bitcoin miners”, individuals who lend their own personal computational power to regulate and keep the intricate system running. Going back to the metaphor of the blockchain being a ledger, every block can be seen as a new page containing all valid transactions since the last page was added, with a new page being created roughly every 10 minutes. Every Bitcoin miner is solving a difficult mathematical problem in order to be the first one to add the new page, thus creating a race where the winner is rewarded with bitcoins from the Bitcoin protocol.³¹ It is this incentive structure that keeps the Bitcoin network maintained, but also adds several important security measures. In order for a dishonest user to falsify one page, he would also have to rewrite every single page that came before at a speed that would have to be faster than all the honest users. For every page confirmation a transaction has, the harder it is to falsify. After six confirmed pages (60 minutes) the falsification is computationally impractical.³² If the dishonest user would manage to secure the vast amount of computational power necessary, he or she would earn more bitcoins from honest mining than deceitful falsification.³³

³⁰ D.L. Chuen, *Handbook of Digital Currency*.

³¹ D.L. Chuen.

³² [Frequently Asked Questions - Find answers to recurring questions and myths about Bitcoin](#), [website], 2016, (accessed 23 February 2010). See “Sending and receiving payments”.

³³ M. Tsukerman, *The Block is Hot*.

2.3.4 The creation of bitcoins

The bitcoins given as rewards to the miners are the sole inflow of new coins in the system. The amount gained from successfully solving a block is as of now 25 bitcoins, but is designed to halve every 210 000 blocks. With the underlying mathematics set to maintain a rate of one block solved each 10 minutes, the reward amount will be cut in half each four years until the last Satoshi (0,0000001 bitcoin) is mined in the year 2140. This will leave the Bitcoin system with a finite supply of approximately 21 million bitcoins.³⁴

2.4 Bitcoin's Role in Money Laundering

Bitcoin was partly created with low transaction costs in mind, which is reflected in many of its built-in features.³⁵ Although this claim is disputed, with Bol and Cerić pointing at high information and control cost,³⁶ Bitcoin's lack of intermediaries between buyers and sellers does make payments generally cheaper and processes transactions faster compared to that of fiat currencies.³⁷ However, these features have also provided transactional benefits to dishonest bitcoin users who aim to use the Bitcoin network for money laundering activities, where three features in particular play a big role in lowering the transaction costs for money launderers.³⁸

Firstly, the decentralized manner in which of Bitcoin is constructed enables users to transfer financial value to one another without a third-party being involved in the deal. As stated in a previous section, a main strategy in traditional anti-money laundering directives is to monitor the intermediaries who stand in between the buyers and sellers in the market, in order to limit the ability of criminals to transfer value without scrutiny.³⁹ The lack of intermediaries in Bitcoin makes the traditional approach impossible and the absence of face-to-face contact when transacting in bitcoins further complicates the identification process.⁴⁰

³⁴ D.L. Chuen, *Handbook of Digital Currency*.

³⁵ S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*

³⁶ S. Bol and A. Cerić, *Bitcoin - a sustainable means of payment? A transaction cost analysis of Bitcoin compared to traditional means of payment*, Master Thesis, Linköping University, 2014.

³⁷ D.L. Chuen, *Handbook of Digital Currency*.

³⁸ N. Ajello, *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, Brooklyn Law Review, Volume 80, Issue 2, Article 4, 2015.

³⁹ KYC, Standard Chartered Bank.

⁴⁰ D.L.Chuen, *Handbook of Digital Currency*.

Secondly, even though every transaction is stored and can be traced in the blockchain, there is no link to the individual or organization behind that transaction. Bitcoin's pseudonymous ecosystem only reveals the arbitrary sequence of numbers that is the public key while the private key is kept hidden, making the tying of a real-life identity to a Bitcoin address extremely difficult. This problem is further compounded by the ease of which a user can have several electronic wallets, giving them multiple public addresses which makes potential money laundering violations hard to investigate.⁴¹

Lastly, the speed and ease of which transactions can be carried out in Bitcoins makes it far superior to the traditional anonymous vehicle utilized to launder money, namely cash. Where traditional paper bills carry with it a physical limitation in the form of weight and size, bitcoins can be stored in the millions on a standard USB device and transacted to any user in the world within 10 minutes.⁴² The flexibility of the Bitcoin payment structure also makes it easier to circumvent regulatory measures by breaking down a transaction into smaller transactions.⁴³

As with money laundering in fiat currency, it is difficult to quantify how much money is actually laundered through Bitcoin. The FBI, European Banking Authority and the Financial Action Task Force of the G7, all acknowledge Bitcoin's role in the money laundering problem but cannot give any hard data.⁴⁴ According to the CEO:s of the Bitcoin traders ICE3X and Vaultoro, money laundering is not a significant problem and only a few suspicious instances could be recalled.⁴⁵ However, the Swedish Financial Supervisory Authority (FSA), Sweden's and Austria's Financial Intelligence Unit (S-FIU and A-FIU) and the Swedish Economic Crime Authority (ECA), all stated that money laundering does happen through Bitcoin, a statement Jonathan Jogenfors an expert on Bitcoin agrees with.⁴⁶

⁴¹ D.L. Chuen.

⁴² N. Ajello, *Fitting a Square Peg in a Round Hole*.

⁴³ N. Ajello.

⁴⁴ *Bitcoins Virtual Currency: Unique Features Present Challenges for Deterring Illicit Activity*, Cyber Intelligence Section and Criminal Intelligence Section (FBI), 2012, *Warning to consumers on virtual currencies*, European Banking Authority, 2013 and [*Guidance for a Risk-based Approach to Virtual Currencies*](#), Financial Action Task Force [website], 2015. (accessed 15 March 2016).

⁴⁵ Gareth Grobler, interviewed by David Bååth and Felix Zellhorn, 2016, Douglas, Linköping University and Joshua Scigala, interviewed by Felix Zellhorn and David Bååth, 2016, Berlin, Linköping University.

⁴⁶ Anonymous employee at the Swedish FIU, interviewed by David Bååth and Felix Zellhorn, Stockholm, Linköping and David Lothigius, interviewed by David Bååth and Felix Zellhorn, 2016, Linköping, Stockholm and Jan Tibbling, interviewed by David Bååth and Felix Zellhorn, 2016, Stockholm, Linköping and E. Scherschneva interview, 2016 and Jonathan Jogenfors, interviewed by Felix Zellhorn and David Bååth, 2016, Linköping, Linköping.

2.5 Whom to Regulate?

According to a paper published by Danton Bryans, controlling for all the aspects of Bitcoin would prove to be a near impossible task because of the complexity of the system. Focus should instead be given on each individual transaction entity in order to determine mainly two things; which entity in the Bitcoin system, if regulated, would impart the highest transaction costs for money launderers, without bearing unreasonably high transaction costs for the regulator and the regulated.⁴⁷

A potential money launderer will have to go through five core entities that makes up the system in order to disguise the true origin of the money. (1) a sender who initiates the transaction of Bitcoin derived from an illegitimate source; (2) a receiver who accepts the dirty bitcoins in order to obfuscate its source; (3) Bitcoin miners who verifies the transaction by completing a block; (4) the Bitcoin development team who keeps the Bitcoin system updated; and (5) Bitcoin traders who exchanges bitcoins for various types of fiat currency and vice versa.⁴⁸ What follows are arguments for and against regulations of the five entities.

(1) The Senders

The pseudonymous and disperse nature of users sending their bitcoins over the network, would likely make regulation unfeasible and not lead to any increased transactional costs for money launderers. No personally identifiable information is interchanged when a transaction is carried out between two users, which makes connecting the dots between a Bitcoin address and a real-life individual extremely difficult.⁴⁹ Furthermore, government regulation of Bitcoin users would most likely see heavy pushback from the community itself, since non-government involvement was one of the key reasons for Bitcoins establishment.⁵⁰ This highly probable opposition in conjunction with an identity cloaked user base would make the cost of such a regulatory implementation outweigh its benefits.⁵¹

⁴⁷ B. Danton, *Bitcoin and Money Laundering: Mining for an Effective Solution*, Indiana Law Journal: Vol. 89: Iss. 1, Article 13, 2014.

⁴⁸ B. Danton.

⁴⁹ D.L. Chuen, *Handbook of Digital Currency*.

⁵⁰ S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*.

⁵¹ B. Danton, *Bitcoin and Money Laundering*.

(2) The Receivers/Launders

Directing focus on the users of the receiving end would allow for a more targeted enforcement on those acting with clear criminal intent, while staying clear of the potential opposition that regulation of the senders would entail. But the problem of pseudonymity would yet again hinder the identification of such intent and law enforcement would have to spend vast amount of resources for miniscule benefits. The result would be the same as with *senders*.⁵²

(3) Miners

The system is built so bitcoin miners have no interaction with the users whose transactions they verify, and vice versa. This makes regulation of miners unnecessary and focus should be put elsewhere.⁵³

(4) Bitcoin Development Team

With Bitcoin being an open-source software, forcing a change on the central authority figure would not garner much results. The development team takes on the role of a standard agency, constantly improving the software but unable to force a change without the complete consensus of its users. Anyone can choose to use any previous version of the software, so an unfavorable change in the Bitcoin protocol would not be adopted.⁵⁴ It is therefore highly improbable that any regulation put on the development team would have any effect on the transactional cost of money launderers.⁵⁵

(5) Bitcoin traders

Most Bitcoin currency exchanges deal in both fiat currency and bitcoins while functioning as a value holder between buyers and sellers. This makes them easily classified as money transmitting intermediaries, making them applicable for standard money transmitter and

⁵² B. Danton.

⁵³ B. Danton.

⁵⁴ *Frequently Asked Questions - Find answers to recurring questions and myths about Bitcoin*, 2016. See “Who controls the Bitcoin network?”.

⁵⁵ B. Danton, *Bitcoin and Money Laundering*.

money exchange laws. These classifications make it easier to apply regulation without ending up in legal grey areas. Furthermore, Bitcoin traders are of a less decentralized and less anonymous nature than the other core entities discussed previously, so regulation of Bitcoin currency exchanges would likely show the greatest benefits for the least costs.⁵⁶ Also, since the Bitcoin traders are a vital part of the integration phase in the money laundering process, regulation has good potential of increasing the transactional cost of money launderers.⁵⁷

2.6 Anti-Money Laundering Regulation in Bitcoin Today

Regulation in Bitcoin varies greatly between regions, with some countries imposing strict requirements, some not regulating at all and some having banned Bitcoin altogether. As will soon become apparent, the regulation that is in place is almost exclusively focused on Bitcoin traders and usually mimics the regulation found in most banks.

In Europe, all Bitcoin traders are forced to follow the third Anti Money Laundering Directive put in place by the European Commission, due to them being classified as money transmitting intermediaries. The directive includes three main regulatory requirements, namely: to identify and verify the identity of their customers and of the beneficial owners of their customers, as well as monitoring their transactions; to report suspicions of money laundering or terrorist financing to the public authorities and; to take supporting measures, such as ensuring the proper training of personnel and the establishment of appropriate internal preventive policies and procedures.⁵⁸

In the US, there is no federal regulation governing Bitcoin, but varying regulatory policies in each state. For example in the State of New York a concept called Bitlicense has been implemented as a way to strengthen the regulation on Bitcoin traders.⁵⁹ The Bitlicense is a business license that entails stricter AML directives, which every trader who wants to do business in the state has to pay for. A cost which caused some traders to leave the New York

⁵⁶ B. Danton.

⁵⁷ [Guidance for a Risk-based Approach to Virtual Currencies](#), Financial Action Task Force, 2015. (accessed 15 March 2016). See paragraph 20, 28, 40 and 63.

⁵⁸ [Frequently asked questions: Anti-Money Laundering](#), European Commission, Press Release Databank, [website], 2013. (accessed 18 April 2016).

⁵⁹ [Regulations Of The Superintendent Of Financial Services Part 200. Virtual Currencies](#), New York State Department of Financial Services, [website], 2015, (accessed 15 April 2016).

market.⁶⁰ In California regulation only forces traders to have bank-style reserves in the event of possible losses⁶¹, while North Carolina is only in the process of pushing forward Bitcoin regulation bills, with no current directives in place.⁶²

The vast majority of South American, African and Asian countries have either no Bitcoin regulation in place or have outright banned the digital currency. In Oceania, New Zealand has currently no regulation in place while Australia only has regulation governing taxes.⁶³

It is difficult to find concrete proof of the effectiveness of the Bitcoin regulation that is in place today. But with the Swedish and Austrian FIU, the Swedish FSA, the Swedish ECA and a Bitcoin Expert saying that money laundering does happen in Bitcoin to a significant scale, the current regulation can be deemed imperfect.⁶⁴

⁶⁰ M. Castillo, [*The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem*](#), New York Business Journal, August 12, 2015). (accessed 6 May 2016).

⁶¹ [*California Legislature— 2015–2016 Regular Session. AB-1326 Virtual currency*](#), Introduced by Assembly Member Dababneh, February 27, 2015. (accesses 3 May 2016).

⁶² [*North Carolina considers law to regulate virtual currencies*](#), Associated Press, May 25 2016. (accessed 25 April 2016).

⁶³ [*Is Bitcoin legal?*](#), Coindesk, 19 Augusti 2014, (accessed 25 April 2016).

⁶⁴ Interview with anonymous employee at the Financial Police of Sweden, 2016; Interview with David Lothigius, 2016; Interview with Jan Tibbling, 2016; Interview with Elena Scherschneva, 2016; Interview with Jonathan Jogenfors, 2016.

3 Method

After distinguishing the problems caused by money laundering activities through an institutional framework, this paper aims to present a feasible solution to combat money laundering specifically designed for Bitcoin. Game theory serves as a powerful tool to observe and analyze incentives, which is why this paper invents several game theoretical models, aiming to create incentives to prevent money laundering from being attractive. The feasibility of the aforementioned model will be thoroughly scrutinized by previous theoretical framework as well as interviews with experts in their respective fields.

3.1 Scientific Approach

To seek validation for the presented model, this paper aims to solve three different problems the model has to overcome. The problem derives down to its feasibility in different aspects, those aspects are as follows:

(1) Incentive

(2) Practical

(3) Technical

(1) The cornerstone of the model is the feasibility of the incentive structures. The incentives created by the model must comply with the desired outcome, otherwise the model does not hold. By interviewing Bitcoin traders, financial state authorities and Bitcoin experts, a broad knowledge on the players' preferences was obtained to balance incentive structures between the different players in the system.

(2) The second issue that is being scrutinized is if the model is practically feasible, meaning if governmental entities and Bitcoin traders would consider the solution viable. This paper controls if the given incentives can practically aid in combating money laundering, as well as controlling to what degree the provided additional information is helpful. In order to solve for

the practical problems, an interview with the Swedish and Austrian FIU was conducted, as well as interviews with the Swedish FSA. Interviews with Elena Scherschneva and David Lothigius at their representative departments strengthen the argument of the practicality of this model. The interview with Emil Elgebrant and his insightful juridical expertise also helped to prove the model right in practical and juridical aspects.

(3) The last issue the signaling game model has to overcome are the technical issues bound to follow in a reward system. Jonathan Jogenfors Ph.D. candidate at the LiU and an expert in the technical field of Bitcoin, gave helpful insights into the technical details of the cryptocurrency. Furthermore, previous studies on the matter completed the technical knowledge required to make the signaling game feasible in the technical department.

3.2 Data Collection

3.2.1 Interviews

Collecting empirical evidence from interviews is highly suitable when dealing with new phenomena and complex assumptions.⁶⁵ With the central model of this thesis fulfilling this criterion, interviews were carried out with respondents who were judged to have relevant knowledge about the model's feasibility. The interviews were chosen to be semi-structured, thus leaving the respondent space to evolve his or her thoughts to the corresponding question without losing track of the objective behind the interview. The semi-structure of the interview also facilitates the replication of the study, since all questions asked in the interview are precisely documented and obtainable in the appendix. Following the advice of Bryman semi-structured interviews also allow for thoughts to be heard that otherwise would not have been brought up by the interview questions.⁶⁶ Since this paper seeks professional validation to a new model, opinions "outside" the box may prove to be of utmost value to the model.

3.2.2 Interview sample

Since the model deals with three conflicts of interest between three players (the state, the traders and the users), whom must all align in order for the model to hold, interview subjects

⁶⁵ M. Descombe, *Ground Rules for Social Research: Guidelines for Good Practice*, Open University Press, 2009.

⁶⁶ A. Bryman, *Social Research Methods*, Oxford and New York, Oxford Press, 2008.

were chosen based on their representativeness of these players. Interviews with an anonymous employee at the Swedish FIU and David Lothigius at the FSA were conducted to provide information about the interests and incentives from the state's perspective, as well as to gain insight into the money laundering problematique. Establishing the incentives of traders was done through interviews with four Bitcoin traders who resided in various geographical regions. Answers determining the incentives of Bitcoin users were gathered indirectly from all 8 interviewees since they all had hands on knowledge about the Bitcoin user base. Beyond the scope of incentives, an expert of Bitcoin and cryptography, Jonathan Jogenfors, was chosen to provide information about the technical feasibility of the model. Emil Elgebrandt, a doctor of juridical science, well versed in the juridical matter surrounding Bitcoin, was chosen to give insight into the practicality of the model.

What follows below is information about each interview respondent, detailing their expertise in their respective fields. The interviewees can be divided into three groups of interest, namely; state authorities, Bitcoin traders and experts.

State authorities

Name	Organization	Occupation	Place	Date
Anonymous	The Swedish Financial Intelligence Unit		Stockholm	22/04 2016

An employee at the Swedish FIU who has experience working with money laundering and other financial crimes. Having worked many years for the FIU, the respondent is deemed to be representable for the organization as a whole.⁶⁷

Name	Organization	Occupation	Place	Date
Jan Tibbling	Swedish Economic Crime Authority	Prosecutor	Stockholm	28/04 2016

⁶⁷ The Swedish FIU interview, 2016.

Jan Tibbling works as a prosecutor for the Swedish Economic Crime Authority. He is an expert at both Bitcoin and money laundering, making him a very viable subject to interview. He has now worked for the Swedish economic crime authority for 12 years.⁶⁸

Name	Organization	Occupation	Place	Date
David Lothigius	Financial Supervisory Authority	Lawyer	Stockholm	18/04 2016

David Lothigius is a lawyer at the FSA, specialized in payment, financial and credit institutions. He worked with preventing money laundering regulations for a couple of years.⁶⁹

Name	Organization	Occupation	Place	Date
Elena Scherschneva	Austrian Financial Intelligence Unit	Head of the A-FIU	Wiener Neustadt	22/04 2016

Elena Scherschneva has worked as the head of the Austrian Financial Intelligence Unit (A-FIU) for four years. Before attaining her current position, she was a criminal police officer for four years and also worked at a crime unit which dealt with internationally organized crime, where the problem of money laundering was a part of the agenda.⁷⁰

Bitcoin traders

Name	Organization	Occupation	Place	Date
Gareth Grobler	ICE3X	CEO of ICE3X	Douglas	14/04 2016

⁶⁸ J. Tibbling, interview, 2016.

⁶⁹ D. Lothigius, interview, 2016.

⁷⁰ E. Scherschneva interview, 2016.

Gareth Grobler is the owner and CEO of ICE3X, a South African online Bitcoin exchange platform founded in 2013. ICE3X trades mostly in South African Rand and Nigerian Naira, thus being a platform for the African market, it however also offers trades in Sterling and US dollars.⁷¹

Name	Organization	Occupation	Place	Date
Joshua Scigala	Vaultoro	CEO of Vaultoro	Berlin	15/04 2016

Joshua Scigala is, together with his brother, a co-founder of Vaultoro, a Bitcoin trader specialized in trading bitcoins for physical gold. Vaultoro was founded in 2015 by the two brothers who both have a wide expertise in technology and the gold industry.⁷²

Name	Organization	Occupation	Place	Date
Anonymous 1	Anonymous trader	Client Engagement	Halifax	20/04 2016

Name	Organization	Occupation	Place	Date
Anonymous 2	Anonymous trader	Legal Counsel on regulatory compliance matters	London	25/04 2016

Experts

Name	Organization	Occupation	Place	Date
Jonathan Jogenfors	Linköping Universitet	Ph.D candidate in information coding	Linköping	19/04 2016

⁷¹ G. Grobler interview, 2016.

⁷² J. Scigala, [About the Founders](#), (accessed 24 April 2016).

Jonathan Jogenfors is a Ph.D candidate in information coding at the Linköping University, he is currently occupied working on time-energy entanglement applied to quantum key distribution. His background in cryptography makes him especially capable in providing information about cryptocurrencies such as Bitcoin.⁷³ He also helps combating money laundering in Bitcoin in cooperation with the Swedish FIU.⁷⁴

Name	Organization	Occupation	Place	Date
Emil Elgebrant	Linköping University	Jur. dr. in Private Law	Linköping	21/04 2016

Emil Elgebrant is a Jur. Dr. in Private Law currently researching and teaching at the Linköping University, his main focus is legal issues arising from the introduction of new property items, such as Bitcoin.⁷⁵ Elgebrant also recently published a book on cryptocurrencies.⁷⁶

3.2.3 Interview preparation

An interview guide was sent by e-mail to all Bitcoin traders and experts, asking if they were willing to participate in an interview. The guide included a short explanation of the purpose of the thesis, an estimation on the duration of the interview and information regarding the choice to remain anonymous. The state authorities were contacted by phone but were provided with essentially the same information as found in the e-mail. The interview questions were sent if asked for, which had the perk of possibly increasing the quality of the answer but the drawback of losing the spontaneity factor.⁷⁷

All Bitcoin traders were provided with the same interview guide and asked the same questions during the interview, as to assert that differing answers among traders were not the cause of a different interview layout. Same logic was applied to the interviews with the Swedish FSA and the FIU who both received the same questions. For the interviews with Jonathan Jogenfors and

⁷³ J. Jogenfors, [Cryptographic currencies: Bitcoin, Litecoin etc.](#), [website], (accessed 10 May 2016).

⁷⁴ J. Jogenfors interview, 2016.

⁷⁵ E. Elgebrant, [Emil Elgebrant](#), 7 April 2016, (accessed 10 May 2016).

⁷⁶ Emil Elgebrant, interviewed by Felix Zellhorn and David Bååth, 2016, Linköpings University, Linköping.

⁷⁷ See appendix 8.4 to view all interview questions.

Emil Elgebrant, unique interview questions were created as to be more tailored to their respective expertise. The layout of all interviews was structured as to first reveal background information about the level of expertise and experience of the respondent regarding the subject of Bitcoin money laundering, followed by more in depth questions. For traders, these questions revolved around their professional opinions about their current AML-directives, ending with questions surrounding the Bitcoin user base. For the rest of the interviewees, the in depth questions dealt with the problem of money laundering and regulation in broader strokes, with Jogenfors being asked more technical questions, Elgebrant more judicial ones, while the state authorities helped to put it all into a greater context. This layout was adopted to create a more natural flow in the interview dialogue, increasing the chances of well-thought out answers and reliable data.

3.2.4 Interview execution

10 interviews were conducted altogether; two in person, three through phone, four through Skype and one by e-mail. The location and manner in which the interviews were conducted were decided by the interviewees themselves, since this incites comfort and security in the respondent.⁷⁸ The preparations done before each interview allowed for a smooth interview structure to be held, with the interviewee being able to discuss freely around the questions without taking over the interview.⁷⁹ During each interview one acted as the interviewer while the other took notes, this made sure that the interviewer could focus on maintaining a good rapport with the respondent, while the notary could concentrate on highlighting the essential parts and better provide a basis for follow-up questions. For the sake of fluidity in the interview, this cooperation was seen as key.⁸⁰ All interviews were also recorded to make sure that no answers were missed and that information could be checked and rechecked. It also allowed for more attention to be focused on the interviewee.

3.2.5 Secondary sources

The secondary sources consist almost exclusively out of electronic sources, collected partly from Scopus or from a professional collection provided by the Bitcoin expert Jonathan Jogenfors. Using these two mediums of distribution ensures a high quality of the secondary sources. These two sources are completed by information from established agencies such as reports from the

⁷⁸ A. Bryman and A. Bell, *Företagsekonomiska forskningsmetoder*, Stockholm, Liber, 2013.

⁷⁹ Lantz, A., *Intervjumetodik*, Lund, Studentlitteratur AB, 2013.

⁸⁰ A. Bryman, *Social Research Methods*.

World Bank, the European Constitution and other established agencies. Printed information about Bitcoin is very rare and in most cases irrelevant to this subject, due to the novelty of Bitcoin. The theoretical framework presented in this paper comes from acknowledged theorists and their work was obtained through the library of Linköping University.

3.2.6 Reference Guide

All primary and secondary sources have been referenced to by using the Oxford referencing system described in the *New Oxford Style Manual*.⁸¹ This system was chosen for its rigorous stating of source information, giving the reader good means of checking the written information. The only departure from the system guidelines is that this thesis attaches website links into the source titles in order to make the footnote sections less cluttered.

3.3 Ethical Statements

Bryman summarized the ethical statements of scientific work to four critical aspects; voluntariness, integrity, confidentiality and anonymity.⁸² Following these guidelines, all interviewees were informed that participation was entirely voluntary and that they could chose to end the interview at any given time if they felt uncomfortable. For those not wanting a certain answer to be connected to their personal identity, information was provided already in the interview guide that they had the choice of being anonymous. In the interview guide, a very brief explanation of the purpose of the interview was also included, carefully balanced to give an informative overview without biasing the respondent. The interview questions were also sent to the interviewee if asked for, in order to allow for more preparation if needed. Lastly, permission to record the interview was asked for before the interview started.

⁸¹ *New Oxford Style Manual - 2nd Edition*, Oxford, Oxford University Press, 2012. For a quick overview of the referencing guidelines, see the following [link](#).

⁸² A. Bryman, *Social Research Methods*.

3.4 Criticism

3.4.1 Reliability

A thesis of high reliability is one which can be replicated to give the same result, an especially important aspect in a qualitative thesis dealing with many underlying assumptions which need to have basis in reliable data.⁸³ Reliability for this thesis was gained through taking several precarious steps in the gathering and handling of the empirical evidence, aiming for a consistent and unbiased methodology. Consistency in the use of interview guides and the standardization of interview procedures gives credit to the results reliability. This in par with the attached interview guides, thoroughly documented interview sources and only three anonymous interviewees, provides a good ground for replicability. The recording of interviews neutralizes the risk of misinterpreting the provided answers and makes sure no information is distorted.

3.4.2 Validity

Another important quality of a well written thesis is its validity, which aims to scrutinize if the conclusion of the thesis is in accordance with its questions and purpose.⁸⁴ This criterion is reached, since the purpose of this paper gets reflected throughout the entire thesis and boils down to the conclusions made in the analysis.⁸⁵ In order to maintain a high level of validity in the thesis and the model, which stands in the center of it, several steps were taken; the primary data was collected from respondents highly knowledgeable about their respective professions and scrutinized in comparison with the secondary data.⁸⁶ The secondary data was in turn gathered from a vast source of electronic articles provided from Jonathan Jogenfors, pared with relevant scientific journals and textbooks.

3.4.3 Source criticism

To further strengthen the scientific relevance of the thesis, it is of value to criticize its weaknesses, especially in the sources. Both primary and secondary sources were carefully selected, always keeping the purpose and research problems as the highest priority. Therefore, only sources with an immediate usability in answering the research questions were selected.

⁸³ Bryman.

⁸⁴ Bryman.

⁸⁵ S. Kvale and S. Brinkmann, *Den kvalitativa forskningsintervjun*, Lund, Studentlitteratur AB, 2009.

⁸⁶ M. Descombe, *Ground Rules for Social Research*.

Even under this careful selection there is however room for criticism, especially in the bias that might surface from both the interviewer and the interviewee.

There is a great geographical disparity between the interviewees. While the Bitcoin traders were situated in diverse locations such as Canada, South Africa, England and Germany, the Bitcoin experts and state authorities were almost all exclusively from Sweden. With anti-money laundering regulation differing between these geographical location, the answers obtained from the interviews might be slightly biased. It is however important to note that with Bitcoin being a global currency, geographically disperse empirical evidence might also provide a more accurate representation of the different preferences.

Bitcoin traders may also have a strong incentive to trivialize the problems of money laundering in Bitcoin, especially if the interviewee is personally connected to the company, which was the case in two of the interviews. The fact that both of these respondents were the CEO and owner of their respective company reveals a very strong bond between their company and themselves. Their validity is however strengthened again by the fact that they chose not to be anonymous, but have both their name and company published. This leads to the conclusion that both respondents actually stand for their statements. The anonymous trader 1 and the anonymous FIU employee chose to be anonymous because they were not sure how their respective institution would react to their statements. The anonymous trader 2's reason for anonymity remains unknown. Since the persons asked for anonymity to be able to talk more freely, even these statements must be considered of high validity, even though the fact of anonymity usually diminishes the relevance of a statement.

Respondents from governmental institutes and experts from academic institutes are considered as less risky to be biased, due to the lack of personal connections to the discussed matter. Their opinions are considered as being purely professional, which however does not guarantee perfect validity, even professional statements can be false or misleading. The risk of intentional bias is however significantly lower. That being said, there is however a risk of bias in the interview conducted with Jonathan Jogenfors, since he worked close with the authors of this paper to help realizing its results. Therefore, the risk of being unintentionally biased by the authors in the interview is higher compared to other respondents. Regarding secondary sources, such as previous research and theories to corroborate the presented models, sources were carefully selected to be of high academic quality and were in most cases from recognized academic

databases. Criteria against the validity of these secondary sources might be the fact that Bitcoin is still a very young and much debated topic, leading to the risk of the presented theories not being scrutinized carefully enough yet, since validation of theories takes time. This paper however guards itself by using multiple sources for different sections, again to strengthen the validity of the thesis.

3.4.4 Method criticism

As previously mentioned interviews with carefully selected respondents were chosen to strengthen the validity of this paper. This paper did however choose not to engage in surveys to bitcoin users, even if it would have been helpful in confirming the relevance of the model. This is due to the fact that finding a variety of experienced Bitcoin users proved to be difficult, as well as the reliability of their possible responses.

4 The Bååth-Zellhorn Model

This section focuses on creating and describing the three previously mentioned models, which are used in order to map out the problems and possible solutions in combating money laundering in Bitcoin. The first part will, through a sequential game, namely the *suboptimal equilibrium game*, give a detailed explanation to what unfavorable equilibrium may occur between the three players on the Bitcoin market (the state, the trader and the user), when a new AML policy is implemented. Afterwards the *optimal equilibrium game* shows what equilibrium is desired to prevail in order for money laundering to be effectively combated without negatively impacting the trade of bitcoins.

To obtain the equilibrium in the *optimal equilibrium game*, a signaling game, namely the *separation game* is developed in this thesis. The *separation game* focuses on the incentives of honest and dishonest users as well as the Bitcoin trader. The idea in the *separation game* is to increase the transaction cost for dishonest users to launder their money, without significantly increasing the costs for the honest user or the trader. If the assumptions in the *separation game* hold, a separating equilibrium is created, forcing the dishonest user to exit the market.

The last game to complete the model is a prisoner's dilemma game, namely the *long-run stability game*. This game serves to prove the equilibrium obtained in the *separation game*, by proving that cooperation between the honest user and the trader is always profitable in the long run. While it is never profitable to cooperate for the dishonest user, neither in the short nor long run. All the games in the model are using Von Neumann–Morgenstern payoffs.⁸⁷

4.1 Illustrating the Problem

Solving the money laundering issues created by Bitcoin requires a distinct definition of the different players on the market and their actions, a model as shown below helps to illustrate the

⁸⁷ D. Prokop, [Von Neumann-Morgenstern utility function](#), [website], 2016, (accessed 25 May 2016).

different roles and equilibria that need to be taken into account when new anti-money laundering directives are put in place in a certain region.

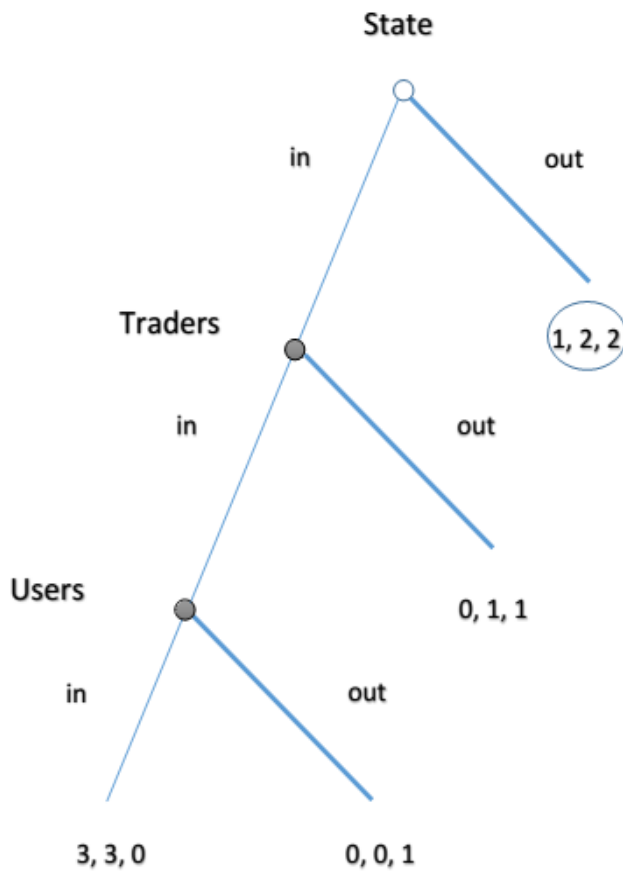


Figure 1 - The suboptimal equilibrium game

Following the traditional characteristics of a sequential game⁸⁸, the composition of the game can be derived as follows.

Players: The state (or governmental entity), the Bitcoin traders, the Bitcoin users
 Player function: State (1), Bitcoin traders (2), Bitcoin users (3)
 Terminal histories: $[in^1, in^2, in^3], [in^1, in^2, out^3], [in^1, out^2], [out^1]$ ⁸⁹
 Player preferences: See assumptions of preferences below

⁸⁸ For a full explanation on extensive games see appendix 8.1.

⁸⁹ Where the ⁿ explains which of the three players take action.

The players have two actions to choose from. "in" or "out". The state chooses "in" if it wants to introduce the new AML directives to the Bitcoin traders and users and "out" if it leaves the market with the current regulations. The traders get to choose between accepting the regulations, thus staying in the region where the AML directive got implemented (in) or by moving out of the area into a non-regulated region (out). If both state and traders chose "in", the users have to evaluate if they want to exchange their bitcoins in a stricter regulated area or not, if they do, they choose "in" if not, they choose "out". The payoffs chosen in the model are based on assumptions made to facilitate the analysis of the current situation.

4.1.1 Assumptions of preferences

All players strive to minimize their respective transaction costs, an objective which is represented by the model's terminal histories. The higher the payoff value, the lower the transaction costs attributed to that particular strategy. Thus all players will play the game with the simple goal of maximizing their payoffs.

The state

The state is assumed to prefer the option of everyone choosing "in" the most, due to the reduced possibility of money laundering. Not investing in any new AML-directives is considered the second best option, as it maintains the status quo, if however the state chooses "in" and the traders or users choose "out", the state loses its Bitcoin market either due to traders or users leaving. This is assumed to lead to loss in taxes, reputation and constrained innovation in the field of cryptocurrencies.

Traders

Bitcoin traders also prefer the outcome [in, in, in] since it provides traders with the reassurance of diminished money laundering activities within their company. The second best outcome for traders would be [out, out, out], since it maintains status quo, thus not losing any investments made to accommodate for new restrictions. The third most preferred outcome for Bitcoin traders is if the state implements the rules and the traders defect by choosing "out". The cost of relocating to a different area is worse than the status quo, however still better than accommodating for restrictions while the Bitcoin users choose to defect, which would be the fourth and worst outcome for the traders.

Users

The model assumes the best outcome for the Bitcoin users to be the status quo, meaning no new restrictions, leaving the users their freedom of relative anonymity. If the state chooses to introduce stricter AML restrictions, [in,out,out] or [in,in,out] yield the highest payoffs to the user, the payoff is worse however, since in both scenarios the user has to trade bitcoins in a different region. All options are better for the user than [in,in,in] because anonymity is lost, which is assumed to be considered very valuable to the users of cryptocurrencies such as Bitcoin.

The *suboptimal equilibrium game* shows that, by using backward induction the equilibrium [out¹,out²,out³] is subgame perfect, meaning it will be the outcome, given all players rationality. The Nash equilibrium reached will therefore reject new AML regulations. In order to better prevent money laundering, the outcome must become [in, in, in], as seen in the *optimal equilibrium game* below.

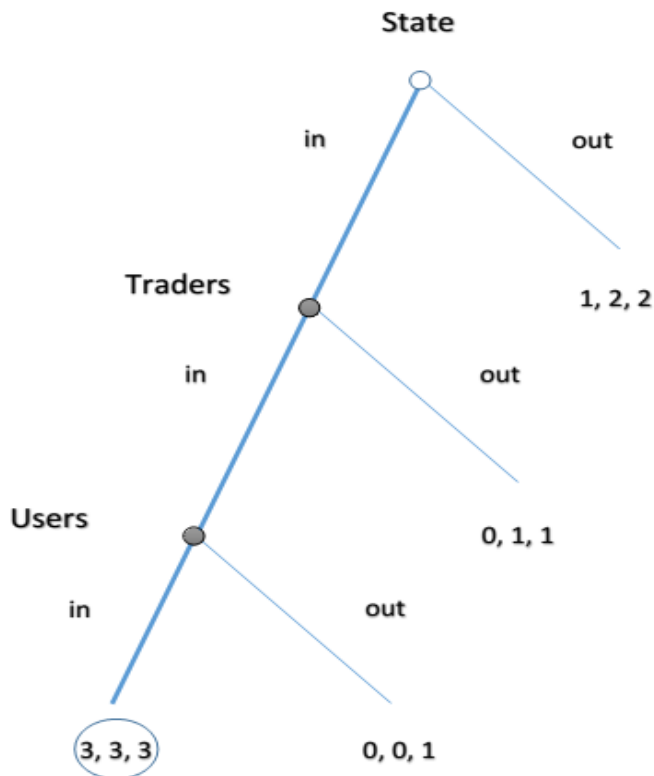


Figure 2 - The optimal equilibrium game

4.2 Solving the Problem

In order to prevent the risk of ending up in the equilibrium [out, out, out] shown in *suboptimal equilibrium game* and instead reaching the equilibrium [in, in, in] shown in the *optimal equilibrium game*, all the players strategies must align. This will only happen if the transaction cost for choosing “in” is lower for all players than choosing “out”. The equilibrium in the *suboptimal equilibrium game* stems from the Bitcoin users’ choice of grabbing the higher payoff by choosing “out”, thus making that strategy more attractive to the rest of the players as well. If the payoff of choosing “in” would be higher than “out”, then that would turn “in” into the user's optimal strategy, as well as the optimal strategy for the rest of the players. If the Bitcoin users have an incentive to cooperate, the other players do too. The equilibrium seen in the *optimal equilibrium game* could therefore be reached if (1) the payoff from “in” is higher than “out” for the user and (2) the payoffs for the traders and the state are either increased or left unchanged. Put in other words, any regulation aimed at Bitcoin has to not only be effective at stopping money laundering, but also reach the minimum requirement of not imparting too high transaction costs on the Bitcoin users. Only then will regulation be unanimously accepted.

One possible solution to attain (1) and (2) would be to implement a reward system which would give the users financial incentives to voluntarily reveal information which would be useful to the traders and the state from an AML perspective. The financial incentive would for the users lead to a neutralization of the small increase in transaction cost that giving up information entails. As long as the incentive is high enough, the regulation will not impart any extra transaction cost, leading the user to grab the higher payoff by choosing “in” and thus attaining (1). As long as the extra information revealed by the users is useful in the combating of money laundering, the traders and the state will also enjoy lower transaction costs and (2) would be attained as well. An equilibrium at [in, in, in] would therefore be reached.

This solution can be modelled in the *separation game* shown below.⁹⁰

⁹⁰ For a full explanation of signaling games, see the appendix 8.2.

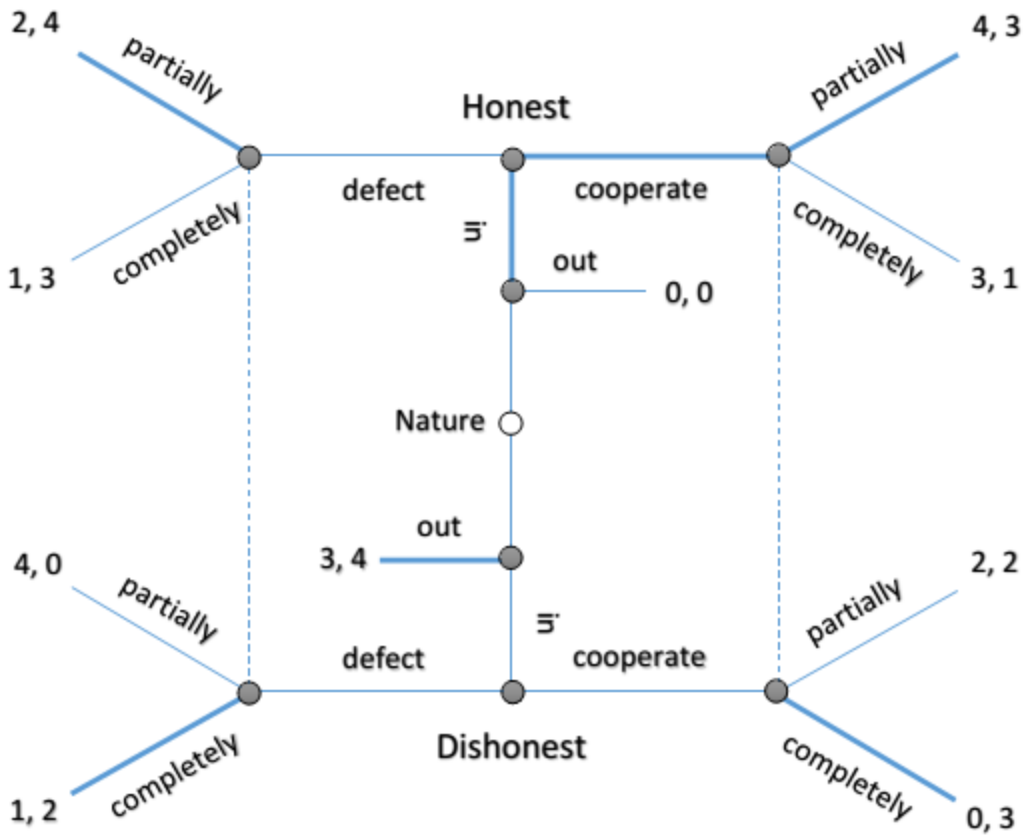


Figure 3 - The separation game

Players: Bitcoin user, Bitcoin trader
 Player function: Bitcoin user (1), Bitcoin trader (2)
 Terminal histories: [out¹], [in¹, defect¹, partially²], [in¹, defect¹, completely²] [in¹, cooperate¹, partially²], [in¹, cooperate¹, completely²]
 Assumption of preferences: See 4.2.2 below.

4.2.1 Explanation of actions and strategies

The game starts with nature that draws either an honest, law-abiding user or a dishonest, money laundering one. Both types stand before the choice of either doing business with the trader (in), or not doing business with the trader (out). If “in” is chosen, the users stand before the choice of giving up extra information in exchange for a financial reward (cooperate), or to not give up any extra information but neither receiving a reward (defect). Note that if “defect” is chosen, the users still give up a small amount of information because of the KYC directives in place in almost

all Bitcoin traders. Depending on the choices made by the users, the trader has to choose between checking all users and the provided information (completely) or only check a partial sample of the users (partially).

4.2.2 Assumption of preferences

As stated before, the assumed payoffs represent the desire for each player to minimize their transaction costs.

The honest user

Choosing “cooperate” whereby the trader responds with “partially”, is considered to be an optimal outcome, (4) since the user receives his or her reward and has the chance of still retaining anonymity. Cooperating while the trader responds with a guaranteed check-up is deemed a close second (3). Along the same logic, choosing not to cooperate whereby the trader checks partially is the third best outcome (2) and choosing not to cooperate while the trader checks completely is preferred fourth (1). Not entering the game at all yields the least favorable outcome since the user has to go through other more time-consuming exchange channels (for example a private exchange) with no chance for a reward (0).

The dishonest user

Highest outcome can be attained by choosing to deviate whereby the trader chooses to check partially (4). Although this would have the dishonest user run a small risk of getting caught, he would still be able to reap the benefits of using a trader. Second best outcome is to never enter the game at all (3), forcing the user to go through more time-consuming channels but avoids the risk of getting caught altogether. Cooperating while the trader checks partially is deemed to be the third best alternative (2), since the user gains the reward but runs an increased risk of getting exposed with the revealing of more information. Defecting while the trader checks completely leads to the fourth best outcome (1), with the user running a very high risk of getting caught while receiving no reward. In the outcome resulting from the user choosing to cooperate while the trader checks completely (0), the reward given to the user is deemed to be heavily outweighed by the very likely chance of being exposed.

The trader

Having the honest user choose to defect while the trader answers with checking partially will yield the highest outcome (4), since the trader does not have to waste time and resources on a non-money laundering user. The two cases where a defect from the user is followed by a complete check by the trader, and cooperation from the user is followed by a partial check by the trader, yield an indifferent outcome (3). Spending a large amount of time checking but not having to give a reward is deemed to be as much of a cost as spending a low amount of time while having to give a reward. The third preferred outcome is for users to cooperate while the trader checks completely (1), since a good deal of both time and money has to be exerted without any money laundering being stopped. The least preferred outcome is for the user to not use the trader at all (0).

When dealing with the dishonest users, the payoffs for the trader shifts. Here, the most preferred outcome is for the dishonest users to not use the trader at all (4). Followed by the user choosing to cooperate while the trader checks completely (3), since the much increased chances of catching the dishonest user outweighs the cost of the reward. The two cases where a defect from the user is followed by a complete check by the trader, and cooperation from the user is followed by a partial check by the trader, yields yet again an indifferent outcome (2). Lastly, having the user deviate while the trader checks partially yields the worst outcome, due to the dishonest user running the lowest chance of getting caught (0).

4.2.3 Playing the game

For an honest user, entering the game will always be more profitable than exiting, so the first action will be to choose “enter”. From the second node, the dominant strategy for an honest user is to always chose “cooperate”, since the model assumes that for an honest user who has nothing to hide, the reward outweighs the cost of giving up information. Put in other terms, the financial incentive offsets the imparted transaction cost. A user who chooses to “cooperate” is therefore signaling that he is of the honest kind and the trader can choose the action “partially”, knowing that the honest user will not need a rigorous check.

For a dishonest user, entering the game is only worthwhile if the trader chooses “partially” after the user chooses “defect”. But this outcome will never happen, because of the trader's belief that anyone who chooses defect is dishonest will make the trader always chose “complete” after

observing “defect”. As a result, the transaction cost for choosing “enter” will be too high and dishonest user will always choose “exit” and not do business with the trader at all.

4.2.4 General concepts of the *separation game*

The separating equilibrium illustrated by the *separation game* can only be reached if the precedent assumptions all hold true. Different preferences of players lead to different outcomes in equilibria, which is why this section focuses on a general concept of the model, where previous assumptions about the model have been relaxed. Let us therefore call the user’s payoffs: A, B, C, D and E. While the trader's payoff is denoted as: a, b, c, d and e. The difference of the payoffs in this section compared to the previous one, is that every payoff function can take any given number, there is thus no determined ranking in preferences put in place. The *separation game* in its general form can be illustrated as follows:

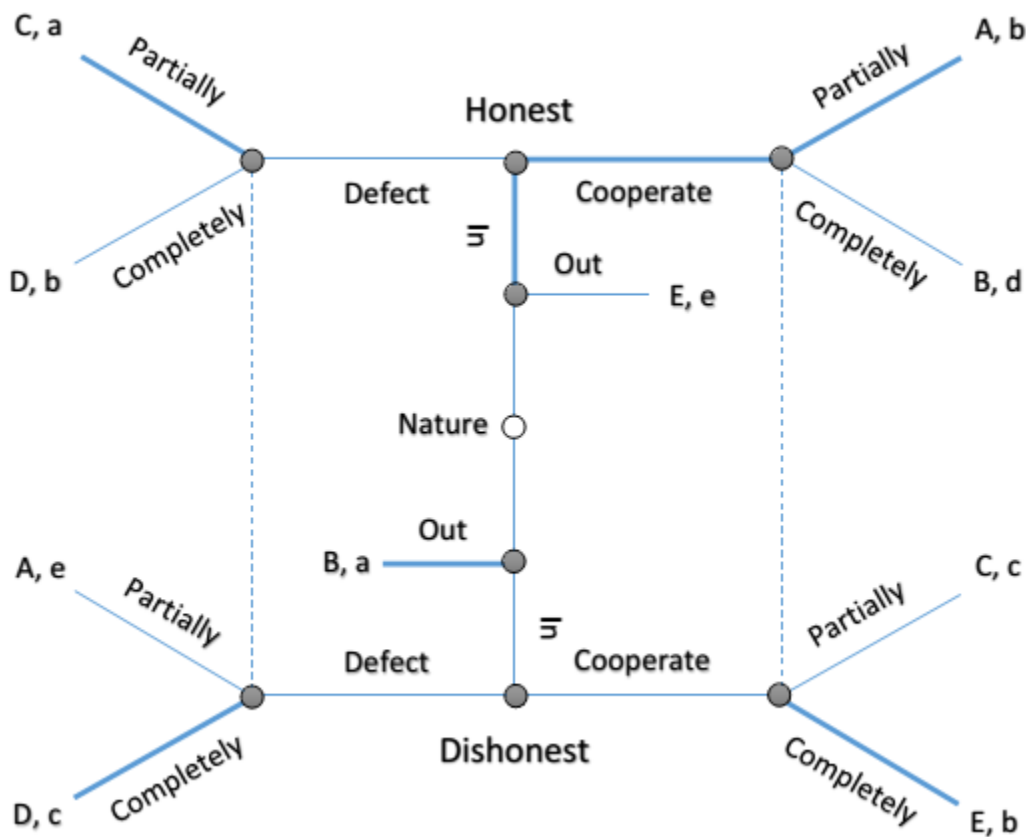


Figure 4 - The general separation game

Examining the model shows that it is exactly the same as the original *separation game*, except for the payoffs being swapped for letters. To reach the separating equilibrium in the original game, following payoff preferences must hold true:

Payoffs: Users: A, B, C, D, E where $\rightarrow A > B > C > D > E$
 Traders: a, b, c, d, e where $\rightarrow a > b > c > d > e$

Following game theoretical logic and given this order of preferences, the game will still end in honest users cooperating with the trader, while dishonest users choose to exit the market. Since this model illustrates the payoff function in its general form, other rankings of preferences can also occur. This section picks out two outcomes that are likely to possibly occur.

For example, there is no absolute logic behind $B > C$, C might as well be greater than B, thus potentially leading to the dishonest user to choose “cooperate” by trying to fool the trader into believing he or she is in fact dealing with an honest user. If the dishonest user manages to deceive the trader, the trader might choose to only check “partially” and the dishonest user manages to get away with its money laundering. The rational thinking trader knows of this danger and chooses to mix his or her strategy by checking “completely” and “partially” in order to maximize his or her payoff. This might then lead to the dishonest user to weigh the risk of being caught as too high and yet again exit the market. Therefore, a separating equilibrium may still be obtained.

There are however many payoff functions that do not lead to a separating equilibrium. If, for example, the financial incentive for giving up personal information is so strong that it outweighs the risk of being caught for a dishonest user, the equilibria would shift to a pooling one. Let us assume following payoff function for the dishonest user: $C > E > A > B > D$. In this instance the dishonest user always chooses to cooperate, (just as the honest user, given that their payoff preferences remain unchanged). The trader cannot tell from the signals if a user is honest or dishonest and will have to mix their strategy according to their beliefs of distribution of honest and dishonest users.

4.3 Confirming the Solution

To prove the validity of the *separating game* above, an indefinitely repeated prisoner's dilemma game can come to serve, namely the *long-run stability game*. It facilitates the understanding of the differences in the incentive structures between the honest and dishonest players and also shows how cooperation between Bitcoin users and Bitcoin traders becomes beneficial in the long run. Furthermore, the *long-run stability game* distinguishes rational honest players from rational dishonest players, confirming the assumptions made in the *separation game* that honest users in the long run choose to cooperate with the traders while dishonest users choose to exit the market. This can be explained by the fact that dishonest users risk getting caught with illicit activities if they choose to cooperate with the trader, if they however refuse cooperation, given all players rationality, traders may rightfully assume dishonesty in defecting users. The models below illustrate these scenarios, the upper models being short run equilibria, the lower ones being long run equilibria.

Players: Honest user (1), Bitcoin trader (2)		Players: Dishonest user (1), Bitcoin trader (2)	
Strategies:	P1: Cooperate, Defect P2: Cooperate, Defect	Strategies:	P1: Cooperate, Defect P2: Cooperate, Defect
Preferences:	P1: $DC > CC > DD > CD$ P2: $CD > CC > DD > DC$	Preferences:	P1: $DC > DD > CC > CD$ P2: $CD > CC > DD > DC$

Short run

		Trader	
		Cooperate	Defect
Honest user	Cooperate	B, b	D, a*
	Defect	A*, d	C*, c*

		Trader	
		Cooperate	Defect
Dishonest user	Cooperate	C, b	D, a*
	Defect	A*, d	B*, c*

Long run

		Trader	
		Cooperate	Defect
Honest user	Cooperate	B, b	D, a*
	Defect	A*, d	C*, c*

		Trader	
		Cooperate	Defect
Dishonest user	Cooperate	C, b	D, a*
	Defect	A*, d	B*, c*

Figure 5 - The long-run stability game

Let us first analyze the game between honest users and Bitcoin traders, the Nash equilibrium in the finite game equals DD, following basic game theoretical logic.⁹¹ In an indefinitely repeated game however, prisoner dilemmas may resolve themselves through cooperation between the two players. This is due to the fact that in a long-run game, the honest user and the trader are left better off with a constant payoff of B, than to defect and getting the payoff A once, and afterwards having to accept payoff C due to the other partner punishing their choice.⁹² The dishonest user will however always choose to defect, which, as analyzed in the *separating game*, leads to the user exiting the market. The Bitcoin trader has incomplete information about the type of player he or she is playing against, but in the long run, the action of the user will reveal what type they are.

4.4 Criticism on the Model

Since this paper focuses on creating and proving its own model, criticizing the model and its assumptions lays at hand. In order for the models and assumptions to hold true, perfect rationality is required, it is apparent that perfect rationality from every individual is a utopia. This fact does however not declare the model as unfeasible. Economic models in its general form

⁹¹ For a full explanation of the prisoner's dilemma game and repeated games, see the appendix 8.3.

⁹² The same payoffs are assumed for the players here as in the *separating game*. Furthermore, this thesis does not analyze the impact of a discount rate, since it is considered to not alter the result in a significant way.

frequently rely on individuals being rational, which to a certain point holds true for most individuals. Another flaw in the model is the fact that it was near impossible to collect feasible data that could indicate the spread of honest and dishonest Bitcoin users. So the model has to work with an unknown probability of nature drawing a dishonest or an honest user. This problematic was overcome due to the separating equilibrium, yet an exact number of dishonest users would have facilitated the validation of the model. The *long-run stability game* chooses to not take any discount rates into consideration. This is due to the fact that any realistic discount rate does not impact the result and would thus only further complicate the analysis of the model.

5 Empirical Evidence, Results and Analysis

With the model presented, let us now focus on the empirical evidence given by the respondents on the matter. In the following section of empirical evidence, the findings will be presented, scrutinized and analyzed in context with the relevant game theoretical model. This serves to prove the validity of the model and to back it up with professional expertise. As previously mentioned, the feasibility of the models can be put into three main aspects; incentives, technicalities and practicalities.

5.1 Incentives

This section focuses on the different assumptions of preferences and their viability throughout all parts of the model.

5.1.1 Presentation of the empirical findings

In the interviews with Jogenfors, Lothigius, Scherschneva and the anonymous trader 1, it was stated that Bitcoin users value their anonymity quite high.⁹³ On the question asked if a financial incentive would increase the willingness for Bitcoin users to give out personal information (thus lowering their anonymity) the opinions went apart, with some saying it would help⁹⁴ and some saying it would not significantly improve the attitude towards the lost anonymity.⁹⁵ There was, however, an almost complete agreement on the fact that honest Bitcoin users care less about their anonymity than dishonest users.⁹⁶ A lot of respondents also claimed that honest users are far more willing to accept the reward and reveal more information than dishonest users are.⁹⁷

⁹³ D. Lothigius, interview, 2016 and J. Jogenfors interview, 2016 and Anonymous Bitcoin Trader 1, interviewed by Felix Zellhorn and David Bååth, 2016, Halifax and E. Scherschneva, interview, 2016.

⁹⁴ Anonymous Bitcoin Trader 1 interview, 2016 and J. Jogenfors interview and J. Tibbling, interview, 2016.

⁹⁵ J. Scigala interview, 2016

⁹⁶ E. Scherschneva, 2016 and D. Lothigius interview, 2016 and Anonymous Bitcoin Trader 1 Interview, 2016 and E. Elgebrant interview, 2016 and the Swedish FIU interview, 2016.

⁹⁷ D. Lothigius interview and J. Jogenfors and Anonymous Trader 1 and the Swedish FIU interview.

When it comes to the traders' preferences, the interviews showed that all Bitcoin traders who were asked said that combating money laundering has a high priority in their company and that users who are suspected of being dishonest get flagged and controlled. The traders also stated that they would finance and implement a stricter AML-policy given that it combats money laundering more effectively.⁹⁸ In the interview with the anonymous trader, the respondent also stated that not giving out information in a rewarding system would raise red flags and that those users would get further scrutinized.⁹⁹

When being asked if they could imagine financing stricter AML-directives, three out of four traders said yes. However, not one of them wished to be subsidized by the state, since they prioritized independence from the state,¹⁰⁰ which, according to Jogenfors, is a keystone in Bitcoin.¹⁰¹ In practice, Scigala and the anonymous trader 1 stated that users who appear to be honest do not get controlled in the sense that their blockchain gets examined.¹⁰² Scigala stated that the task of the Bitcoin trader is to act according to the law, but not to surveil their customers. At Vaultoro, users can trade for a sum of under \$5000 without registration. ICE3X and the anonymous trader follow the AML restrictions put in place, which in Europe equals 7500€ without registration.¹⁰³

5.1.2 Empirical findings analyzed and applied to the model

Checking the feasibility of the optimal equilibrium game

The assumptions of the *optimal equilibrium game* are based on the state wanting to implement a stricter AML-policy, but the users are choosing to defect to a different area (as happened with Bitlicense), thus the traders choose to exit the market as well. In the *suboptimal equilibrium game* all this is anticipated and therefore the state chooses not to implement it. Given the right incentives however, this thesis argues that a different equilibrium can be reached.

⁹⁸ J. Scigala interview, 2016 and Anonymous Bitcoin Trader 1 Interview, 2016 and G. Grobler interview, 2016.

⁹⁹ Anonymous Bitcoin Trader 1 interview.

¹⁰⁰ Anonymous Bitcoin Trader 2, interviewed by Felix Zellhorn and David Bååth, 2016, London.

¹⁰¹ J. Jogenfors interview, 2016.

¹⁰² J. Scigala interview and Anonymous Bitcoin Trader 1 interview.

¹⁰³ J. Scigala interview

Let us first see if the assumption that users leave the market (just as with Bitlicense) when the restrictions get too intense, holds true. Bitcoin traders were convinced that this would not be the case. The state authorities and the technical expert however argued that a decrease in anonymity for the users would cause an uproar and be seen as very unwelcome. To draw the conclusion that all Bitcoin users would defect and move their bitcoin trading out of the area might be a bit far-fetched. Nevertheless, it is probable that a stricter AML-policy would lead to a significant commotion in the Bitcoin community, putting pressure on traders and governments.

The traders were assumed to comply with the government by preferring to choose “in”, but instead they chose “out” because of the users defection. In the interviews with the traders it became clear that the traders minimize their dependence on governmental entities, but that they will always comply with the existing rules as long as it does not clash with their customers. Even if this slightly goes against the assumption that Bitcoin traders wish to put in place stricter rules, the result remains the same. The Bitcoin trader will always comply with the state, so choosing “in” will be the preferred choice for the trader, given that the state implements the new rule. However, if the users defect by relocating their trades to different markets, the traders are also better off by defecting and will thus choose “out”. Even if no significant empirical data backed up the state's preferences, given normal rationality, the state would also then choose “out”, in order not to lose the entire Bitcoin market. With the right incentives, this paper aims to show how to reach the equilibrium in the *optimal equilibrium game*.

Checking the feasibility of the separation game

To check the feasibility of the *separation game*, the assumptions of the players' incentives in the *the separation game* need to be scrutinized through the empirical data collected through the interviews. The easiest assumption to verify is the fact that dishonest users value their anonymity the highest of all players and that financial incentives in no way outweigh the cost of getting caught. Therefore, the assumption that dishonest users always play “defect” rather than “cooperate” must hold true. Even though many honest users are considered to value their anonymity quite high, many respondents felt that the combination of the financial incentive and the fact that they have nothing to hide may outweigh the loss of anonymity. It is therefore possible to assume that at least the majority of rational honest users choose to “cooperate” by revealing extra information about themselves.

An honest player with nothing to hide prefers to be “partially” checked while getting a reward over being partially checked and not getting one. The player also prefers to be “partially” checked over “completely”, since he or she still cares about privacy. Given that all players are rational, the assumption of the dishonest user exiting the market will also hold true. As previously mentioned, the equilibrium for all honest users is to cooperate, but for dishonest users the dominant strategy is to defect. As one trader mentioned in the interview, this will lead to traders drawing the conclusion that all users who provide information and collect the reward are honest, thus all users who don’t follow that principle will be suspected of being dishonest. This leads to a complete check and most likely to the prosecution of the dishonest user. To avoid this from happening, the dishonest user only has one choice, to never enter the market in the first place, since it is strictly logical that getting caught and being prosecuted is a worse outcome than avoiding the Bitcoin market.

When it comes to the traders, the assumption of preferring to “partially” check honest users and consequently “completely” check all dishonest users shows to hold true as well. All interviewed traders stated that they checked all dishonest users.¹⁰⁴ Also the fact that no Bitcoin trader checks every customer’s blockchain, strengthens the assumption that traders prefer to only partially check their honest users. The Bitcoin trader will always prefer to pay as little money as possible, given it does not impact the catch rate of the dishonest users. Given that more dishonest users will get caught, the trader will always choose to pay the extra amount of money. Even if this statement is debatable, with Scigala saying that it is not his task to surveil customers, being associated to illicit money transfers can still viably be seen as a worse payoff for the trader.

The preferences and payoff structures in the *separating game* can therefore be seen as reasonable. Given rationality, the model holds true.

Checking the feasibility of the long-run stability game

The last game, namely the *long-run stability game*, aims to explain why the incentives to cooperate rationally make sense, especially in the long run. The empirical data, as previously mentioned, proves that honest and dishonest users clearly have different payoff functions. To “cooperate” yields a higher payoff to the honest than the dishonest user. Even in the case of

¹⁰⁴ All traders said they checked all “suspicious” users. Suspicious is a subjective term, but in this case it is perfectly legitimate to assume that “suspicious” and “dishonest” can be put together to refer to the same type of users.

“defect” being the strictly dominant strategy for both users in the short run, in the long run honest users gain welfare by “cooperating” while dishonest users do not. The empirical evidence backs up this statement. Therefore the assumed incentives for the players hold true even for this model, allowing the proof of “cooperation” at least from the honest user.

Considering the trader, empirical data also points to the long run equilibria of “cooperation”. All traders asked were willing to finance an improved AML-policy given it improves combating money laundering. This leads to the conclusion that all traders have incentives to “cooperate” with the honest users, especially in the long run.¹⁰⁵ Dishonest users will therefore always reveal themselves when playing defect, making the signals given in the signaling game highly effective to detect money launderers.

Reaching equilibrium in the optimal equilibrium game

After carefully examining the incentive structures of the different players, it is now possible to draw the conclusion that all models hold from an incentive standpoint. Given a new AML-policy that includes financial incentives to the Bitcoin user, traders have incentives to implement it, honest users have incentives to stay in the market and thus giving up information and “cooperating” with the state and trader, while dishonest users have to exit the market. The state is rational and sees this and does therefore choose to implement the new policy.

5.2 Practicality

This section focuses on the practical issues that need to be solved in order for the model to hold.

5.2.1 Presentation of the empirical findings

Emil Elgebrant stated that the regulation of Bitcoin traders is juridically feasible.¹⁰⁶ Lothigius means that Bitcoin is already under the regulation of the current AML-directives put in place by the European Union, a statement that is shared by Emil Elgebrant, Jonathan Jogenfors, Jan

¹⁰⁵ The explanation is specified in section 4.3.

¹⁰⁶ E. Elgebrant interview, 2016.

Tibbling and the Swedish FIU.¹⁰⁷ Elena Scherschneva and the anonymous Bitcoin trader 2 however claimed that Bitcoin does not fall under any regulation, since digital cryptocurrency, as of today, is not regulated.¹⁰⁸ All respondents were however in agreement over the fact that it should be regulated and that regulating the Bitcoin trader, whether it is voluntarily or by law, is a good approach to combat money laundering.¹⁰⁹

When it came to what information is practically viable for the Bitcoin traders in an implemented AML-policy, all respondents agreed on standard KYC information being the most important one.¹¹⁰ Lothigius also expressed that the origin of the exchanged money and its purpose of use is important information that would increase the possibilities for the Bitcoin traders to identify illicit transactions and users.¹¹¹ Jogenfors and Scherschneva shared this opinion, also by adding that not only knowing where the bitcoins come from is viable information for the traders, but also what other future transactions will be made from that particular Bitcoin account.¹¹² Scigala claimed that further information is not needed, in order to keep in line with their customers.¹¹³ Gareth Grobler claims that his customers already provide all the information needed and would also not mind providing more information, since his customers in South Africa have very little privacy. He also claims that the regulation in itself is not the problem, but the way it is implemented, a statement that is shared by Elgebrant and Lothigius.¹¹⁴

Jogenfors mentioned that better exchange rates are a good example of incentives which would make the Bitcoin users give up more personal information, an idea that Elgebrant and the anonymous Bitcoin trader 1 shared. Vaultoro, with Scigala as the CEO, even had active plans to implement a rewarding system for verification.¹¹⁵ The Bitcoin user Kraken already uses a rewarding system, not for verification, but for trade amounts.¹¹⁶ There were also voices against

¹⁰⁷ E. Elgebrant interview and J. Jogenfors interview, J. Tibbling Interview, 2016, D. Lothigius Interview, 2016 and the Swedish FIU interview, 2016.

¹⁰⁸ E. Scherschneva interview, 2016 and Anonymous Bitcoin Trader 2 interview, 2016.

¹⁰⁹ The Swedish FIU interview and E. Elgebrant interview and E. Scherschneva interview and Anonymous Bitcoin Trader 2 interview and J. Jogenfors interview and D. Lothigius interview.

¹¹⁰ The Swedish FIU interview and E. Elgebrant interview and E. Scherschneva interview and Anonymous Bitcoin Trader 2 interview and J. Jogenfors interview and D. Lothigius interview and J. Scigala interview, 2016 and Anonymous Trader 1 interview, 2016.

¹¹¹ D. Lothigius interview, 2016.

¹¹² J. Jogenfors interview, 2016 and E. Scherschneva interview, 2016.

¹¹³ J. Scigala interview, 2016.

¹¹⁴ G. Grobler interview, 2016 and E. Elgebrant interview and D. Lothigius interview.

¹¹⁵ J. Scigala interview, 2016.

¹¹⁶ Kraken, [Fee Schedule](#), (accessed 12 May 2016).

the improved exchange rate as a reward, with Lothigius and the Bitcoin trader 2 claiming that Bitcoin users won't be attracted by this sort of incentive to give up personal information.¹¹⁷ Another idea from Jogenfors on viable incentives was to grant customers that provide more information about themselves faster trades, he however also claimed that this would be difficult to practically put in place.¹¹⁸

5.2.2 Empirical findings analyzed and applied to the model

After analyzing the feasibility of the models from an incentive structured point of view, this section focuses on the practical issues, especially in the *separating game* since it is there the incentives will be implemented into the model. First of all, it is noteworthy to point out that the incentive structures (analyzed in 5.1.2) are implementable. Emil Elgebrant stated that a rewarding system can be juridically implemented. Whether it is the state forcing the Bitcoin trader to implement it or the traders choosing to implement it voluntarily, has no effect on the juridical possibility to implement this system. Same logic applies to whether the state or the traders choose to finance the system. Furthermore, all respondents agreed that Bitcoin should be regulated in order to prevent money laundering. The practical problems occur in the actual implementation of the rules. Just as Grobler said in the interview, the problem does not lay in the regulation, but in how the regulation is implemented. As previously mentioned, the opinions went apart regarding the issue if a reward incentive will actively improve combating money laundering. This was due to the fact that many respondents (mainly Bitcoin traders) doubted that a rewarding system would trigger the incentive for honest users to give up more information. It is however still viable to argue for the feasibility to practically implement a rewarding system, due to the fact that almost all the experts and state authorities agreed on its viability. Also, traders agreed they would always obey the necessary requirements the state demands. Furthermore, all traders were willing to finance any new system, given it more effectively combats money laundering. The issue was therefore not the unwillingness to finance the rewarding system, it was the lack of trust in its success. Noteworthy is also to point out that all traders agreed to finance and implement a policy that combats money laundering voluntarily, while when asked, no Bitcoin trader wanted to accept a governmental subsidy. This can be

¹¹⁷ D. Lothigius interview, 2016 and Anonymous Bitcoin Trader 2 interview, 2016.

¹¹⁸ J. Jogenfors interview and E. Elgebrant interview and Anonymous Bitcoin Trader 1 interview, 2016 and J. Scigala interview.

explained with the fact that traders value their independence very highly, since state independency is one of the keystones in Bitcoin.

In order to create incentives for the honest user to “cooperate” with the trader and for the dishonest user to “defect”, two criteria need to be fulfilled;

1. The incentive needs to be high enough for an honest user to go through the trouble of giving up information, while it is low enough for the dishonest user to not risk getting caught.
2. The information given to the Bitcoin trader must be revealing enough to effectively improve the chances of catching dishonest users, but not be so demanding that honest users choose to not provide it.

Let us start with analyzing criterion 1. The first idea that came into mind, both for the authors of this thesis and for many respondents, was a financial reward that is given to the users by providing personal information. An example given by Jogenfors was that customers receive a better exchange rate (bitcoin - fiat currency) when trading with a trader after they provided valuable information. The advantages with such a system is that rewards will be given proportionally, meaning the bigger the trade the bigger the reward, which gives greater incentives for users to provide the extra information. With an incentive getting stronger the bigger the trade, vice versa this implies that users trading bigger sums without wanting to give up the voluntary information for the beneficial exchange rate raise red flags for the traders immediately. The *separation game* thus grants greater security the bigger the trades. Using a lump sum for the financial reward would fail to grant greater security the higher the trading sum gets, but would catch the smaller trades, where the users otherwise might have considered the incentive as too weak to provide the extra information. Obviously a combination between these two methods lays at hand, where the reward is paid out as a lump sum and for any trade where the percentage reduction would be greater than the lump sum, the exchange rate method can be used instead. Other, non-financial incentives might also be viable, such as faster trading or prioritized trades at the Bitcoin trader where one provides information. Since the standard duration for a completely secure Bitcoin trade cannot be below 60 minutes, this solution has obvious flaws in its practicality.

As for the second criterion, various ideas have also been given by the respondents. All interviewees agreed on KYC standards to be the most important and viable information. Many Bitcoin traders use KYC standards for their trades and follow the AML-policies that are put into place for the banks. This means that for all Bitcoin traders that were interviewed, identification and place of address need to be filled out, at least when the trade is exceeding 7500€. However, there is still money laundering happening even when this information is provided, which is why additional, voluntarily given information can practically help to combat money laundering very effectively. As mentioned in the preceding section, viable information serves to verify where the bitcoins came from and for what purpose they are exchanged to fiat currency. According to the Swedish FSA, the FIU in Austria and the FIU in Sweden this information is considered viable to identify illicit money transfers. Since the honest users received their bitcoins through legal activities and will use their exchanged fiat currency for legal payments, one can consider the information given by the honest users as appropriate and not too demanding, given that an appropriate reward is given to the user. For the dishonest user however giving this sort of information makes it practically impossible to use the trader to launder money, since the origin and purpose of the source of money is illicit, the dishonest user is left with no choice but to defect and not give up their information. As previously analyzed in the signaling game, this leads to the trader receiving the signal that the user is of the dishonest type and does thus a throughout interrogation, which will most likely lead to the prosecution of the dishonest Bitcoin user. Being fully rational the user knows this and does not bother to enter the market. It is therefore possible to draw the conclusion that the information and the incentives developed together with the interviewees can be considered practically possible.

5.3 Technicality

This section focuses on the technical issues that need to be overcome for the model to hold.

5.3.1 Presentation of the empirical evidence

According to Jonathan Jogenfors, any regulatory solution that aims to change the Bitcoin system itself will not be technically feasible because of its decentralized nature. He stated that a

technical solution could however be viable on Bitcoin traders, depending on what information is sought after.¹¹⁹

Information that reveals that a user is sending bitcoins from only one wallet, could be technically accomplished by a system where the trader sets up a temporary public key to which the user can send his or her bitcoins.¹²⁰ Jogenfors continued by explaining that the trader can check the temporary key with an arbitrary method and only confirm the transaction if all regulatory criteria are met. He stated that clustering¹²¹ can further be done to find out how the user obtained certain bitcoins, revealing if they have been earned from mining or trading. Jogenfors added that the clustering method could also help the trader to see not only transaction information specific to their trade, but other transactions made by the user as well.

Jogenfors stated that a reward system based on giving financial incentive in exchange for more information, should not pose a problem on the technical level but could not give a specific example on how it could be structured.¹²²

5.3.2 Empirical findings analyzed and applied to the model

With a modification of the Bitcoin system being virtually impossible, technical innovation has to be focused on where the bitcoins flow out; namely the Bitcoin traders. Jonathan Jogenfors suggestion of temporary public keys being used as digital floodgates, could be one of many viable forms the model can take. Any user who wants to “cooperate” and receive a reward can use one of these temporary keys instead of the standard methods of transferring. From there, the trader can choose to check all temporary keys “completely” or check only “partially”, confirming the transaction as long as no red flags are raised. Jogenfors idea of using clustering could further be used in combination with the temporary keys to create a technical system that better reveals where each user’s bitcoins came from.

¹¹⁹ J. Jogenfors interview, 2016.

¹²⁰ J. Jogenfors interview.

¹²¹ The process of organizing objects into groups whose members are similar in some way. A common technique for statistical data analysis. S.Meiklejohn, et al, [A Fistful of Bitcoins: Characterizing Payments Among Men with No Names](#), [website], 2013, (accessed 25 May 2016).

Tan, Steinbach and Kumar, [Data Mining Cluster Analysis: Basic Concepts and Algorithm](#), 18 April 2004, (accessed 10 May 2016).

¹²² J. Jogenfors interview.

Creating the incentive system described in the *separation game* was deemed to be highly probable by Jogenfors from a technical standpoint. Although no specific details were given, it is worth to note that the idea of financial incentives is already established in some Bitcoin traders. The Bitcoin trader Kraken has incorporated a reward system which gives its customers more favorable exchange rates if larger quantities of bitcoins are traded. Replacing trade quantities with information would not yield a much different concept, thus giving the technical implementation of the proposed reward system much legitimacy. The idea of a non-financial incentive, such as having the user's transactions being cleared faster if more information is given, could prove harder to accomplish. Jogenfors stated that the technical aspects of it could prove troublesome and no other source, primary nor secondary, have shown technical proof of the concept. Therefore, a financial incentive in the form of a cheaper exchange rate is deemed to be the most technically feasible alternative.

To conclude, a system which allows users to give up information that is useful from an AML standpoint in exchange for a financial incentive, as described by the *separation game*, is deemed technically possible.

5.4 Interpreting the Results

The three previous sections have proven the model to hold on all three necessary criteria. The assumed incentives hold up to empirical scrutiny, the proposed system of giving up information is viable, rewards and legal implementation are confirmed and potential solutions to the technical issues have been put forward. Summarized in a sentence, the result states that the proposed model's ability to combat money laundering is viable. However, in order to make clear of the underlying mechanisms which make this possible, a more in depth explanation is needed.

As mentioned before, dishonest users will launder money as long as the transaction costs to do so are low enough for the crime to be profitable. Increase the costs enough, and the crime is no longer worthwhile. The results of the model show that the transaction costs for dishonest Bitcoin users can be increased by introducing a reward system, forcing the dishonest users to choose between three outcomes. (1) The money launderer agrees to reveal more information and increases the risk of getting caught. (2) The money launderer refuses to give up extra information and thereby sends a signal to the trader that the user is dishonest. The trader will

then check him or her more thoroughly and the risk of getting caught increases. (3) The money launderer never enters into business with the trader, choosing more time-consuming means of money laundering but does not run the risk of getting caught. In all three outcomes the transaction costs for the dishonest user has increased, but since the cost is lowest for outcome three, that option will be preferred.

The result also signifies that the transaction costs attributed to an honest user will not increase as much as with the dishonest one. Giving up more information for an honest user does not come with the severe consequence of getting caught, only the cost of less anonymity. As long as the financial incentive is high enough, this cost will be offset and an honest user stands before three outcomes. (1) The honest user gives up extra information, receives a reward and sends a signal to the trader of being honest. The trader will only sample check the user and the cost of anonymity for the user has a chance of remaining low. (2) The honest user does not give up extra information, does not receive a reward and will send a signal to the trader that he is dishonest. The trader will then check the user thoroughly and a cost of anonymity will be imparted on the user. (3) The honest user never enters into business with the trader, choosing more time-consuming means of exchanging bitcoins. Outcome one will be preferred by an honest user since that will entail the lowest transaction cost.

As apparent, the outcomes chosen by the honest and dishonest players are in line with what was predicted by the model. The results indicate that all assumptions made in the model hold and is thus able to effectively separate honest Bitcoin users from dishonest ones by giving them incentives to deviate from each other. This deviation is the result of the core concept that lays at the base of the model; information is much costlier for a dishonest user than for an honest one. By increasing the transaction cost on dishonest users and keeping the cost neutral for the honest users through rewards, money laundering can be combated without forced regulation.

6 Discussion

Money laundering in Bitcoin is an issue, especially due to the granted anonymity. Even though no clear estimation on the total volume of illicit Bitcoin transactions could be made, due to its limited volume one can state that the possibility to launder great sums in Bitcoin is restricted. The possibility for large scale laundering, should Bitcoin significantly grow, is however eminent and quite serious. The game theoretical model we presented in this work contributes to combat money laundering by increasing the transaction costs significantly for the dishonest users without forcing a regulation upon the honest user. The earlier this system gets implemented, the easier it can prevent money laundering if or when Bitcoin grows to bigger, more threatening volumes. The solution presented here, can therefore be seen as a preventive measure. Following the expertise from the interviewed state authorities, the Bitcoin crimes that occur today are not to be ignored. One can state that already now Bitcoin money laundering poses a threat and needs an adequate solution to be dealt with.

The incentive solution presented in this work relies on a variety of Bitcoin traders to implement them. If only one trader in a region uses the system, the dishonest users can just turn to another trader. The model in itself however guards itself from this problem, by creating incentives for such a situation not to happen. If one Bitcoin trader in a market uses financial incentives for their customers to provide useful information, all rational honest users in the same market have incentives to trade with the one Bitcoin trader that offers the financial reward. Since the other traders would then lose their customers, they would have to implement the same financial reward system. At last all Bitcoin traders in the market would use the financial reward system, honest users would provide information and dishonest users will be forced to exit the market. If all Bitcoin traders on all Bitcoin markets use the same system, an equilibrium would be reached where no illicit bitcoins could be traded. If all markets implemented this system, the problem of juridical differences of Bitcoin would also be solved. A global solution where Bitcoin is regulated equally, would hinder money launderers to exploit differences in the system. One has to note however that this is highly hypothetical, since it requires all players on all markets to act rational. Honest users, dishonest users and traders. Perfect rationality will not prevail, but if a

majority of users act rational in this sense, the model will contribute to the fight against money laundering.

There is another related criterion that we find noteworthy to discuss in this section, namely being the fact that the majority of Bitcoin users have to be of the honest type. Since we assume rationality throughout the paper, one also has to assume rationality in the following statement: Bitcoin traders care a great deal about their possibility to increase their business. The reason we state this is, if the majority of the Bitcoin user base is of a dishonest kind, implementing regulation that prevents money laundering will diminish the income of the trader. Since moral aspects also play a role, this argument does not solely rely on the income for the Bitcoin trader. With moral aspects we mean that Bitcoin traders might not want to be a platform for money laundering, since it is against the law. Another aspect for Bitcoin traders to prevent money laundering, even if it financially hurts their business, is that the traders can be punished, since they also break the law if they voluntarily let someone launder money through their business. Nevertheless, we do find it important to point out that the traders' incentives to enforce regulation which stops money laundering will greatly increase if it implies a possibility to increase their amount of customers. For that, the majority of Bitcoin users need to be of the honest kind.

We argue that an increase in regulation will also have a significant impact on Bitcoin's reputation. Bitcoin as of today has the reputation of being used for shady business and money laundering, due to the large potential it offers for it. Cutting down this potential will ultimately also lead to a change in attitude toward Bitcoin and thus possibly draw more honest customers to the system. We argue that there are mainly three types of Bitcoin users¹²³: (1) The shady type who uses Bitcoin for crimes; (2) The technological innovator who uses Bitcoin for its technological benefits¹²⁴ (3) The commercial type who uses Bitcoin to speculate or as a way of payment. If Bitcoin becomes more widely accepted it is primarily the third group of users that will significantly grow, which leads to an increase in the honest user pool. Leading to an even stronger incentive for the Bitcoin traders to implement the rewarding system, which then again improves Bitcoin's reputation. A domino effect is thus created, leading to a further and further

¹²³ We are aware that we throughout the paper referred to two types, honest and dishonest. Type 2 and 3 are both of the honest kind and are, for a game theoretical analysis, easier to put together.

¹²⁴ With benefits we mean the pseudonymity and the non-third party involvement that Bitcoin offers.

diminished possibility to launder money through Bitcoin and also putting the dishonest users further and further into a minority where it becomes harder to use markets to launder money in.

Noteworthy to point out is also that the incentive structure presented in the game theoretical model is applicable, in theory, to any other cryptocurrency. This paper focused solely on Bitcoin due to it being the biggest and most accepted cryptocurrency as of today. However, we see no reason why this method would not be applicable to other cryptocurrencies since they are much alike in their structure. Although fiat currency differs from bitcoins in many aspects, the financial intermediaries who stand in between the buyers and seller in both currencies, do not. As Elgebrant pointed out, banks and Bitcoin traders share many similar attributes and therefore our incentive structured model could be used to combat money laundering in fiat currency as well.

To implement this model in reality, obviously further deep going technical analysis need to be conducted. This paper focused on the technical aspects only so much as to secure its feasibility. Developing an actual technical solution for implementing the incentive model would be of great scientific value to take the next step toward successfully combating money laundering in Bitcoin. This paper laid down the theoretical foundation on how to successfully combat money laundering in Bitcoin. A difficult task, this paper proved to be accomplishable.

7 Conclusion

Can an incentive model combat money laundering in Bitcoin?

This paper indicates how incentives to provide personal information can distinguish Bitcoin users into two different groups; users who launder money and users who do not. This is due to the fact that giving up personal information has a higher transaction cost for dishonest users than for the honest type. The Bitcoin trader and the state can thus more effectively invest resources in controlling the dishonest users. By knowing this, rational dishonest users do not enter the market to trade their bitcoins under such conditions. This leads to a diminished possibility to launder money through Bitcoin exchangers, leading to the conclusion that an incentive model does effectively provide a solution to combat money laundering in Bitcoin.

Can the model be realistically implemented?

The feasibility of the three researched steps, namely incentives, practicalities and technicalities are the three requirements to implement the presented model. This paper proves that a financial reward, such as a cheaper exchange rate, is a practically viable way to create distinguishing incentives and thus equilibria. The personal information that increases transaction costs significantly more for dishonest users than for the honest users is seen to be identification, the origin of money, as well as its future purpose. As of the technical feasibility, interviews with a technical expert deemed the model to be technically possible. Further reaching studies will have to be conducted in order to create a technical solution to provide information and receive a reward. In this paper it suffices to prove the possibility of a technical solution. This allows for the conclusion that the model can be realistically implemented along all three steps.

Sources

Ajello N., *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, Brooklyn Law Review, Volume 80, Issue 2, Article 4, 2015.

Anti-Money Laundering/Combating the Financing of Terrorism, International Monetary Fund, [website], <https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>, (accessed 4 March 2016).

Baeten J. and Den Butter F., *Welfare gains by reducing transaction costs: Linking trade and innovation policy*, 2006.

Bitcoins Virtual Currency: Unique Features Present Challenges for Deterring Illicit Activity, Cyber Intelligence Section and Criminal Intelligence Section (FBI), 2012.

Bol S. and A. Cerić, *Bitcoin - a sustainable means of payment? A transaction cost analysis of Bitcoin compared to traditional means of payment*, Master Thesis, Linköping University, 2014.

Bryman A., *Social Research Methods*, Oxford and New York, Oxford Press, 2008.

Bryman A. and A. Bell, *Företagsekonomiska forskningsmetoder*, Stockholm, Liber, 2013.

California Legislature— 2015–2016 Regular Session. AB-1326 Virtual currency, Introduced by Assembly Member Dababneh, February 27, 2015,

http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB1326

(accessed 3 May 2016)

Camdessus, M., *Money Laundering: The Importance of International Countermeasures*, [website], 1998,

<https://www.imf.org/external/np/speeches/1998/021098.htm> (accessed 10 March 2016).

Castillo, M., *The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem*, New York Business Journal, August 12, 2015,

<http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html> (accessed 6 May 2016)

Chuen, D.L., *Handbook Of Digital Currency. Bitcoin, Innovation, Financial instruments, And Big Data*, USA, Academic Press, 2015.

Danton, B., *Bitcoin and Money Laundering: Mining for an Effective Solution*, Indiana Law Journal: Vol. 89: Iss. 1, Article 13, 2014.

Descombe, M., *Ground Rules for Social Research: Guidelines for Good Practice*, (hitta publishing location), Open University Press, 2009.

Ekobrottsmyndigheten, *Om Oss*, 3 March 2014, <https://www.ekobrottsmyndigheten.se/om-oss/>, (accessed 10 May 2016)

Ekstedt H., *Money in Economic Theory*, Routledge, London, 2015.

Elgebrant E., *Emil Elgebrant*, 7 April 2016, <https://www.iei.liu.se/affratt/elgebrant-emil?l=sv>, (accessed 10 May 2016).

Examination Procedures BSA/AML Compliance Program, [website]

https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_008.htm

(accessed 20 March 2016).

Finansinspektionen, *Vårt Uppdrag*, <http://www.fi.se/Om-FI/Vart-uppdrag/>, (accessed 10 May 2016)

Frequently asked questions: Anti-Money Laundering, European Commission, Press Release Databank, [website], 2013.

http://europa.eu/rapid/press-release_MEMO-13-64_en.htm?locale=en (accessed 18 April 2016)

Frequently Asked Questions - Find answers to recurring questions and myths about Bitcoin, [website], <https://bitcoin.org/en/faq>, 2016, (accessed 23 February 2010).

Groenewegen J., et al, *Institutional Economics: An Introduction*, Basingstoke, Palgrave Macmillan, 2010.

Guidance for a Risk-based Approach to Virtual Currencies, Financial Action Task Force [website], 2015.
<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
(accessed 15 March 2016)

International Monetary Fund: Anti-Money Laundering/Combating the Financing of Terrorism, [website], <https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>, (accessed 2016-05-04).

Is Bitcoin legal?, Coindesk, 19 Augusti 2014,
<http://www.coindesk.com/information/is-bitcoin-legal/>, (accessed 25 April 2016).

Jogenfors J., *Cryptographic currencies: Bitcoin, Litecoin etc.*, [website],
<http://people.isy.liu.se/icg/jonfo33/bitcoin/>, (accessed 10 May 2016).

Kvale S. and Brinkmann S. *Den kvalitativa forskningsintervjun*, Lund, Studentlitteratur AB, 2009.

KYC, Standard Chartered Bank, [website] <https://www.sc.com/in/important-information/kyc.html>, 2016 (accessed 2 March 2016).

Lantz, A., *Intervjumetodik*, Lund, Studentlitteratur AB, 2013.

Mankiw, G., *Brief Principles of Macroeconomics - 7th edition*, USA, Cengage Learning, 2014.

Meiklejohn S., et al, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, [website], 2013, <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf> (accessed 25 May 2016).

Money Laundering and Terrorist Financing: Definitions and Explanations, World Bank, [website]
<http://www1.worldbank.org/finance/assets/images/01-chap01-f.qxd.pdf>, p.2 2003. (accessed 17 February 2016).

Money Laundering Impacts Development, The World Bank, 2003. See section A-3.,
<http://www1.worldbank.org/finance/assets/images/02-chap02-f.qxd.pdf> (accessed 26 April 2016)

Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, [website], 2008.
<https://bitcoin.org/bitcoin.pdf> (accessed 28 March 2016).

New Oxford Style Manual - 2nd Edition, Oxford, Oxford University Press, 2012.

North Carolina considers law to regulate virtual currencies, Associated Press, May 25 2016.
http://www.journalnow.com/news/state_region/north-carolina-considers-law-to-regulate-virtual-currencies/article_dbd9a4ac-6e14-5b3a-81bf-e1b6ad458a9d.html, (accessed 25 April 2016).

Number of Worldwide Non-Cash Transactions for North America, Europe, Mature APAC, Latin America, CEMEA and Emerging Asia in 2012, 2013 and 2014E, [website], 2015
<https://www.worldpaymentsreport.com/reports/noncash> (accessed April 12 2016).

Osborne M., *An introduction to Game Theory*, Oxford and New York, Oxford University Press, 2009.

Pietschmann, T. et al., *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, United Nations Office on Drugs and Crime (UNODC), 2011, http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf (accessed 12 March 2016).

Prokop D., *Von Neumann-Morgenstern utility function*, [website], 2016,
<http://global.britannica.com/topic/von-Neumann-Morgenstern-utility-function> (accessed 25 May 2016)

Regulations Of The Superintendent Of Financial Services Part 200. Virtual Currencies, New York State Department of Financial Services, [website], 2015, <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf> (accessed 15 April 2016).

Rikskriminalpolisen, *Årsrapport Finanspolisen 2009*, [website], 2009, https://www.polisen.se/Global/www%20och%20Intrapolis/Arsredovisningar/02%20Rikspolisstyrelsen/Arsrapport_FIPO_2009.pdf (accessed 6 July 2010)

Rouse M., *What is Peer-to-Peer?*, August 2014, <http://searchnetworking.techtarget.com/definition/peer-to-peer> (accessed 10 May 2016)

Schneider F. and Windischbauer U. Money laundering: some facts. *European journal for law and economics* 26., 2008.

Scigala J., *About the Founders*, [website], <https://www.vaultoro.com/> (accessed 24 April 2016).

Tan, Steinbach and Kumar, *Data Mining Cluster Analysis: Basic Concepts and Algorithm*, [website], 2004, https://www.users.cs.umn.edu/~kumar/dmbook/dmslides/chap8_basic_cluster_analysis.pdf (accessed 10 May 2016).

Tasca, P., *Digital Currencies: Principles, Trends, Opportunities, and Risks, 2015*. Available from: SSRN, (accessed 10 May 2016).

Thakur, D., *Alphanumeric Codes*, [website], <http://ecomputernotes.com/digital-electronics/binary/alphanumeric-codes> (accessed 10 May 2016).

Tsukerman, M., *The Block is Hot: a Survey of the State of Bitcoin Regulation and Suggestions for the Future*, Berkeley Technology Law Journal, Vol. 30, 2015. Available from: SSRN, (accessed 23 February 2016).

Virtual Currencies: Key Definitions and Potential AML/CFT Risks, Financial Action Task Force, [website], <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (accessed 15 April 2016)

Warning to consumers on virtual currencies, European Banking Authority, 2013

Williamson, O. *Markets and Hierarchies*: The Free Press, New York, 1975.

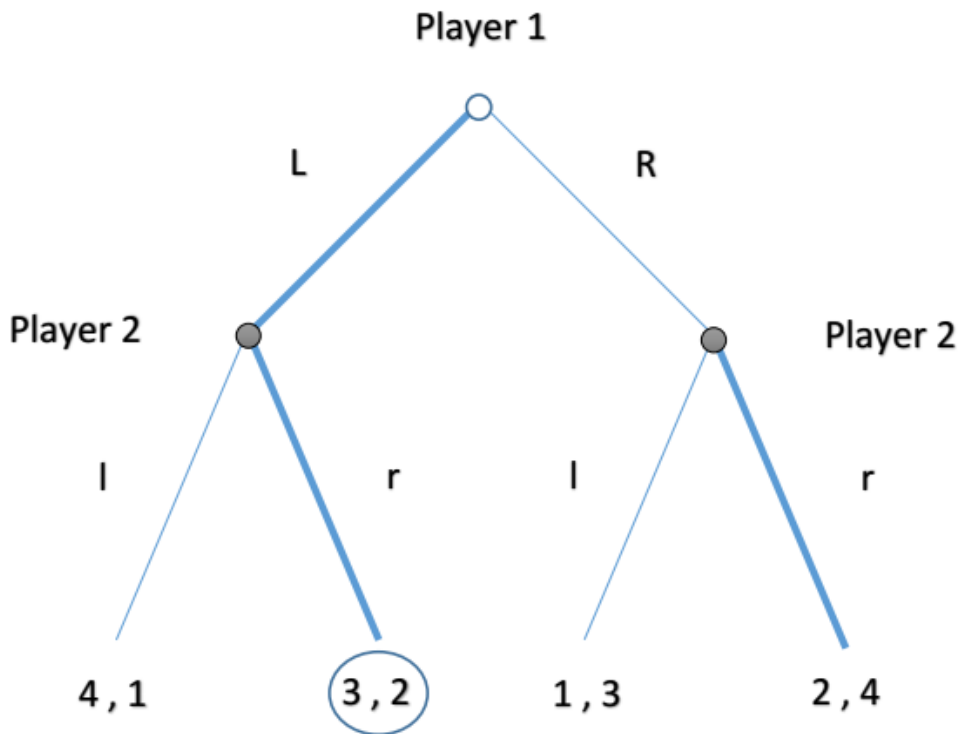
Yeandle, M., et al, *Anti-money Laundering Requirements : Costs, Benefits And Perceptions*, [website], 2005, http://www.zyen.com/PDF/AMLR_FULLL.pdf (accessed 5 April 216)

8 Appendix

8.1 Extensive Games

The most characteristic trademark for extensive games (also referred to as sequential games) is that players are moving sequentially, ergo they take turns. In the most basic form of this game, just as in a prisoner's dilemma, perfect information is assumed to prevail for all playing parties. This means, that in a sequential game where players take turns, all players know of the player's terminal nodes (the payoff for all players) and also know what decision previous players have made. In a sequential game, it is also necessary to be aware of the player's function, knowing which player can take what action and when. Lastly, the preferences of terminal nodes have to be known, to know which player prefers what outcome. ¹²⁵ To facilitate the understanding of an extensive game an example shall serve to help.

¹²⁵ M .Osborne, *An introduction to Game Theory*, New York, Oxford University Press, 2009. See chapter 5.



Figur 6 - The extensive game

Players: 1 and 2

Terminal history: (4,1) , (3,2) , (1,3) , (2,4)

Players function: Player 1 (1), Player 2 (2)

Player preferences: Player 1: $Ll > Lr > Rr > Rl$ Player 2: $Rr > Rl > Lr > Ll$

To solve for the outcome of this game, backward induction is used as an analyzing tool. Backward induction analyzes and solves a game from behind. In this example this would be done as follows: Player 2 can choose l or r and depending on the previous choice of player 2, this will yield different payoffs, if player 1 chooses L, r will be the smartest response by player 2, if player 1 chooses R, player 2 will choose r as well. Given that information is perfect and player 1's rationality, his or her choice will fall on L, simply because player 1 realizes how player 2 will react to his or her choice and by that ensuring him or herself the highest payoff. The outcome [L,r] is called subgame perfect, this is the Nash equilibrium that will be played given all players

rationality, where no player has an incentive to deviate from his or her strategy.¹²⁶

8.2 Signaling Games

The general concept

In some games, one player has information the other does not. While the informed player can make up a strategy set based on actual information, the uninformed player is forced to base their strategies on what he or she observes the informed player is doing. In other words; what signals he sends. It is for this reason that these types of games are called signaling games and can be generally defined as a strategic setting in which players can use the actions of their opponents to make inferences about hidden information.

A good example of such a setting is the labour market where employers try to distinguish between ambitious types of workers and lazy ones. The employer is the uninformed player in this game, who cannot distinguish between the two types and is therefore looking for a credible signal which can point him or her in the right direction. The informed player in this scenario is the worker who knows full well which type he or she is, but needs a credible way to signal his or her type. An example of a credible signal which could show the employer which type of worker he or she is, could be a relevant university diploma or a willingness to go through a difficult application process. If the signal is beneficial for the ambitious type but too costly for the lazy one, then we can distinguish between the two types and we have a *separating equilibrium*. If the signal is equally beneficial or costly for both types, then we cannot distinguish between them and we get a *pooling equilibrium*. A *pooling equilibrium* can also be reached, if sending the signal that characterizes ambitious players is more costly for lazy players but by sending the ambitious signal, the lazy player increases the chances of being confused with ambitious players, thus ensuring him or herself a higher payoff. In this scenario, the additional cost for the lazy player will be weighed against the belief of the employer that players signaling ambitiously also are ambitious. This will be easier to understand after examining the following model illustrating this example.¹²⁷

¹²⁶ M. Osborne. See chapter 5.

¹²⁷ M. Osborne. See chapter 10.

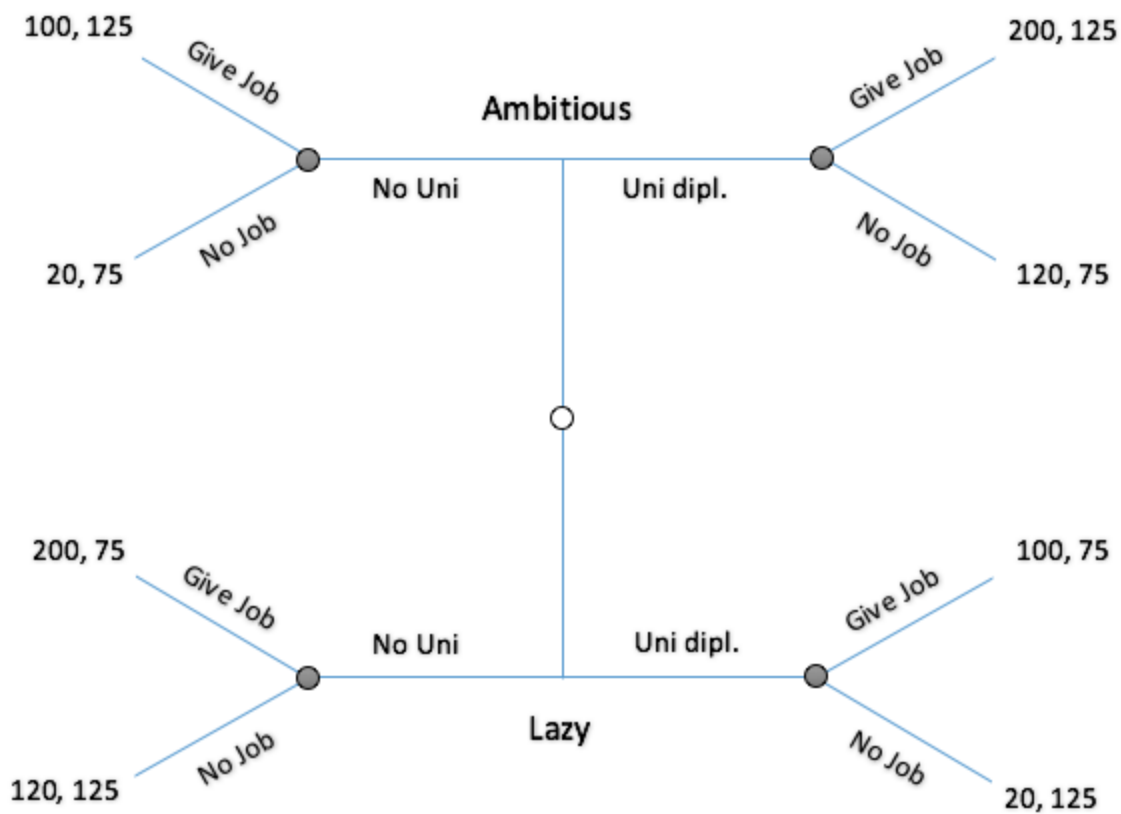


Figure 7 - The signaling equilibrium game

This model is an illustration of a classical signaling game with a *separating equilibrium*. It separates the two player types, since choosing a university degree for ambitious players always ends up in the higher payoff, regardless if a job is obtained or not. The lazy worker prefers not going to university at all times, even if he then doesn't get a job. Therefore a lazy worker will always choose "No Uni" whilst an ambitious worker always chooses "Uni dipl.". By being rational, the employer knows this and bases their decision of their action on this information. So by maxing their utility, employers choose to give the job to people attending university and to not give jobs to people who did not obtain university diplomas. The employer therefore has the belief, that all lazy people choose not to attend University, whilst ambitious people do, the outcome is thus separated. A *pooling equilibrium* can be demonstrated by partly swapping the payoff for the lazy person, if [No Uni, No Job] yields payoff 100 and [Uni, Give Job] yields 120,

even the lazy person suddenly has an incentive to go to university. This is due to the fact that the lazy person knows that if he chooses to not go to university, the employer manages to separate the two players and does not give him or her a job, if the lazy player however does go to university, he or she sends the same signal as the ambitious player, which makes it impossible for employers to separate workers with a university degree. Who gets the job, is now decided by the distribution of lazy and ambitious people, so the employer has to mix between his or her choice. This will lead to some lazy players to get the job, while some ambitious players do not. If it is worth for the lazy person to try to “trick” the employer, can be calculated as follows:

The lazy player obtains either 100 as a certain payoff, for choosing [No Uni, No Job] or get a mixture between [Uni, Give Job] = 120 [Uni, No Job] = 20. To decide which one is to prefer, one has to know the beliefs of the employer and the probability of a randomly selected worker being lazy or ambitious, the calculation can therefore be constructed as follows:

$$100 = 120 * P + 20 * (1 - P) \text{ solving for } P \text{ gives: } P=0.8$$

Where P = Probability of a worker being ambitious

With P = 0.8 , more than 80% of all workers have to be ambitious for lazy workers to choose “Uni“ over “No Uni”. Given that $P > 0,8$ a *pooling equilibrium* is reached.¹²⁸

8.3 Repetitive Games

In the most classic of strategic game examples, namely the prisoner's Dilemma, there are players with a set of actions whose strategies are determined by which action garners the highest payoff. Every player makes a decision simultaneously and under complete information, knowing full well of the payoffs and set of actions of the other players. From these game rules, optimal strategies for each player can be calculated using the method of dominant strategy equilibrium, iterative elimination of dominant strategies or Nash Equilibrium (NE). What these optimal

¹²⁸ M. Osborne. See chapter 10.

strategies will be, highly depends on if the game is a single-shot game, a finite repetitive game or an infinite repetitive game.

Single-shot game

In a standard prisoner's dilemma set up where the players only play the game once, the optimal strategy for each player can be found by identifying the unique NE for this particular game.

Defecting (D) gives a higher individual payoff than to cooperate (C) for both players, leading to a NE at [D,D].

		Player 2	
		C	D
Player 1	C	2, 2	0, 3
	D	3, 0	(1, 1)

Figur 8 - The prisoner's dilemma game

Finitely repeated game

With more than one turn added to the game, it now turns into a sequential game with perfect information and simultaneous moves. The game will end in n turns, and with both players knowing this information, a subgame perfect Nash equilibrium (SPNE) can be calculated by using backwards induction. It will quickly become apparent that the strategy to defect will be used by both players regardless of the value of n . In a game lasting for $n=5$ turns where both players are aware of the coming end and in which both players choose to begin with cooperating together, the rational player 1 would realize that defecting on the last round while player 2 chooses to cooperate would give him or her a higher payoff and player 1 would therefore break off the agreement. The rational player 2 would realize this as well and safeguard by defecting one turn earlier, giving him or her a higher payoff. This line of thought would continue with every player realizing that defecting one turn before the other is the optimal strategy, until round 1 where both players choose to defect. The inevitability of a future conflict sabotages cooperation in the present.

Infinitely repeated game

In this game the amount of turns is set to $n=\infty$, making the endpoint unfixed and the behaviour of the players vastly different. The setting of an infinite time scale is not so much about illustrating a real-life situation, as it is capturing the perception of players who do not know when the game will end. Going back to the previous prisoner's dilemma example, the strategy to always defect is now not so clear, since backward induction has been rendered impossible. A new strategy is needed for the rational players to make a decision.

In the long run both players benefit from a mutual cooperation, since no "last game" is distinguished. This holds true given both players' rationality and a relatively high discount rate. The discount rate is used to calculate how much a player values a payoff today, which is made in the future. There is justified reason to assume a player prefers a payoff, the sooner it gets paid out. Therefore CC (both players cooperating) might not be the only solution in an indefinitely repeated game. Another strategy could be to defect in the first game, while the other player assumed a cooperation, thus obtaining a payoff of 3 in the first game and afterwards going back to the payoff of 1 in the DD NE. When it is better to choose cooperation and when not, depends on the discount rate.

The breakeven discount rate in which a player is indifferent between the two strategies can be calculated as follows:

$$[CC] * 1/(1 - a) = [DC] + a * ([DD] * (1/(1 - a)))$$

Formula 1 - The general formula

Where [CC] denotes the payoff for player 1 for both players cooperating

[DC] denotes the payoff for player 1 for player 1 defecting and player 2 cooperating

[DD] denotes the payoff for player 1 for both players defecting.

Since the game is mirrored, the payoff for player two looks exactly the same.

More concrete for this particular example:

$$2 * 1/(1 - a) = 3 + a * (1 * (1/(1 - a)))$$
$$a = 0.5$$

Formula 2 - The concrete formula

In this example, δ has to equal to 0.5 for a player to be indifferent between defecting for all eternity or cooperating for all eternity (assuming the other player cooperates on the first turn, thus giving the player pay off 3 in the first move). Any discount rate above 0.5 leaves both players strictly better off when choosing to cooperate with each other. ¹²⁹

		Player 2	
		C	D
Player 1	C	2, 2	0, 3
	D	3, 0	1, 1

Figure 9 - The infinitely repeated prisoner's dilemma game

¹²⁹ M. Osborne. See chapter 15.

8.4 Interview Questions

Questions for the Bitcoin Traders

What is your occupation in the company?

How many years of experience do you have in the Bitcoin business?

What is your company's experience of money laundering? Is it a constantly occurring problem?

How big of a priority is it to combat money laundering in your company?

What Anti-Money Laundering directives are you using today?

What is your professional opinion about your company's current AML directives?

Are they implemented voluntarily or by the EU or by your corresponding government?

Are the current AML directives adequately implemented according to your professional opinion? If not, what could have been done differently?

Would you implement and finance an improved AML policy, given that it more effectively prevents money laundering? Would you implement it given it is subsidized by the corresponding government?

How do your customers respond to the current AML directives put in place?

How do you think they would respond to stricter directives that would lead to a decrease in anonymity for your customers?

Do you think they would respond better to stricter directives if they would be given a financial incentive? For example a financial reward for more personal information given?

Would you consider financing this reward if it serves the purpose to combat money laundering more effectively? Would you implement the rewarding system if the corresponding government subsidizes the reward?

Do you consider the KYC-information provided by your customers to be trustworthy?

What do you consider suspicious customer behavior?

What is the standard procedure when a customer acts suspiciously?

Can you give an estimation on how many suspicious customers there are in your system?

Do you check the past transactions of your customers in the Bitcoin? If yes, in what cases? If no, why not?

Do you believe that money laundering would be more effectively combated if your customers revealed more personal information about themselves?

Questions for the Financial Inspection Unit (Swedish Original)

Vilka är dina arbetsuppgifter?

Hur många års erfarenhet har ni av penningtvättsbekämpning?

Vilken är er kunskap rörande Bitcoin?

Vilken är er kunskap rörande Bitcoin penningtvätt?

Hur storskaligt är Bitcoinpenningstvätt i jämförelse med penningtvätt i fiatvaluta?

Varför är penningtvätt ett problem?

Hur skiljer sig Bitcoinpenningtvätt från vanlig penningtvätt?

Hur motverkar ni penningtvätt i fiatvaluta i dagsläget?

Hur motverkar ni penningtvätt i Bitcoin i dagsläget?

Hur regleras penningtvätt i Bitcoinmarknaden idag?

Vem reglerar penningtvätt i Bitcoinmarknaden idag?

Hur ser ni på regleringen idag? Vad är bra och vad är dåligt?

Regleras Bitcoinhandlarna i dagsläget med avseende på penningtvätt?

Hur balanserar ni er verkställning av anti-pengatvätts direktiv, så att de effektivt motverkar penningtvätt utan att kväva Bitcoinmarknaden?

Tror ni att mer utförligare uppgifter om Bitcoinanvändarna till Bitcoinhandlarna skulle effektivisera penningtvättsbekämpningen?

Hur tror ni att Bitcoinanvändare hade reagerat på anti-pengatvätts direktiv som minskar anonymiteten?

Tror ni att de skulle reagera bättre på ett sådant direktiv om Bitcoinanvändarna skulle få ett finansiellt incitament? Till exempel en belöning för givandet av mer personlig information.

Om ja, vem skulle kunna bekosta det finansiella incitamentet?

Är det tekniskt möjligt att införa ett sådant belöningsystem?

Vilka uppgifter om Bitcoinanvändaren skulle vara hjälpsamma för att motverka penningtvätt?

Har ni något förslag på hur AML direktiven skulle kunna förbättras?

Questions for the Financial Inspection Unit English Translation

Which are your work tasks?

How many years of experience do you have combating money laundering?

What is your knowledge of Bitcoin?

What is your knowledge of money laundering in Bitcoin?

How big is money laundering in Bitcoin compared to money laundering in fiat currencies?

Why is money laundering a problem?

How does money laundering in Bitcoin differ from money laundering in fiat currencies?

How do you combat money laundering in fiat currencies as of today?

How do you combat money laundering in Bitcoin as of today?

How is the Bitcoin market currently regulated?

Who regulates the Bitcoin market as of today?

How do you see the current regulations? What is good and what is bad?

Are the Bitcoin traders currently regulated considering AML directives?

How do you balance the execution of AML directives so that they effectively combat money laundering without constraining the Bitcoin market?

Do you think more personal information about the user for the trader would lead to an improved money laundering prevention?

How do you think Bitcoin users would respond to stricter directives that would lead to a decrease in anonymity?

Do you think they would respond better to stricter directives if they would be given a financial incentive? For example a financial reward for more personal information given?

If so, who should bear the cost of the financial reward?

Is it feasible to introduce such a system from a technical perspective?

What kind of information about the user would be useful to combat money laundering?

Do you have any suggestions on how the AML directives could be improved?

Questions for Emil Elgebrant (Swedish Original)

Vilka är dina arbetsuppgifter?

Hur många års erfarenhet har du av att jobba med Bitcoin?

Vilken är er kunskap om penningtvätt i fiat valuta?

Vilken är er kunskap om penningtvätt i Bitcoin?

Hur regleras penningtvätt i fiatvalutor i dagsläget?

Hur skiljer sig penningtvätt i fiatvalutor mot penningtvätt i Bitcoin från ett juridiskt perspektiv?

Är det problematiskt att tillämpa befintliga regelverk om penningtvätt på Bitcoinmarknaden?

Är Bitcoinmarknaden i Sverige reglerad med avseende på penningtvätt idag och i så fall hur?

Vilka juridiska aspekter måste tas i åtanke när Anti-Money Laundering (AML) direktiv implementeras på Bitcoinmarknaden i Europa?

Tror du att implementeringen av AML-direktiv i Europa påverkas av att bitcoin klassifieras olika i olika EU-länder (t.ex. finansiellt instrument i Tyskland, kapital egendom i Norge)?

Vilka aktörer på Bitcoinmarknaden är lättast att reglera, med avseende på penningtvätt, från ett juridiskt perspektiv?

Är det juridiskt möjligt att reglera Bitcoinhandlarna? Om ja, hur? Om nej, varför inte?

Hur tror ni att Bitcoinanvändare hade reagerat på anti-pengatvätts direktiv som minskar anonymiteten?

Tror ni att de skulle reagera bättre på ett sådant direktiv om Bitcoinanvändarna skulle få ett finansiellt incitament? Till exempel en belöning för givandet av mer personlig information.

Vem skulle kunna bekosta det finansiella incitamentet?

Tror ni att mer utförligare uppgifter om Bitcoinanvändarna till Bitcoinhandlarna skulle effektivisera penningtvättsbekämpningen?

Vilka uppgifter skulle vara hjälpsamma för att motverka penningtvätt?

Har ni något förslag på hur AML direktiven skulle kunna förbättras?

Questions for Emil Elgebrant (English Translation)

Which are your work tasks?

How many years of experience do you have in the Bitcoin business?

What is your knowledge on money laundering in fiat currencies?

What is your knowledge on money laundering in Bitcoin?

How is money laundering regulated in fiat currency as of today?

How does money laundering in Bitcoin differ from money laundering in fiat currencies seen from a juridical perspective?

Is it problematic to apply the current AML directives on the Bitcoin market?

Is the Bitcoin market in Sweden regulated on the account of money laundering and if so, how?

What kind of juridical aspect must be kept in mind when applying AML directives to the Bitcoin market in Europe?

Do you believe that the implementation of AML directives in Europe is influenced by the fact that different countries classify Bitcoin differently? (for example, a financial instrument in Germany, capital property in Norway)

What agents on the Bitcoin market are easiest to regulate regarding AML policies, from a juridical perspective?

Is it juridically possible to regulate the Bitcoin traders? If yes, how? If no, why not?

How do you think Bitcoin users would respond to stricter directives that would lead to a decrease in anonymity?

Do you think they would respond better to stricter directives if they would be given a financial incentive? For example a financial reward for more personal information given?

If yes, who should bear the cost of the reward?

Do you think more personal information about the user for the trader would lead to an improved money laundering prevention?

What kind of information about the user would be useful to combat money laundering?

Do you have any suggestions on how to more effectively combat money laundering?

Question for Jonathan Jogenfors (Swedish Original)

Vilka är dina arbetsuppgifter?

Hur många års erfarenhet har du av att jobba med Bitcoin?

Vilken är er kunskap om penningtvätt i fiat valuta?

Vilken är er kunskap om Bitcoin penningtvätt?

Hur skiljer sig Bitcoinpenningtvätt från vanlig penningtvätt?
Regleras Bitcoinhandlarna i dagsläget med avseende på penningtvätt?
Hur ser ni på regleringen idag? Vad är bra och vad är dåligt?

Hur effektiva är Bitcointraders på att motverka penningtvätt i dagsläget?
Enligt din professionella åsikt, agerar Bitcointraders alltid i statens bästa intresse?

Hur tror ni att Bitcoinanvändare hade reagerat på anti-pengatvätts direktiv som minskar anonymiteten?

Tror ni att de skulle reagera bättre på ett sådant direktiv om Bitcoinanvändarna skulle få ett finansiellt incitament? Till exempel en belöning för givandet av mer personlig information.

Är det tekniskt möjligt att införa ett sådant belöningssystem?

Om ja, vem skulle kunna bekosta det finansiella incitamentet?

Tror ni att mer utförligare uppgifter om Bitcoinanvändarna till Bitcoinhandlarna skulle effektivisera penningstvättsbekämpningen?

Vilka uppgifter av användarna skulle vara hjälpsamma för att motverka penningtvätt?

Har du som teknisk Bitcoinexpert ett förslag på en lösning som kan bekämpa penningtvättningen i Bitcoin?

Question for Jonathan Jogenfors (English Translation)

Which are your work tasks?

How many years of experience do you have in the Bitcoin business?

What is your knowledge on money laundering in fiat currencies?

What is your knowledge on money laundering in Bitcoin?

How does money laundering in Bitcoin differ from money laundering in fiat currencies?

Are the Bitcoin traders regulated with AML directives?

How do you see the current regulations? What is good and what is bad?

How efficient are Bitcoin traders in combating money laundry as of today?

According to your professional opinion, do Bitcoin traders always act in the state's best interest?

How do you think Bitcoin users would respond to stricter directives that would lead to a decrease in anonymity?

Do you think they would respond better to stricter directives if they would be given a financial incentive? For example a financial reward for more personal information given?

Is it feasible to introduce such a system from a technical perspective?

If so, who could bear the cost of the reward?

Do you think more personal information about the user for the trader would lead to an improved money laundering prevention?

What kind of information about the user would be useful to combat money laundering?

Do you as a technical expert on Bitcoin have a suggestion on how to more effectively combat money laundering?

8.5 Interview Guides Sent to Bitcoin Traders

Hello,

We are two master students from Linköping University who are writing our master's thesis about combating money laundering in Bitcoin. We are wondering if someone at your organization would agree to a Skype interview and answer some questions regarding this issue? Preferably someone with a good deal of insight into your Bitcoin operation in Europe, as our paper is focused on that geographical area in particular.

The interview is estimated to not take more than 30 min and the interviewee can be anonymous if so wished.

Yours sincerely

David and Felix