THE UNIVERSITY OF AMSTERDAM

Is the FATF travel rule effective in the fight against money laundering via virtual currencies?

By

Marte Schaaf
(10720855)

January 2021

A paper submitted in partial fulfillment of the requirements for the Master Private Law (Commercial Law)

Supervisors: D.M. Weber, J.M. Vazquez & R.A. Michgels

Abstract

This thesis seeks to answer the question whether the FATF travel rule is an effective means to combat money laundering via virtual currencies. The travel rule, also known as 'recommendation 16', requires virtual asset service providers (VASPs) to collect and exchange information about their customers. For the purpose of preventing and detecting money laundering the travel rule aims to increase the amount of information available about users transferring virtual currencies.

This thesis comprises of multidisciplinary, descriptive research and statements that are both predictive and normative. To gain a deeper understanding of the properties of virtual currencies, this thesis includes a multidisciplinary section exploring Bitcoin as a peer-to-peer payment system and 'bitcoin' as a currency for transmitting value. Subsequently, this thesis analyses the risks of money laundering associated with virtual currencies and the current legal framework addressing those risks. This thesis will be concluded by predictive and normative statements about the effectiveness of the FATF travel rule.

The findings show that the travel rule is an effective first step in the fight against money laundering. The application of a risk-based approach (RBA) is crucial to the effectiveness of the travel rule. A risk-based approach allows VASPs to focus on financial activities with the highest risk factor. This thesis stresses that a part of the transactions using virtual currencies will remain outside the scope of the travel rule since users can also transact without a VASP. The application of a RBA allows for this latter kind of transactions to be labelled as 'riskier' from an anti-money laundering (AML) perspective. The presence of potential suspicious activity should encourage further investigation of the sources of funds that allow the users to be identified. Subsequently, this thesis discusses the sunrise issue. Jurisdictions will implement the travel rule according to their own implementation deadlines. Eventually, most jurisdictions are expected to implement the revised FATF recommendations. A coordinated approach across jurisdictions is required to mitigate the risks during the sunrise period. While the travel rule and other AML requirements are likely to bring about a more harmonized and robust AML framework, money laundering via virtual currencies will remain an issue that needs to be closely monitored.

Table of Contents

Chapter 1 Introduction

The idea of virtual currency is as old as the internet itself. In the 1990s, a movement of cryptographers called ‘Cypherpunks’ dedicated themselves to the creation of a currency based on cryptographic proof and liberated from the oversight of governments and banks.[1] For almost two decennia, all efforts to create a virtual currency were in vain[2] until, in 2008, the momentum changed. An alias ‘Satoshi Nakamoto’ revealed a white paper in which many of the earlier ideas had been combined: ‘Bitcoin: A Peer-to-Peer Electronic Cash system’.[3]

Bitcoin was invented on October 31st, 2008, less than two months after the bankruptcy of Lehman Brothers. The financial crisis underscored the fragilities of the existing financial system. The health of the financial system depended on third parties, like banks, of which people have no choice but to trust they will make the right decisions with their given money.[4] The inherent weaknesses of a payment system based on trust were an important subject of Satoshi Nakamoto’s writings.[5]

Bitcoin is a collection of concepts and technologies which, together, form the basis of a digital money ecosystem.[6] The premise of the Bitcoin is to allow electronic payments to be sent directly without the interference of third parties, like banks, PayPal, or credit card companies.[7] Bitcoin is based on a trustless system – users in the peer-to-peer network do not need to know or trust each other for the system to function. Bitcoin does not eliminate the need for trust entirely but allows people to trust in abstract concepts rather than institutions or other third parties.[8]

[1] Wallace, *Wired* 23 November 2011

[2] Ecash, an anonymous system launched in the early 1990s by cryptographer David Chaum, failed in part because it depended on the existing infrastructures of government and credit card companies. Other proposals included bit gold, RPOW, b-money. Wallace, *Wired* 23 November 2011

[3] Nakamoto 2009

[4] Arslanian & Fischer 2019, p. 95, *True Energy Crypto* 28 September 2017, 05:08m

[5] Nakamoto 2009

[6] Antonopoulos 2014, chapter 1, par. 1

[7] Nakamoto 2009

[8] Taçoğlu, *Binance Academy* 2020 par. 3

The currency of Bitcoin, called bitcoin, is used to transmit value among participants in the bitcoin network.[9] Since bitcoin is not a generally accepted payment method, it is not considered money.[10] Yet, mainstream adoption of virtual currencies is gaining traction by the day, with businesses such as Amazon and Starbucks allowing customers to pay in bitcoin.[11]

Virtual currencies and distributed ledger technologies have the potential to generate benefits. By eliminating the need for a central third party, virtual currencies could make payment transfers significantly easier and faster, charging lower transaction fees than those changed by traditional institutions.[12] Virtual currencies can also improve access to financial services, and thus promote financial inclusion.[13] Beyond payment systems, distributed ledger technologies can be applied to a variety of markets, and function as a fast, accurate and secure record keeping system.[14]

At the same time, virtual currencies carry a risk of being misused for illegal activities.[15] A pressing and immediate concern is the use of virtual currencies for the purpose of money laundering. Most virtual currencies are pseudo-anonymous – meaning that users are not easily or immediately identified on the distributed ledger technology underpinning that particular asset type. Combination with the speed and ease with which transactions can be carried out on a global scale, this feature renders virtual currencies susceptible to misuse by money launderers.[16]

[9] Bitcoin is a cryptography-based virtual currency also known as cryptocurrency

[10] Madeira, *Cointelegraph* 29 February 2020, par. 13,

[11] *Chainalysis* January 2020, p. 5

[12] He 2016 (SDN/16/03), p. 6. The potential benefits such as claimed cost advantage need to be further analyzed, whether they remain if virtual currencies become subjected to regulatory requirements.

[13] The software can be run on a wide range of computing devices, including smartphones. According to the World Bank, 1.7 billion adults around the world remain unbanked, but two-thirds of them own a mobile phone. Virtual currencies can provide an alternative payment method to under- and unbanked Madhavji, *Altcoin Magazine* 26 November 2019, par. 1 & *The World Bank* 19 April 2018, par 3

[14] He 2016 (SDN/16/03), p. 6

[15] This includes, among others, tax evasion, terrorist financing, consumer protection, darknet markets, scams. *Chainalysis* January 2020, p. 6, & Houben & Sneyers, PE 619.024 2018, p. 9-10

[16] Houben & Sneyers, PE 619.024 2018, p. 53

For the purpose of combating money laundering via virtual currencies, regulators recognized the need for a harmonized approach among jurisdictions. However, the decentralized nature of virtual currencies does not easily fit within traditional regulatory models. Decentralized systems eliminate the role of a central authority such as an issuer or payment processor.[17] Under such circumstances, the question then becomes "who to regulate?" An interesting development towards answering this question is the emergence of service providers. These businesses offer products and services to facilitate obtaining, storing, and using virtual currencies.[18]

In response to the rise of service providers, the Financial Action Task Force (FATF), an international money laundering and terrorist financing watchdog, updated its recommendations.[19] The update of the FATF in 2019 requires a broad range of service providers, called virtual asset service providers (VASPs) to be subjected to regulations already applicable to traditional financial institutions, including the travel rule (or recommendation 16). The travel rule aims to bring a further layer of transparency to transactions using virtual assets, including virtual currencies.[20]

The travel rule introduced by the FATF reaches beyond the requirements posed by The Fifth Anti-Money-Laundering Directive (AMLD5). [21] Entering into force in 2018, AMLD5 places anti-money laundering (AML) requirements on crypto-fiat exchanges and custodian wallet providers, the most common way for users to enter and interact with the virtual currency market.[22]

In terms of travel rule implementation, several unique technical and legal challenges must be addressed.[23] Despite these challenges, jurisdictions implement the travel rule into their national law. On 23 September 2020, the Dutch central bank announced that the Sanctions

[17] He, 2016 (SDN/16/03), p. 9

[18] Houben & Sneyers, PE 619.024 2018, p. 26-27, He, 2016 (SDN/16/03), p. 25

[19] FATF (2012-2020)

[20] FATF (2012-2020), p. 76-77

[21] Directive (EU) 2018/843

[22] Houben & Sneyers, PE 619.024 2018, p. 27

[23] For example, how to transmit data? How to ensure that data is being stored and transmitted in line with privacy and data regulations? Shin, *Unchained* 4 August 2020, 58:00m

Act (Sanctiewet 1977 – SW) obliges virtual currency service providers to identify the counterparty involved in a transaction.[24] As jurisdictions are implementing the travel rule, a crucial question needs to be answered: *is the FATF travel rule effective in the fight against money laundering via virtual currencies?*

This thesis aims at answering this question. To do so, it analyses the topic of research along three sections. The first section explains the peer-to-peer electronic payment system that underpins virtual currencies. An understanding on this matter will help to understand the identified money-laundering risks associated with virtual currencies. There are, however, many virtual currencies, each with their own distributed ledger, standards, and operating procedures. To not overcomplicate the subject, this thesis solely discusses Bitcoin and a transaction with bitcoin, the first established virtual currency. To further clarify the virtual currency ecosystem, this section also discusses service providers that offer products and services to facilitate obtaining, storing, and using virtual currencies. In the second section, this thesis explores the money laundering risks associated with virtual currencies and provides an overview of AML frameworks that aim to mitigate these risks. For this purpose, this section discusses AMLD5, followed by the FATF travel rule, the core regulation covered by this thesis. The third section aims to answer the main question and explores whether the FATF travel rule is effective in the fight against money laundering.

[24] DNB, *De Nederlandse Bank* 23 september 2020

Chapter 2 The rise of Bitcoin

2.1 Introduction

Back in 1999, Milton Friedman mentioned in an interview that the internet is going to be one of the major forces for reducing the state of power: *'the one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A'*.[25] Nine years later, in 2008, when the world experienced the financial crisis, Satoshi Nakamoto, proposed Bitcoin, a peer-to-peer electronic cash system.[26] Transactions using bitcoin are pseudonymous – allowing B to receive funds from A, without B knowing A or the other way around.

Since its creation, bitcoin has experienced significant highs and lows. To better understand this, it is essential to discuss some elements of its history. The Bitcoin software was made available to the public for the first time in 2009. However, since it had never been traded, it was impossible to assign a monetary value. [27] This changed on May 22nd in 2010, when someone bought two pizzas for 10,000 (BTC), the equivalent of US$41 at the time. [28] It was very difficult to acquire bitcoin, and, thus, exchanges emerged were users could buy, store and trade virtual currencies.[29] In the following years, bitcoin increased in popularity, and experienced an important boom in 2013. As the idea of a decentralized and a pseudonymous currency caught on, alternative virtual currencies emerged which sought to deliver other advantages, for example faster speed of settlement or increase anonymity. These alternative virtual currencies also became known as altcoins.[30]

Over the next two years, the price of bitcoin started to decline. The decline was mainly caused by public events such as bitcoin's association with Silk Road marketplace arrests and the hack

[25] Cawrey, *Coindesk* 5 March 2014

[26] Nakamoto 2009

[27] Marr, *Bernard Marr & Co, 2010*

[28] At today's prices the pizza would be worth US$115,730,292.87, bitcoin's price is set at 1 BTC would be US$ 11,565.21 see also xe.com & Marr, *Bernard Marr & Co, 2010*

[29] *True Energy Crypto* 28 September 2017, 17:40m

[30] Among the first to emerge were Namecoin and Litecoin see Marr, *Bernard Marr & Co, 2011*

of bitcoin exchange Mt. Gox.[31] Yet, the usage of bitcoin increased during that time, mainly due to an increase in the number places where bitcoin could be bought and spent.[32]

From 2015 on, the tide slowly started to change in favor of bitcoin and the broader virtual currency ecosystem.[33] Suddenly, Bitcoin was being discussed on media platforms such as Bloomberg. Additionally, the technology behind Bitcoin, blockchain, emerged in different parts of the traditional financial system, even outside the context of virtual currencies. Blockchain, a type of distributed ledger technology (DLT), can be applied in various sectors and has a wide array of potential applications, like shortening the time to settle securities transactions, for example, and decentralizing online services on the basis of smart contracts.[34]

While the excitement about the potential of blockchain technology continues to grow, the price of bitcoin and many other virtual currencies crashed in 2018.[35] The causes remain unclear, but there are several explanations, including concerns about regulation, light trading volumes in Asia, and an unsustainable price run-up.[36] The crash of 2018 revived the debate between optimists, who claim that virtual currencies will alter payments around the world, and pessimists, who claim that they will eventually collapse.[37] Underlying these differing views is disagreement about what virtual currencies are and how they work.[38] In the following pages, this chapter will explore the Bitcoin protocol and the transaction structure bitcoin. It also discusses the emergence of service providers within the virtual currency industry.

[31] Slik Road is an online marketplace for illegal goods such as drugs, and uses bitcoin as its chief form of currency. With bitcoin, anyone could purchase drugs or other illegal goods without revealing their identities. Mt Gox allowed users to buy, sell, convert and keep their bitcoins and fiat currencies with the exchange. A massive hack led to the loss of 744,408 bitcoins due to a lack of security. Arslanian & Fischer 2019, p. 106-107, Lemereis *rtlnieuws* 25 February 2014

[32] Arslanian & Fischer 2019, p. 106

[33] Arslanian & Fischer 2019, p. 107

[34] Arslanian & Fischer 2019, p. 103

[35] The price of bitcoin closed at US$4,000 Arslanian & Fischer 2019, p. 108

[36] Williams-Grut, *Insider* 17 January 2018, par. 3 ff.

[37] Arslanian & Fischer 2019, p. 108 and Narayanan & J. Bonneau 2016, p. xvii

[38] Narayanan & J. Bonneau 2016, p. xvii

2.2 Bitcoin: a peer-to-peer electronic cash system

Bitcoin is a payment system based on an intellectual experiment that allows people to bypass the central banking system.[39] Creating a distributed and reliable system without any central authority to enforce trust is extremely challenging. A thought experiment also known as the Byzantine General's Problem illustrates the issue of trust between parties in a decentralized system in terms of a story:[40]

> *Imagine a military operation in which several generals and their armies are positioned around a rebel city. Each general and army is based in a separate camp and communication between the generals is only possible by messengers who must cross the open terrain from one camp to another. In this comparison, only a coordinated attack by all generals leads to victory.[41] However, some of the generals or messengers may be traitors, trying to prevent the other generals from reaching agreement which will result in a lost battle.*

The challenge is to agree on a course of action by exchanging information within an unreliable and potentially compromised network.[42] The problem faced by the Byzantine generals is similar to the problems faced by distributed computing systems: whilst in the Byzantine army this could be a general communicating false information or a messenger not passing on the message correctly, it could be someone seeking to process fraudulent transactions in distributed technology.[43] In the specific case of virtual currencies, the possibility to spend the same coin twice would fundamentally undermine trust in the system, also known as the problem of double-spending.[44] Bitcoin solves the problem of double-spending by introducing the concept of Proof-of-Work, which allows transactions in a peer-

[39] Nakamoto 2009, p. 1

[40] The Byzantine Generals Problem was introduced by mathematicians Leslie Lamport, Robert Shostak and Marshall Pease in 1982. It explains a computer related problem consisting in finding an agreement by communicating through messages between different components of the network. Küfner, *Nakamo.to* 15 August 2018, par. 2 & Gatti, *The Cryptonomist* 4 August 2019, par 2 ff.

[41] *Bitpanda Academy* 2014, par. 3

[42] Antonopoulos 2014, chapter 1

[43] Küfner, *Nakamo.to* 15 August 2018, par. 3

[44] *Bitpanda Academy* 2014, par. 1

to-peer network to be validated and cleared.[45] It is 'trustless' because participants in the bitcoin network are not required to trust anything except for the Proof-of-Work algorithm that underpins the system.[46]

To explain the problem of double-spending in more detail, the term 'bitcoin network' refers to a collection of independent computers running the Bitcoin software, also referred to as nodes.[47] Everyone can join the bitcoin network, transfer money, and participate in the authorization of transactions.[48] Users in the network that wish to transfer bitcoins send nodes transaction messages. Imagine that Alice wants to purchase a book at Bob's bookstore. When Alice wants to pay Bob, what she actually does is broadcast a transaction to all nodes that make a peer-to-peer network (figure 1).[49]

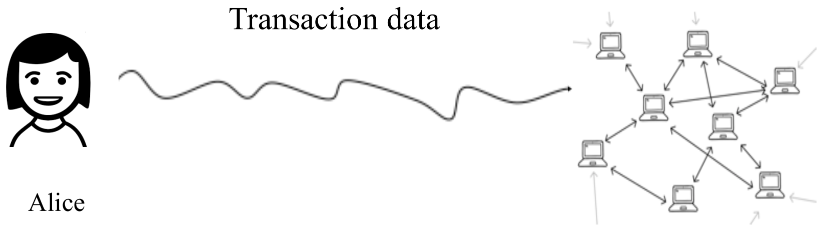


Figure 1: P2P network consisting out of computers (nodes)

Nodes pass on information about new transactions by sending each other messages.[50] However, nodes do not hear about new transactions instantly. Instead, transactions travel across nodes within the network by being passed from one to another. The nodes, then, store transactions in a memory pool. The memory pool may best be understood as a waiting room for new transactions .[51]

[45] Antonopoulos 2014, chapter 10, par. 1

[46] Taçoğlu, *Binance Academy* 2020

[47] Narayanan & J. Bonneau 2016, p. 28

[48] Antonopoulos 2014, chapter 8, par. 1

[49] Narayanan & J. Bonneau 2016, p. 30

[50] Laurence 2019, p. 23

[51] *Learn me a bitcoin* 2015, Mining, Memory Pool

Due to the way transactions travel within the network, it is possible to create conflicting transactions. For example, Alice can create two separate transactions spending the same bitcoin and send both of these transactions into the network at the same time (double-spending). [52] In figure 2, Alice purchases a book at Bob's bookstore, and buys a drink at Clements's bar using the same bitcoin. In this situation, the network would be conflicted about whether Alice wants to purchase the book or the drink.

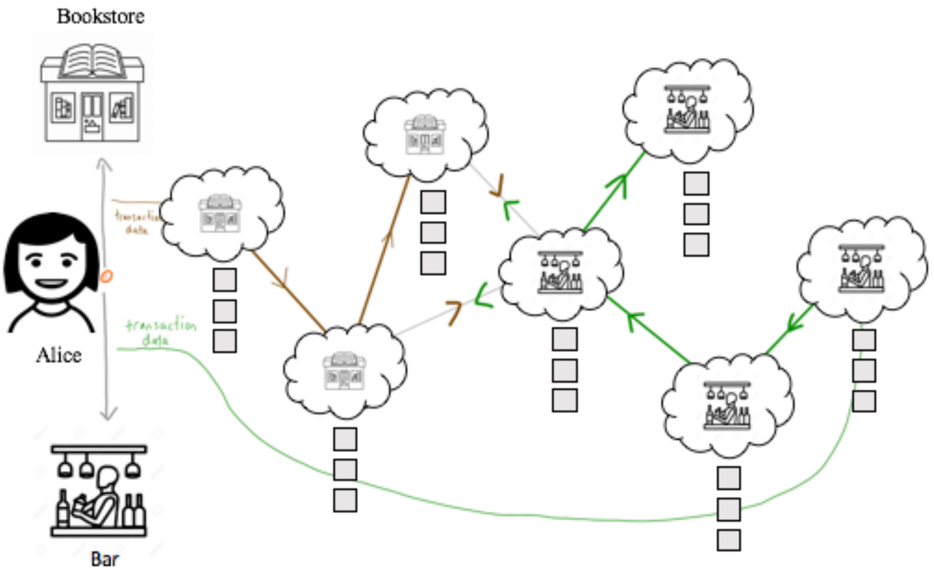


Figure 2: double-spending

Bitcoin solves the problem of double-spending by the concept of Proof of Work, a consensus algorithm that allows a group of independent computer systems to agree on the chronological order of transactions.[53] The Proof of Work mechanism may be thought of as a network-wide competition in which a group of nodes in the network, called miners, solve a complex computational problem.[54] This process is commonly referred to as mining, and forms the mechanism by which transactions are validated and cleared.[55]

The mining process begins by selecting multiple transactions from a nodes memory pool and creating a 'candidate block'; a temporary block that will be either validated or discarded by

[52] *Learn me a bitcoin* 2015, Mining

[53] Nakamoto 2009 p. 2

[54] Anyone may operate as a miner. However, mining is a very energy-intensive possess and to solve the problem first miners need a lot of computing power. Antonopoulos 2014, chapter 10

[55] Antonopoulos 2010, chapter 10

the network (figure 3).[56] Subsequently, miners in the network will compete with each other by solving a complex mathematical puzzle with the data in that specific block.[57] The Bitcoin protocol requires a majority of the nodes to agree that the miner has solved the puzzle. Each miner that successfully solves the puzzle is allowed to record the set of transactions in that specific block and to collect a reward in bitcoins. The more computing power a miner has, the better are its chances of solving the puzzle first.[58]

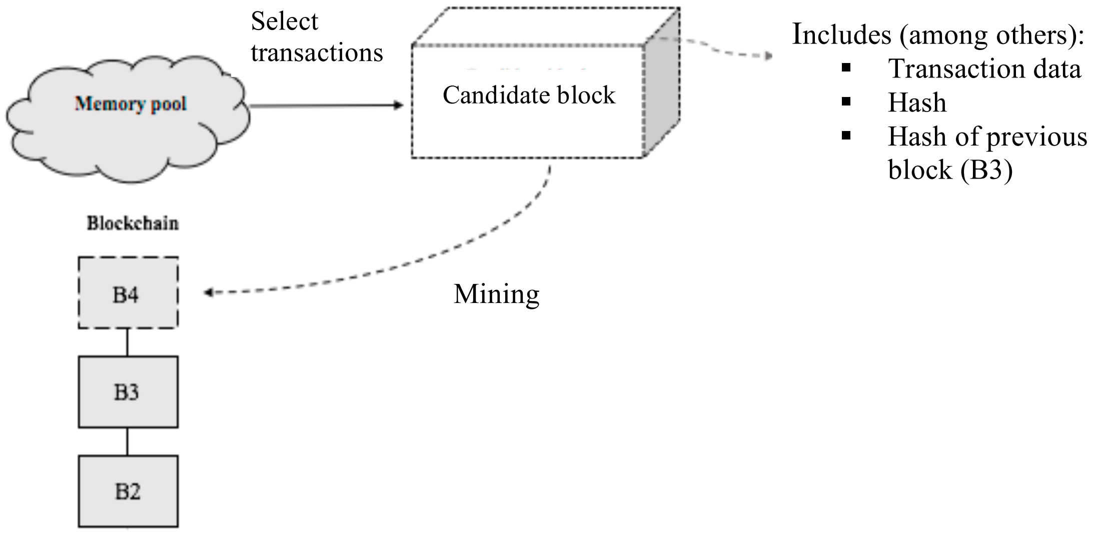


Figure 3: Mining

When Alice spends the same bitcoin twice, the one transaction located in the ‘winning’ candidate block will be added to the blockchain, also referred to as the ledger. A ledger is a file containing a list of all transactions ever made which all participants in the bitcoin network accepts as the authoritative record of ownership.[59] Everyone in the network shares a copy of this file, and it updates roughly every 10 minutes to include the latest transactions (figure 4).[60]

[56] *Learn me a bitcoin* 2015, Candidate block & Mining

[57] *Learn me a bitcoin* 2015, Mining

[58] Mining is also the process by which new coins are created. Each miner that successfully solves the puzzle is rewarded with a brand-new bitcoin (and a transaction fee). Bitcoin mining, thus, decentralizes the currency-issuance and clearing functions of a central bank. Antonopoulos 2014, chapter 10, par. 1

[59] Antonopoulos 2014, chapter 10

[60] *Learn me a bitcoin* 2015, Mining

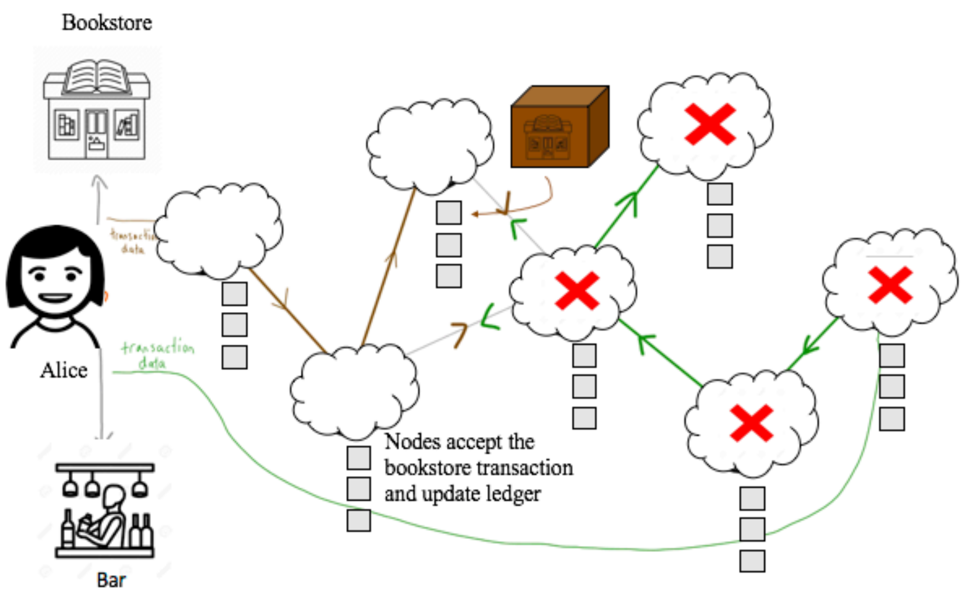
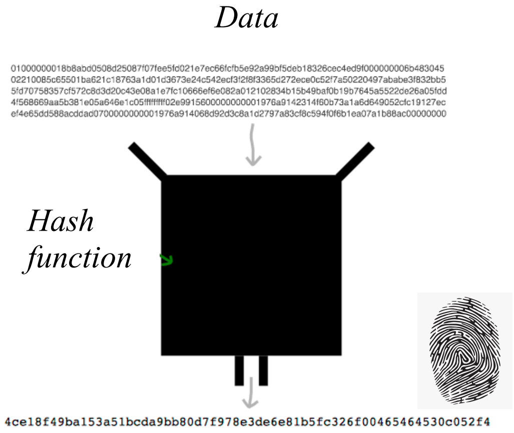


Figure 4: how Bitcoin solves the problem of double spending

With the transaction added to the ledger, it is necessary that the blockchain cannot be tampered with. The blockchain is secured by hashes, the Proof of Work mechanism, and its decentralized nature.[61]

Each block within the blockchain is identified by a hash.[62] A hash is created by a computer program that takes all data, scrambles it, and gives it a unique fixed length result. Hashes are also called digital fingerprints – presenting a unique identification code (figure 5).[63]



```
0100000018b8abd0508d25087f07fee5fd021e7ec66fcfb5e92a99bf5deb18326cec4ed9f000000006b483045
02210085c65501ba621c18763a1d01d3673e24c542ecf3f2f8f3365d272ece0c52f7a50220497ababe3f832bb5
5fd70758357cf572c8d3d20c43e08a1e7fc10666ef6e082a012102834b15b49baf0b19b7645a5522de26a05fdd
4f568669aa5b381e05a646e1c05ffffffff02e991560000000000001976a9142314f60b73a1a6d649052cfc19127ec
ef4e65dd588acddad0700000000001976a914068d92d3c8a1d2797a83cf8c594f0f6b1ea07a1b88ac00000000
```

```
4ce18f49ba153a51bcda9bb80d7f978e3de6e81b5fc326f00465464530c052f4
```

Figure 5: hash function

[61] *Simply Explained* 13 November 2017, 2:08m

[62] *Learn me a bitcoin* 2015, Block Header

[63] *Learn me a bitcoin* 2015, Hash function

Blocks on the chain contain a hash of the previous block and, so, enable a chronological order of the chain (figure 6). [64]

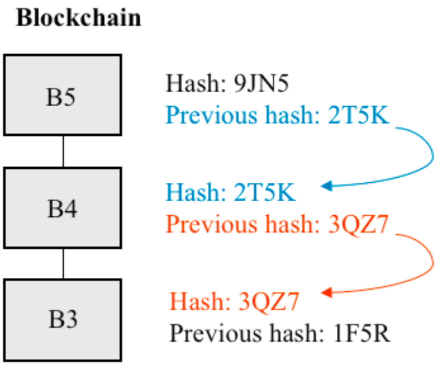


Figure 6: chronological order of blocks

Removing a block or changing a single detail of data in a transaction would break the record and would instantly be noticeable to the participants in the network.[65] Imagine Alice wants to 'undo' a transaction within block 4. This would cause the hash of block 4 to change. As a result, block 5 and all following blocks are rendered invalid because they no longer store a valid hash of the previous block (figure 7).[66]

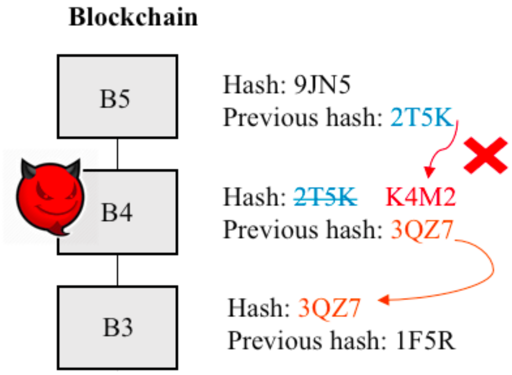


Figure 7: tampering with the blockchain

[64] *Simply Explained* 13 November 2017, 2:09m

[65] Laurence 2019, p.3

[66] *Simply Explained* 13 November 2017, 2:30m

Still, hashes alone do not prevent tampering. Computers today can calculate thousands of hashes per second,[67] meaning that Alice could effectively tamper with block 4 and recalculate the hash of block 5 and all following blocks. Bitcoin solves this problem by using the Proof of Work mechanism that slows down the creation of new blocks. Approximately 10 minutes are needed to calculate the required Proof of Work. In order to tamper with the block on the chain, Alice needs to recalculate the Proof of Work of all following blocks. Tampering is particularly difficult because each node has a copy of all the transactions that have occurred and can, therefore, verify that everything is in order. Blocks that are tampered with will be rejected by other nodes in the network.[68] To sum up, if Alice wants to tamper with the blockchain, she needs to recalculate the hashes, redo the proof of work, and take control over the majority of the hashing power. As the Bitcoin blockchain uses a lot hashing power, this is very unlikely.

2.3 Bitcoin transaction

2.3.1 Cryptography

To understand how bitcoin transfers from one person to another, it is necessary to discuss the role of cryptography in bitcoin. Asymmetrical cryptography (or public key cryptography) allows bitcoin to be transferred securely from one address to another.[69]

Imagine Alice is new to Bitcoin and wants to participate in the network. The first step would be for her to download and install the Bitcoin software on her computer.[70] Then, an algorithm will generate two (cryptographic) keys.[71] These keys are a random number and come in pairs consisting of a private key and a – therefrom generated – public key. The public key is used to create a bitcoin address. Alice can give her public key (and address) to anyone, while the private key must be kept secret. Think of the public key as a bank account number that gives others an address to transfer bitcoin to, and think of the private key as a PIN code or password

[67] *Simply Explained* 13 November 2017, 2:53m

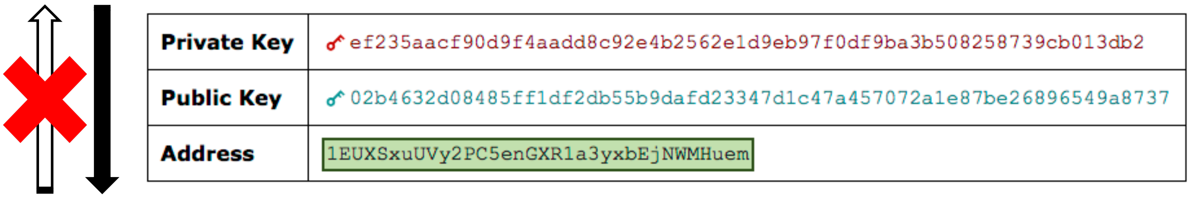
[68] *Simply Explained* 13 November 2017, 3:31m

[69] Laurence 2019, p. 18

[70] *Learn me a bitcoin* 2015, Getting started

[71] Arslanian & Fischer 2019, p. 91

which gives access to the account with the corresponding bitcoin address.[72] The keys are created and stored by users in a file or in a simple database called ‘a wallet’. The wallet is entirely independent of the Bitcoin protocol and can be managed without reference to the blockchain or access to the internet. [73] Asymmetrical cryptography enables secure communication because the public key can be calculated from the private key, but not the other way around (see figure 8).[74]



Private Key	ef235aacf90d9f4aadd8c92e4b2562e1d9eb97f0df9ba3b508258739cb013db2
Public Key	02b4632d08485ff1df2db55b9dafd23347d1c47a457072a1e87be26896549a8737
Address	1EUXSxuUVy2PC5enGXR1a3yxbEjNWMHuem

Figure 8: Asymmetrical cryptography[75]

2.3.2 Transaction structure

In the following pages, this chapter will discuss transactions within blocks on the blockchain. In Bitcoin, people don’t own a token that lives on the internet. Instead, they own the ‘rights’ to move bitcoin from one place to another.[76]

Throughout this chapter, the blockchain may be thought of as a public storage facility for safe deposit boxes which each hold a various amount of bitcoin. When Alice engages in the act of paying some bitcoin to Bob, she is not ‘sending’ the bitcoin from her address to Bob’s address. Instead, she is unlocking the safe deposit box in which her bitcoins are stored to, then, place her bitcoins in a new safe deposit box accessible only with a key (figure 9). The lock thus prevents others in the network from ‘taking’ the bitcoin and ensures that Bob (and everyone with Bob’s key) can access the safe deposit box.[77] Bob should safeguard his key

[72] Antonopoulos 2014, chapter 4

[73] Antonopoulos 2014, chapter 4

[74] Arslanian & Fischer 2019, p. 91

[75] *Learn me a bitcoin* 2015, keys and addresses

[76] Andrew, *Byzantine* 18 May 2018, par. 5

[77] *Learn me a bitcoin* 2015

carefully because the key is not linked to Bob's real identity. If Bob loses his key, he will lose access to all safe deposit boxes linked to this particular key.[78]

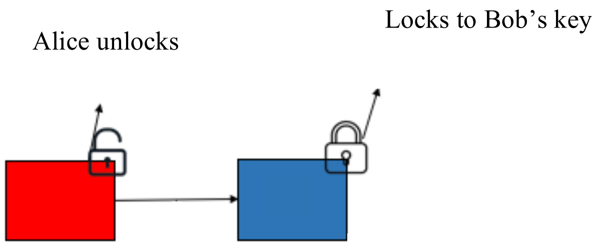


Figure 9: locking and unlocking

To explain the transaction structure in technical terms, when Alice wants to send some bitcoin to Bob, she is broadcasting transaction data to all the nodes that make a peer-to-peer network.[79] The transaction data encodes a *transfer of value* from a source of funds, called an *input*, to a destination, called an *output*.[80] Transaction inputs and outputs are not linked to real identities. Instead, they are locked to keys that only the owner, or a person who knows the key, can unlock.[81] In practice, this works as follows:

Input

- When Alice initiates a transaction, she needs to select an unspent transaction output (UTXO) that she can unlock. [82] Think of UTXO as the above-mentioned safe deposit box that contains bitcoin and is locked to a particular key. In this example, Alice can unlock the red UTXO (see figure 10).

[78] Antonopoulos 2014, Chapter 4

[79] *Learn me a bitcoin* 2015, Transactions

[80] Andrew, *Byzantine* 18 May 2018, Antonopoulos 2014, Chapter 5

[81] Antonopoulos 2014, Chapter 5

[82] *Learn me a bitcoin* 2015, How do transactions work?

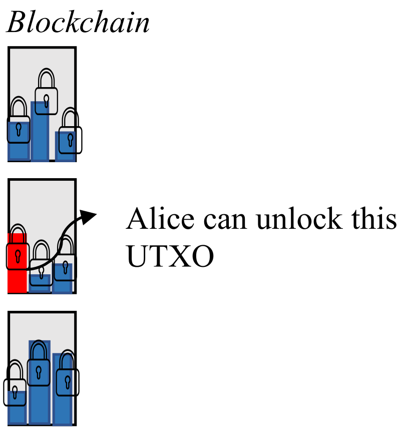


Figure 10: UTXOs

The transaction data contains information about the *value of transfer*. [83] UTXO's consist out of batches of bitcoins, [84] which means that when the selected red UTXO consists out of 10 bitcoins and Alice wants to send only 6 bitcoins to Bob, she is sending 4 bitcoins back to herself (see figure 11).[85]

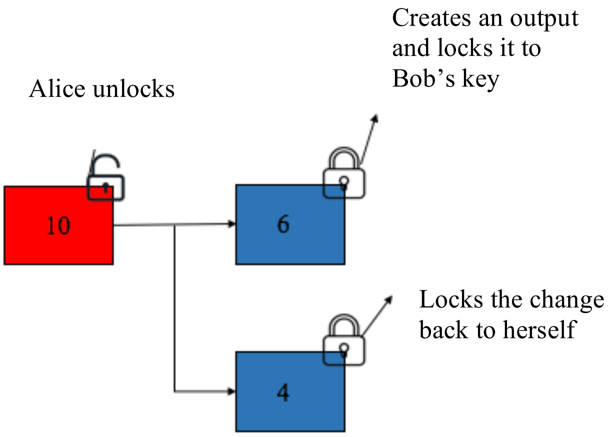

Creates an output and locks it to Bob's key
Alice unlocks
10
6
Locks the change back to herself
4

Figure 11: transaction amount

- To not overcomplicate this chapter, Alice is sending the whole UTXO to Bob (10 bitcoins). When an UTXO is spent in a transaction, this is referred to as an input.[86] To

[83] Antonopoulos 2014, Chapter 5

[84] *Learn me a bitcoin* 2015, How do transactions work?

[85] *Learn me a bitcoin* 2015, How do transactions work?

[86] Andrew, *Byzantine* 18 May 2018

send bitcoin to Bob, Alice needs to unlock the input. This part of the transaction gives others in the network information about *the source of funds.*[87] The input is locked to Alice's bitcoin address generated to the public key and can only be unlocked with the corresponding private key. The private key is used to prove 'ownership' of the bitcoins at the time of transfer.[88] However, the blockchain is a public network and the private key must remain secret at all times – otherwise the whole network may access this key and, subsequently, unlock all the UTXOs that are linked to its corresponding public key (see figure 12).[89]

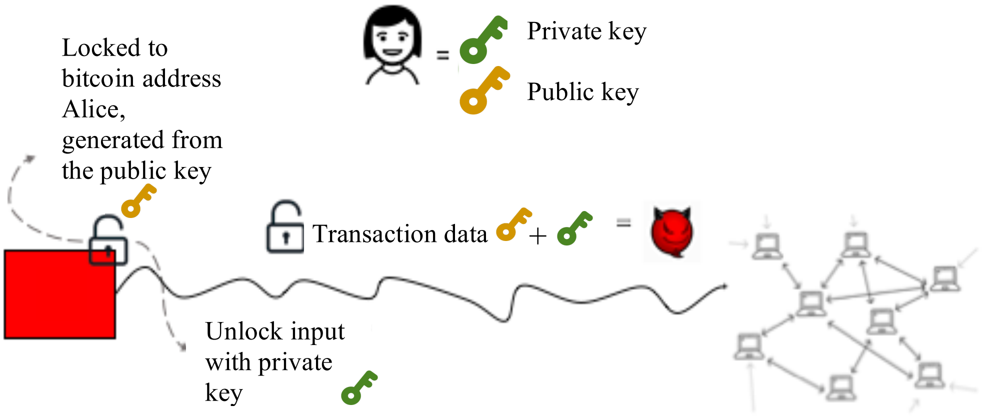


Figure 12: unlock with private key

Thus, Alice needs to find a way to unlock the input while keeping her private key a secret. Rather than using her private key directly, she uses her private key to create a digital signature (figure 13).[90] This method is reliable because Alice would not have been able to create this digital signature without having the correct private key. Additionally, a digital signature is only valid for the transaction it was created for, so it cannot be used to unlock other bitcoins.[91]

[87] *Learn me a bitcoin* 2015, How do transactions work?

[88] Antonopoulos 2014, Chapter 4

[89] *Learn me a bitcoin* 2015, Digital Signatures

[90] Liu 2011, p. 56

[91] *Learn me a bitcoin* 2015, Digital Signatures

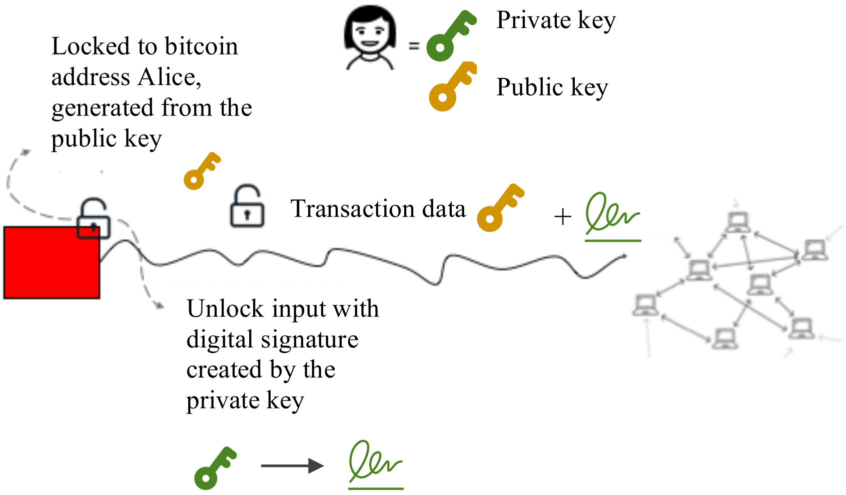

Private key
Public key
Locked to bitcoin address Alice, generated from the public key
Transaction data
+
Unlock input with digital signature created by the private key

Figure 13: unlock with the digital signature

Output

- To prevent others in the network from ‘taking’ the bitcoin, Alice needs to create a new output and put a lock on it. This provides others in the network with information about the *destination of funds.*[92] In this transaction, Alice locks the output to Bob’s key by placing Bob’s bitcoin address inside the lock of output (figure 14).[93] Whenever Bob receives the bitcoin, the amount is recorded within the blockchain as an UTXO. Subsequently, when Bob wants to spend the bitcoin he received from Alice, he repeats the process.[94]

[92] Antonopoulos 2014, Chapter 5

[93] *Learn me a bitcoin* 2015, Output locks

[94] Antonopoulos 2014, Chapter 6

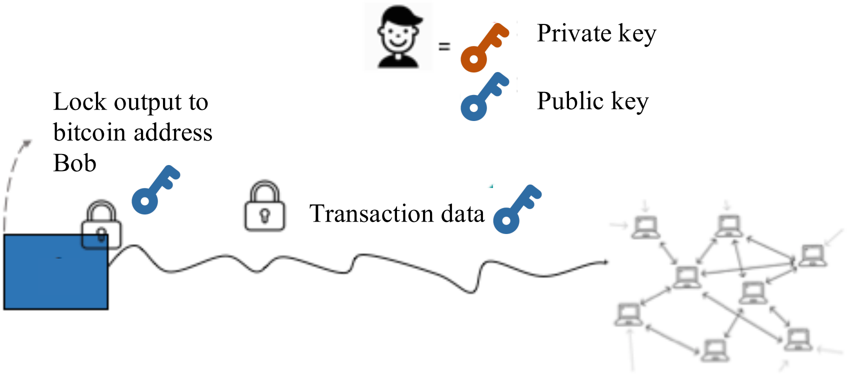


Figure 14: lock with public key

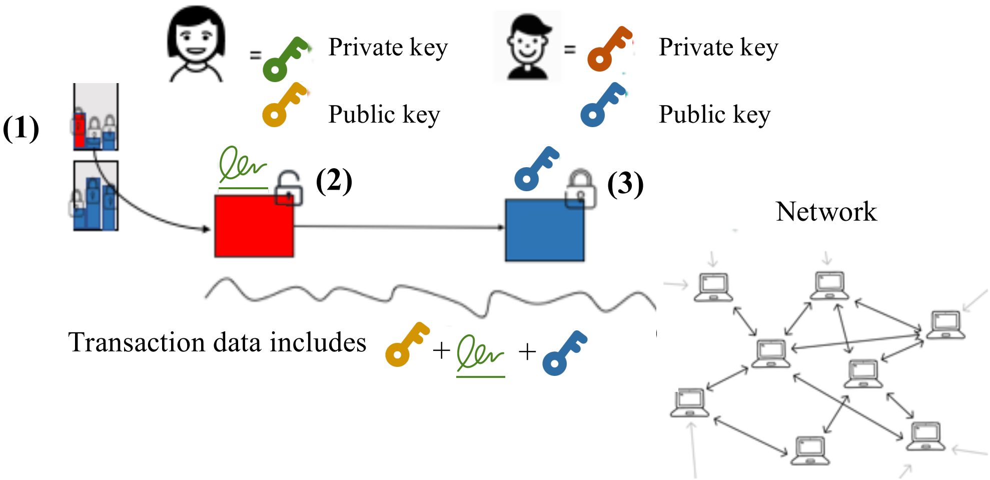


Figure 15: complete transaction

So, in a transaction where Alice wants to pay Bob in bitcoin, she not ‘sending’ the bitcoin from her address to Bob’s address. Instead, she is creating new outputs and locks them, sending the transaction data to the Bitcoin network, and waits for it to get mined in the blockchain.[95] When a miner receives the transaction data, it will check if Alice’s digital signature matches the public address by solving a mathematical puzzle.[96]

[95] *Learn me a bitcoin* 2015, Output locks

[96] *Learn me a bitcoin* 2015, Digital Signatures

Transactions with bitcoin (and other virtual currencies) differ in an important way from other online payment systems. First, in bitcoin an identity is formed by a pair of cryptographic keys. Unlike bank accounts, bitcoin addresses are not tied to the identity of users (figure 16).[97]

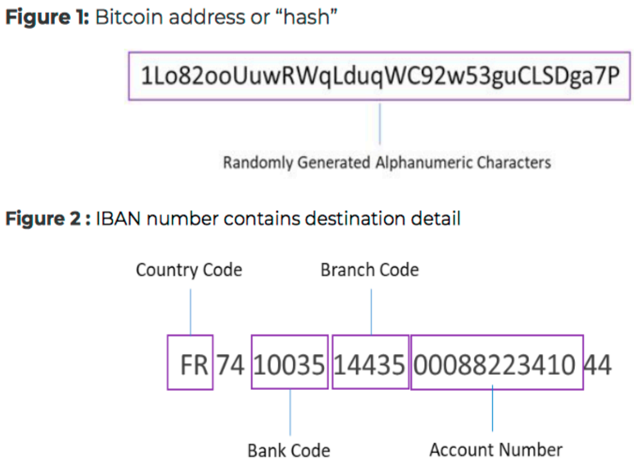


Figure 1: Bitcoin address or "hash"
1Lo82ooUuwRWqLduqWC92w53guCLSDga7P
Randomly Generated Alphanumeric Characters
Figure 2 : IBAN number contains destination detail
Country Code
Branch Code
FR 74 10035 14435 00088223410 44
Bank Code
Account Number

Figure 16: bitcoin address vs. IBAN[98]

Second, bitcoin transactions form a graph structure in which the movement of bitcoins is connected by a series of transactions that generated or transferred the bitcoin.[99] In technical terms, this is called a transaction with multiple inputs (figure 17, marked red).[100]

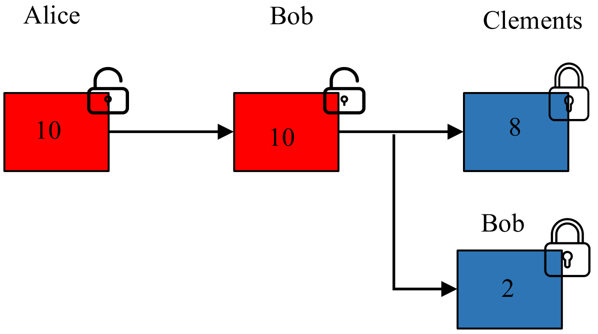


Figure 17: a series of transactions

[97] Van Wirdum, *Bitcoin Magazine* 18 November 2015, par. 8

[98] GDF April 7 2019, p. 6-7

[99] *Learn me a bitcoin* 2015, How do transactions work? Transaction Data

[100] Andrew, *Byzantine* 18 May 2018

Third, the transfer happens on the public blockchain. All transactions are completely traceable by all participants in the network.[101] Clements (and everyone else) could see that Bob received the bitcoin from Alice's bitcoin address (figure 17).

2.4 The crypto-ecosystem

Since the creation of bitcoin, the virtual currency industry has rapidly evolved. An important development is the emergence of businesses such as exchanges and custodian wallet providers. These service providers offer a variety of third-party payment products and services to facilitate obtaining, storing, and using virtual currencies.[102]

2.4.1 Centralized exchange (CEX)

Centralized exchanges are used to buy and sell virtual currencies against payment of a certain fee.[103] Examples of popular centralized exchanges are Bitfinex, HitBTC, Kraken, Binance, Poloniex, and Coinbase.[104] A difference can be made between two main types of centralized exchanges. The first is an exchange type that allows users to conduct exchanges from fiat money to virtual currency or the other way around (e.g. Coinbase). The second type only facilitates the exchange of one virtual currency for another (e.g. Poloniex).[105]

Centralized exchanges also operate as wallet providers. Wallet providers safeguard keys on behalf of their customers and are therefore called custodian wallet providers. The wallets are referred to as hosted wallets. [106] In this model, Alice holds the public key of the exchange. In order to trade on the exchange, she deposits the currency in the exchange in return for a claim against the exchange (see figure 18). The central exchange has one or more public-private keys which it uses to interact with the virtual currency network.[107]

[101] At least for bitcoin, as so-called privacy coins can deviate from this.

[102] Houben & Sneyers, PE 619.024 2018, p. 26-27

[103] Houben & Sneyers, PE 619.024 2018, p. 26

[104] *Coingecko* 2020, under 8, 22, 3, 1, 2, 3, 13

[105]Houben & Sneyers, PE 619.024 2018, p. 26

[106] Hardjono et al. 30 April 2020, Part III, 13(4)

[107] Hardjono et al. 30 April 2020, Part III, 13(4)

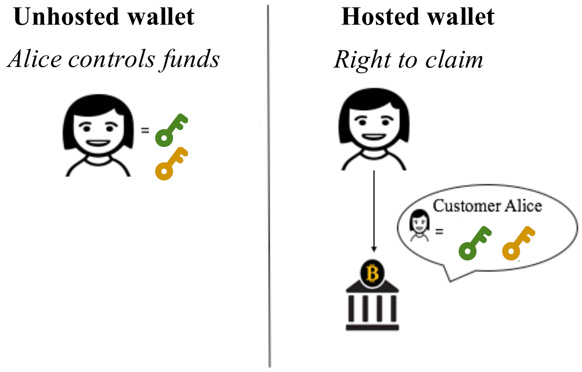


Figure 18: unhosted vs. hosted wallet

To further clarify a transfer through a centralized exchange, figure 19 illustrates a transaction between Alice, a customer, and Bob, a non-customer.

- First, Alice sends bitcoin (BTC) to the public key address of the exchange through the blockchain. As far as the blockchain is concerned, the bitcoin is now owned by the exchange. The bitcoin sits inside the exchange's wallet(s) where the exchange stores the keys. Alice has a claim over her portion of the bitcoin managed and held by the exchange.[108]

- From there, Alice places orders with the exchange. Alice requests a transfer to Bob. In this situation, the exchange initiates a transaction in which it sends the bitcoin to Bob's public address.[109]

[108] *Everbloom Crypto Exchange Blog* 7 June 2018

[109] *Everbloom Crypto Exchange Blog* 7 June 2018

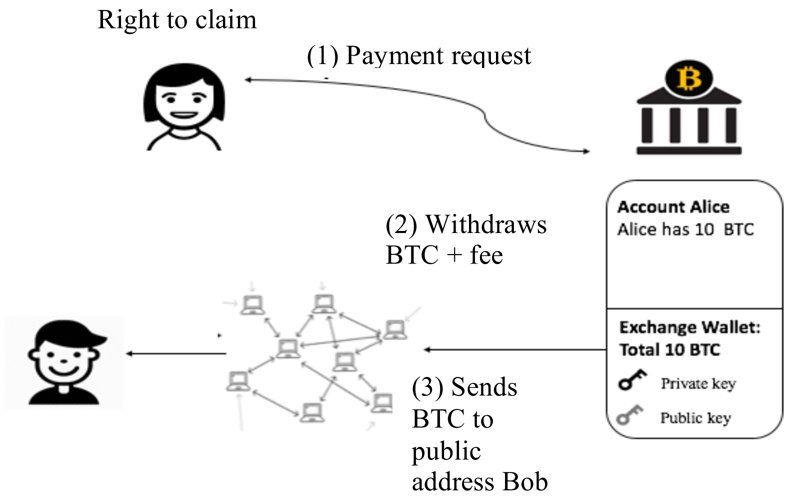


Figure 19: Alice requests transfer of funds that are stored at exchange

Currently, a vast majority of exchanges are centralized and seem to account for a significant majority of the global virtual currency trade volume.[110] One of the reasons that centralized exchanges are popular is that they make it easier for users to use and transfer virtual currencies.[111]

2.4.2 Decentralized exchange (DEX)

A decentralized exchange is an online platform in which each function (for example, matching buyers and sellers, and trade) related to trading is performed by the blockchain system itself.[112] Examples of popular decentralized virtual currency-only exchanges are Uniswap (v2), Curve Finance, JustSwap, and dYdX.[113] A well-known decentralized exchange that supports fiat currencies as well is Bisq.[114]

Decentralized exchanges use smart contracts to facilitate trade.[115] A smart contract is an agreement between two people in the form of computer codes. Transactions covered in a

[110] O'Neal, *Cointelegraph* 13 October 2019, par. 6

[111] Mandel, *BQT.io* 7 April 2019

[112] Houben & Sneyers, PE 619.024 2018, p. 27

[113] *Coingecko* 2020, under 1, 3, 9, 21

[114] *Coingecko* 2020, under 40

[115] Houben & Sneyers, PE 619.024 2018, p. 27

smart contract are processed by the blockchain, which implies that users trade directly without a third party. The transactions only happen when the conditions in the agreement are met. [116]

Decentralized exchanges are also referred to as non-custodial exchanges, a term which reflects the fact that no centralized party takes "custodianship" of the funds of users.[117] The wallets are called unhosted wallets, just like a regular peer-to-peer transaction (see figure 18).

Figure 20 illustrates the process of trading on a decentralized exchange. In this example Alice wants to trade Ether for BAT (another token tradable on the Ethereum blockchain).

- First, Alice deposits Ether into a smart contract. Unlike a centralized exchange, the decentralized exchange has no control over the deposit. Only Alice can access the funds, either via a withdrawal, or via trade submitted to the contract. [118]

- Subsequently, Alice signs an order to buy another token, BAT. The order is a message that says "Alice authorizes trade of 1 ETH (owned by her) for 1000 BAT (from someone else)" and includes a digital signature to prove it came from Alice. She, then, sends the order to the DEX order book to store and share the order with other users.[119]

- Imagine Bob sees Alice's message and takes her order from the DEX order book. Bob deposits 1000 BAT into the smart contract to cover the opposite side of Alice's order. Bob, then, signs a Ethereum Blockchain transaction that includes Alice's signed order and his authorization to be 'the someone else' to that order. He submits this transaction to the trade function of the smart contract; the funds get swapped in the smart contract and, ultimately, Alice is credited with BAT and debited with ETH, and Bob vice versa. Alice is now free to withdraw BAT by sending a transaction to the blockchain. She can do this without any assistance from the decentralized exchange.[120]

[116] M., B*itDegree* 11 September 2020

[117] *Everbloom Crypto Exchange Blog* 7 June 2018

[118] *Everbloom Crypto Exchange Blog* 7 June 2018

[119] *Everbloom Crypto Exchange Blog* 7 June 2018

[120] *Everbloom Crypto Exchange Blog* 7 June 2018

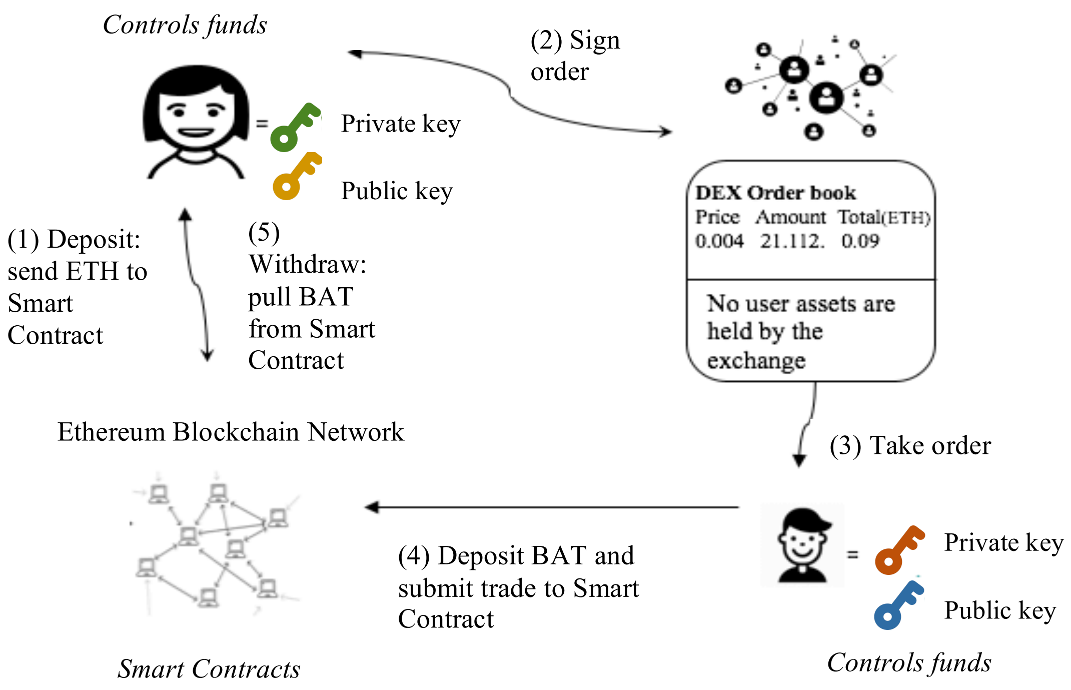

Controls funds
(2) Sign order
Private key
Public key
(1) Deposit: send ETH to Smart Contract
(5) Withdraw: pull BAT from Smart Contract
DEX Order book
Price Amount Total(ETH)
0.004 21.112. 0.09
No user assets are held by the exchange
(3) Take order
Ethereum Blockchain Network
(4) Deposit BAT and submit trade to Smart Contract
Private key
Public key
Smart Contracts
Controls funds

Figure 20: trading on a decentralized exchange

2.5 Conclusion

Bitcoin is a digital payment system that allows online payments to be sent directly from one party to another. The Proof of Work method solves the problem of double-spending and allows participants in the network to agree on a chronological order of transactions. Once transactions are stored on the public blockchain, it is nearly impossible to tamper with. Asymmetrical cryptography serves an important function in the transfer of bitcoin and other virtual currencies. It enables secure communication since the public key can be calculated from the private key, but not the other way around. Additionally, it allows private communication, as the pair of keys are not linked to the personal information of users within the network. In recent years, service providers have emerged that offer a variety of products and services to facilitate obtaining, storing, and using virtual currencies. Today, most transfers using virtual currency occur through the use of a centralized exchange.

Chapter 3 Anti-Money Laundering regulation

3.1 Introduction

The previous chapter explained the concepts and technologies that form the basis of the Bitcoin peer-to-peer electronic payment system, and bitcoin as means to transmit value among participants in the network. Building forth on this knowledge, this chapter discusses the risks of money laundering via virtual currencies, and the regulatory framework addressing those risks.

The term money laundering is used to describe the process by which proceeds of criminal activities are 'cleaned' and brought into the lawful economy so that its original source cannot be traced.[121] Many cases of money laundering involve the transfer funds through banks located in different jurisdictions to hide the source of funds.[122]

Considering the international nature of money laundering activities, regulators recognized the need for cooperation. Globally, the key policy-making body is the Financial Action Task Force (FATF), established in 1989.[123] The FATF currently has 39 members, and develops and promotes policies to protect the global financial system from abuse.[124] The recommendations issued by the FATF are not binding and therefore regarded as soft regulation (or soft international law). Yet, the FATF attempts to complement its lack of binding power by frequently issuing specific guidelines of prudent behavior and by monitoring its members.[125]

Within the European Union, the European Commission has the power to monitor the implementation of EU law by EU Member States and to propose new legislation to the European Parliament. In 1991, the EU adopted the First Anti-Money Laundering Directive on 10 June 1991 (AMLD1). The EU has since updated the AMLD five times, and strengthened the framework to combat money laundering and terrorist financing.[126]

[121] Houben & Sneyers, PE 619.024 2018, p. 59, See also Art. 1(3) Directive (EU) 2015/849

[122] Reuter & Truman November 2004, p. 26, 30

[123] *FATF*, About/ History of the FATF, p. 46-47

[124] FATF Members include the United States, Russia, China, as well as the European Commission and 14 EU Member States, *FATF*, About/ History of the FATF

[125] *FATF*, About, Members

[126] Houben & Sneyers, PE 619.024 2018, p. 58-60

For the purpose of combating money laundering, regulations have been introduced that aim to increase transparency to transactions. Money laundering can occur in all parts of the economy. For this reason, regulations do not only address traditional financial institutions, but also other entities such as estate agents, or providers of gambling services.[127] These entities are subjected to AML requirements, including licensing and registration, customer identification, monitoring practices, and reporting.[128] Financial institutions are, in addition, obliged to send information about their customers when sending payments.[129] The obligation to collect and exchange customer information is also known as the travel rule.[130]

Over the past decade, AML requirements led to an increase in costs and complexity,[131] while the effectiveness and efficiency of AML controls remain an issue. For example, AML controls have led to more reports of suspicious behavior, but not necessarily to better quality of reports.[132] Another key challenge is the lack of information sharing between foreign branches and subsidiaries.[133] To this date money laundering through the traditional financial system remains a major concern.[134]

Recently, the threat of money laundering is becoming complex, as criminals exploit advances in technology to hide the source of funds.[135] One of these advances has been the rise of virtual

[127] Article 2 Directive (EU) 2015/849

[128] Article 11 Directive (EU) 2015/849, Article 13 Directive (EU) 2018/843, FATF (2012-2020), recommendation 10 ff. p. 14

[129] FATF (2012-2020), recommendation 16, p. 71, Directive (EU) 2015/847

[130] FATF (2012-2020), recommendation 16

[131] International Finance Corporation 2019, p. v

[132] Customer information is obtained from databases such as World-Check. These databases monitor media reports and lawsuits about money laundering and other criminal activities worldwide. If a name appears in the database, this can lead to a report to the anti-money laundering authorities in a country. Whether these payments are also suspicious is not reported. Groot & Leupen, *Het Financieele Dagblad* 25 September 2020

[133] Countries may determine the scope and the extent of information sharing, based on the sensitivity of the information, and its relevance to AML risk management. A recent example is Dutch bank ING that has been carrying out billion-dollar transactions for companies from one of the largest Russian money laundering networks ever exposed. ING's Polish subsidiary played a central role in this money laundering scandal. Groot & Leupen, *Het Financieele Dagblad* 22 September 2020, FATF (2012-2020), INR 18(4), p.79, see also Article 45 Directive (EU) 2015/849 & Directive (EU) 2018/843

[134] HM Treasury December 2020, p. 70

[135] HM Treasury December 2020, p. 70

currencies. The main problem is the anonymous nature of virtual currencies, spanning from complete anonymity to pseudo-anonymity, which prevents transactions from being adequately monitored.[136]

In an effort to address the risks related to the (pseudo)anonymity, the FATF updated its recommendations in 2019.[137] Virtual asset service providers (VASPs) are now subjected to AML requirements, including the travel rule.[138] The FATF update of 2019, exceeds the requirements introduced by the EU AMLD5, which entered into force in 2018.[139]

In the following pages, this chapter will illustrate how virtual currencies are used to launder money. Subsequently, this chapter will explore AMLD5 and discusses the FATF travel rule, the focal point of this thesis.

3.2 Money laundering via virtual currencies

Concerns about money laundering via virtual currencies originate from the fact that most virtual currencies are pseudonymous and that it is technically feasible, though complex to identify the users behind a transaction.[140] In Bitcoin for example, addresses allow any participant in the network to transfer bitcoin from any address to which it controls the corresponding private key, without submitting any personal information.[141]

Other characteristics that render virtual currencies susceptible to abuse are accessibility and global reach.[142] In traditional payment methods, national boundaries heavily restrict processing times and the transfer of physical currency. By contrast, virtual currencies are

[136] Houben & Sneyers, PE 619.024 2018, p. 53

[137] FATF (2012-2020)

[138] FATF (2012-2020), INR 15, p. 77-78

[139] Directive (EU) 2018/843, the European Union's Sixth Anti-Money-Laundering Directive (Directive 2018/1673), entered into force on 3 December 2020. AMLD6 does not pose any additional requirements in the area of virtual currencies, but introduces a unified list of predicate offences, criminal liability for organizations and increased international co-operation.

[140] Houben & Sneyers, PE 619.024 2018, p. 33

[141] Van Wirdum, *Bitcoin Magazine* 18 November 2015

[142] FATF (2020), p. 66

global currencies and enable criminals to quickly move funds across national borders at scale.[143]

The transaction speed is in particular concerning because virtual currency transactions commonly rely on complex infrastructures that involve multiple service providers such as exchanges, often spread across different countries and subjected to different (national) regulations. [144] For example, an exchange located in Panama may be subjected to different AML obligations and oversight, but still offer their products and services to customers located in France. Many cases of money laundering via virtual currencies involve exchanges that lack (effective) AML controls. In that way service providers (e.g. exchanges) can be thought of as the equivalent of banks. Though, as discussed in the previous chapter, users can also transact without the use of a service provider like an exchange.

To better understand the risks, it is important to gain insight in the process of money laundering via virtual currencies. In most cases, money laundering takes place in three distinct phases: placement, layering and integration (figure 21).

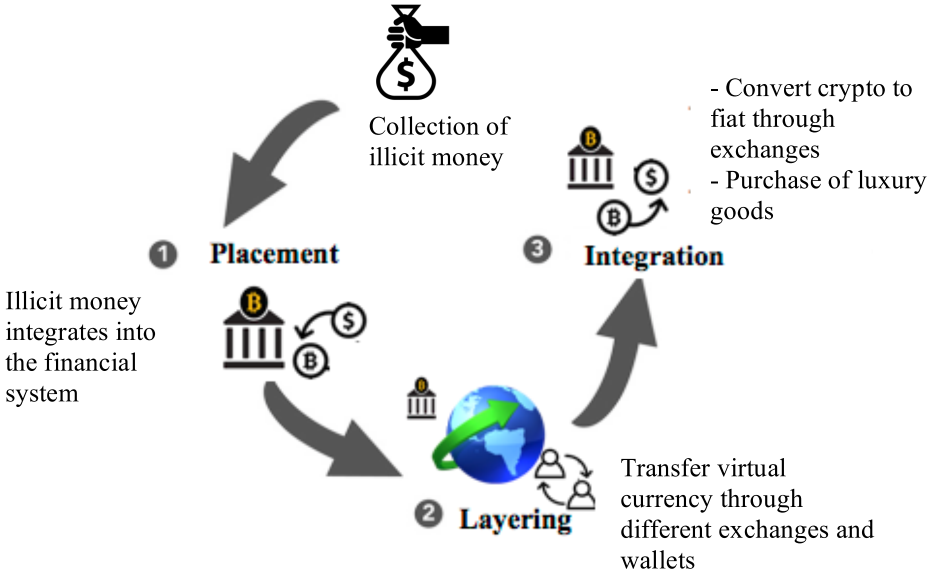

Collection of illicit money
- Convert crypto to fiat through exchanges
- Purchase of luxury goods
1 Placement
3 Integration
Illicit money integrates into the financial system
2 Layering
Transfer virtual currency through different exchanges and wallets

Figure 21: stages of money laundering via virtual currencies

- The process of money laundering via virtual currencies generally starts with placement, where money is gained from illegal activity and is moved from its source

[143] Madhavji & Tan, *Cointelegraph* 30 July 2020

[144] *Elliptic* 18 September 2019, HM Treasury December 2020, p. 71

by placing it into the (virtual currency) system.[145] Criminals can purchase virtual currencies using illicit money at an exchange. The purchase is mostly done at exchanges with little-to-no AML controls in place. Regulated exchanges apply AML controls and can therefore link addresses to real identities.[146]

- From there, the funds need to be hidden from the source, also called the stage of layering. Every transaction is recorded in a publicly visible ledger, and can therefore be followed.[147] To launder money, criminals need to create a money trial that is impossible to track. There are different methods to obfuscate the trail.[148] In most cases, obfuscating the trial is done by simply trading the virtual currency a number of times across various markets at exchanges that lack (adequate) AML controls.[149] Criminals can also swap for privacy coins such as Monero and Zcash, designed to enhance anonymity.

  Another method to hide the funds source is by using anonymity-enhancing tools such as mixers (also called tumblers). A mixer breaks the connection between the sending address and the receiving address. The process starts with breaking down the virtual currency into smaller parts. From there, the mixer 'mixes' the coins with other coins from other addresses, followed by paying the target addresses.[150]

  Mixing services can be an attractive tool to hide the destination of funds.[151] Even if blockchain analytic tools can identify that Alice 'owns' coin X, it is difficult to figure

[145] In other money laundering cases, the placement step is already part of the criminal activity as virtual currency is received by the criminal. For example, in case of ransomware that extorts for Bitcoin or darknet vendors selling drugs for virtual currency.

[146] For example, Bitcoin addresses can be linked to real identities if these real identities are used in combination in with the bitcoin address in some way. This includes addresses used to deposit or withdraw money to or from a (regulated) exchange or wallet service Van Wirdum, *Bitcoin Magazine* 18 November 2015

[147] *Elliptic* 18 September 2019

[148] Other methods include crypto ATMs, gambling websites, use of OTC brokers and prepaid cards loaded with cryptocurrency see Madhavji & Tan, *Cointelegraph* 30 July 2020 & *Elliptic* 18 September 2019

[149] Madhavji & Tan, *Cointelegraph* 30 July 2020

[150] Albrecht, *Cryptoticker* 20 January 2020

[151] Regulated exchanges are likely to further investigate a transaction using mixers or privacy coins. FATF (2019), p. 28, recital 110

out whether Alice paid the coin to B, D or F (Figure 22). Think of the mixer as a smoothie maker and coins from an original address as fruit. When the smoothie is made, it is difficult to identify which fruit produces a specific flavor.[152]

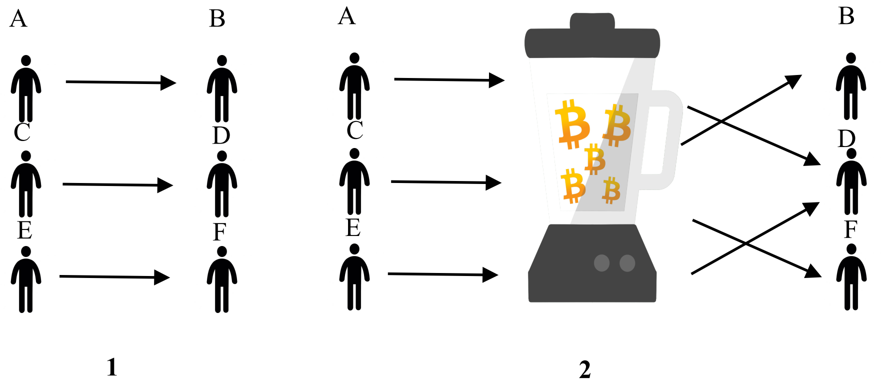


figure 22: Mixer

- The final stage includes integrating the money to legitimize the proceeds derived from illegal activity. Despite the currency no longer being directly tied to the crime, money launders still need to explain how they came into possession of the currency. Possibly, the profits could be presented as the as the result of a successful enterprise or another currency appreciation.[153] At exchanges criminals can convert the virtual currencies it into local fiat money.[154] Throughout 2019, more than $2.8 billion worth of bitcoin was sent from criminal entities to exchange, and 52% of it went to the top two exchanges, Binance and Huobi.[155]

Money laundering via virtual currencies confront regulators with significant challenges. Yet, regardless the level of anonymity, criminals are likely to exchange the acquired virtual currency for fiat currency at some point.[156] The monitoring of such transaction, within and across distributed ledger technologies, can help in detecting money laundering.[157]

[152] Albrecht, *Cryptoticker* 20 January 2020

[153] *Elliptic* 18 September 2019

[154] *Elliptic* 18 September 2019

[155] Madhavji & Tan, *Cointelegraph* 30 July 2020

[156] Rebora, *Coinmonks* 29 December 2019

[157] Rebora, *Coinmonks* 29 December 2019

3.3 The Fifth Anti-Money Laundering Directive

The terrorist attacks in Paris and Brussels, and ongoing scandals such as the Panama Papers, have brought the European Commission to undertake rapid further action towards emerging new trends, including virtual currencies.[158] Proposed in July 2016, the Fifth Anti-Money-Laundering Directive (AMLD5), amending the Fourth Anti-Money-Laundering Directive (AMLD4), entered into force on 9 of July 2018.[159]

AMLD5 subjects crypto-fiat exchanges and custodian wallet providers to the EU's AML framework.[160] Reading AMLD5 at first glance would suggest that crypto-crypto exchanges, would not be subjected to AMLD5 – as customers will buy and sell virtual currency and not fiat. However, when these crypto-crypto exchanges safeguard keys on behalf of their customers, they are operating as custodian wallet providers, and subjected to the requirements of AMLD5.[161]

In an effort to link the wallet addresses to real identities, crypto-fiat exchanges and custodian wallet providers are required to apply AML controls at the point of registration or at the time of a transaction in excess of EUR 15.000.[162] Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures require crypto-fiat exchanges and custodian wallet providers to identify and verify the customer, and to undertake monitoring practices to ensure that

[158] The Panama Papers are an unprecedented leak of 11.5m files from the database of an offshore law firm, Mossack Fonseca. The documents show the ways in which the rich can exploit secretive offshore tax regimes. Harding, *The Guardian* 5 April 2016 Houben & Sneyers, PE 619.024 2018, p. 63

[159] Article 4 Directive (EU) 2018/843

[160] For legal certainty, AMLD5 defines virtual currencies as '*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or traded electronically*' and custodian wallet providers as *'an entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies'* see also article 3 (d*)* Directive (EU) 2018/843 Virtual currency exchanges are described as *'providers engaged in exchange services between virtual currencies and fiat currencies'*. See also Article 1 (g) Directive (EU) 2018/843

[161] Miggiani, *Regulation Y* 14 June 2020

[162] Article 11 Directive (EU) 2015/849

emerging money laundering threats are identified as quickly as possible.[163]

The application of a risk-based approach allows for crypto-fiat exchanges and custodian wallet providers to focus on activities with the highest risk.[164] The risk assessment carried out by Member States should take into account potential higher risk situations set out in the directive, such as geographic risk factors or risks related to transactions.[165] While the directive does not explicitly mention virtual currencies as a potential high risk, the directive does refer to transactions that might favor anonymity.[166] Transactions using virtual currencies, thus, might be subjected to enhanced customer due diligence controls, and may allow for an increase in the degree and nature of monitoring.[167]

To detect money laundering, suspicious transactions and other information relevant to money laundering should be reported to the competent Financial Intelligence Unit (FIU).[168] FIUs are established in every Member State and analyze suspicious transactions.[169] To effectively do so, AMLD5 requires customer information to become immediately available.[170]

[163] Article 11 Directive (EU) 2015/849, Article 13 Directive (EU) 2018/843

[164] Article 18 Directive (EU) 2015/849

[165] Article 18, Annex 3 Directive (EU) 2015/849, Directive (EU) 2018/843 recital (44)

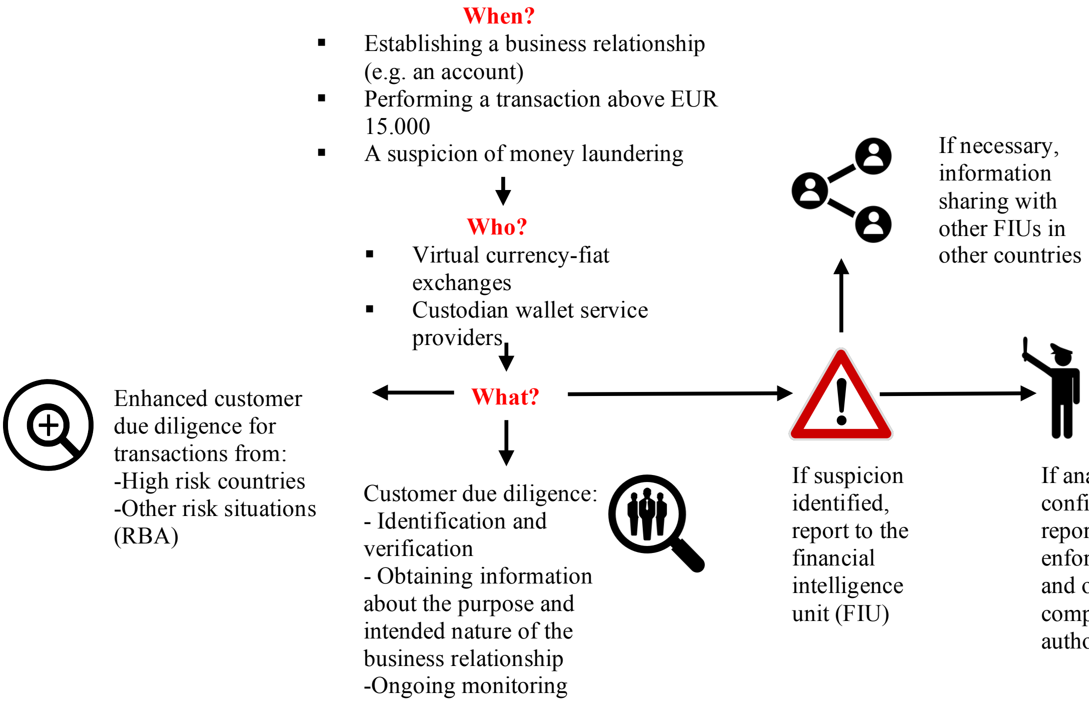
[166] Annex 3 Directive (EU) 2015/849

[167] Article 18 Directive (EU) 2015/849

[168] Article 32 Directive (EU) 2015/849

[169] Directive (EU) 2018/843, recital 17, Directive (EU) 2018/843, recital 18

[170] Article 32 Directive (EU) 2015/849


When?
Establishing a business relationship (e.g. an account)
Performing a transaction above EUR 15.000
A suspicion of money laundering
Who?
Virtual currency-fiat exchanges
Custodian wallet service providers
What?
Enhanced customer due diligence for transactions from:
-High risk countries
-Other risk situations (RBA)
Customer due diligence:
- Identification and verification
- Obtaining information about the purpose and intended nature of the business relationship
-Ongoing monitoring
If suspicion identified, report to the financial intelligence unit (FIU)
If necessary, information sharing with other FIUs in other countries
If analysis confirmed, report to law enforcement and other competent authorities

F*igure 23: AMLD5*

Member states had to bring into force laws to comply with AMLD5 by 10 January 2020.[171] The directive sets minimum standards. In such circumstances, member states have the right to set higher standards than those set in the directive. Countries such as Austria, Germany, the Netherlands, and France are implementing forward looking measures that go beyond AMLD5's scope.[172] The Netherlands in particular drew a lot of criticism. Virtual currency-fiat exchanges and custodian wallet providers need to register at the Dutch Central Bank and need to pass a screening on a company level as well as on the directors' personal level. Furthermore, the costs of supervision are estimated at EUR 29,850 on a yearly basis, in addition to one-time registration fees of at least EUR 5,000.[173] Accordingly the Dutch approach is likely to squeeze out small exchanges that cannot afford it.[174] Exchange Deribit,

[171] Article 4 Directive (EU) 2018/843

[172] For example, Germany introduces AML procedures for brokers/traders/market places of crypto assets and to implement a new regulatory basis for crypto assets, and Austria introduced strict license requirements to a broad range of crypto companies, including ATMs, peer-to-peer platforms, token issuers. Holzborn & Oleshchuk, *Orrick* 9 December 2019, Hamacher, *Decrypt* 14 Jan 2020

[173] *De Nederlandse Bank* 4 mei 2020

[174] Foxley, *Coindesk* 27 April 2020

for example, moved its operations to Panama and the SimpleCoin mining pool closed down completely.[175]

3.4 The FATF travel rule

Over the last few years, the virtual currency ecosystem has been expanded considerably and seen the rise of new business models, activities and interactions, including virtual currency-virtual currency exchanges and decentralized exchanges and platforms.[176] These service providers remained unregulated as existing regulation only covered virtual currency-fiat exchanges and custodian wallet providers.[177] Lack of effective regulation in combination with the broader application of virtual currencies, increased the risk of virtual currencies being used for money laundering.[178]

Based on these developments, the FATF updated its recommendations in 2019. The update of the FATF requires virtual asset service providers (VASPs) to be subjected AML requirements, including the travel rule.[179] The travel rule aims to increase the amount of information available about users transferring virtual currencies, improving transparency of users and law enforcement's ability to 'follow the virtual currency'.[180]

Prior to the update of the FATF, some VASPs were required to apply AML controls in order to identify and monitor the customer. AML requirements did not require VASPs to identify the counterparty, nor was this necessary – virtual currencies are transferred by a wallet address. The travel rule increases AML requirements for VASPs significantly since it requires VASPs to obtain, hold and exchange information of *both parties* in a transaction.[181] Information about the users transferring virtual currencies could be particularly useful in

[175] Martin, *Cointelegraph* 15 April 2020

[176] FATF (2019), p 6 recital 4

[177] FATF (2019), p 6 recital 3, Directive (EU) 2018/843

[178] HM Treasury December 2020, p. 70

[179] FATF (2012-2020), INR 15, p. 77-78

[180] FATF (2012-2020), INR 15, p. 77-78

[181] FATF (2012-2020), INR 15, p. 77-78, Bryant, *The Startup* 25 September 2019

combination with blockchain technology that allows to monitor and record transactions (figure 24).[182]

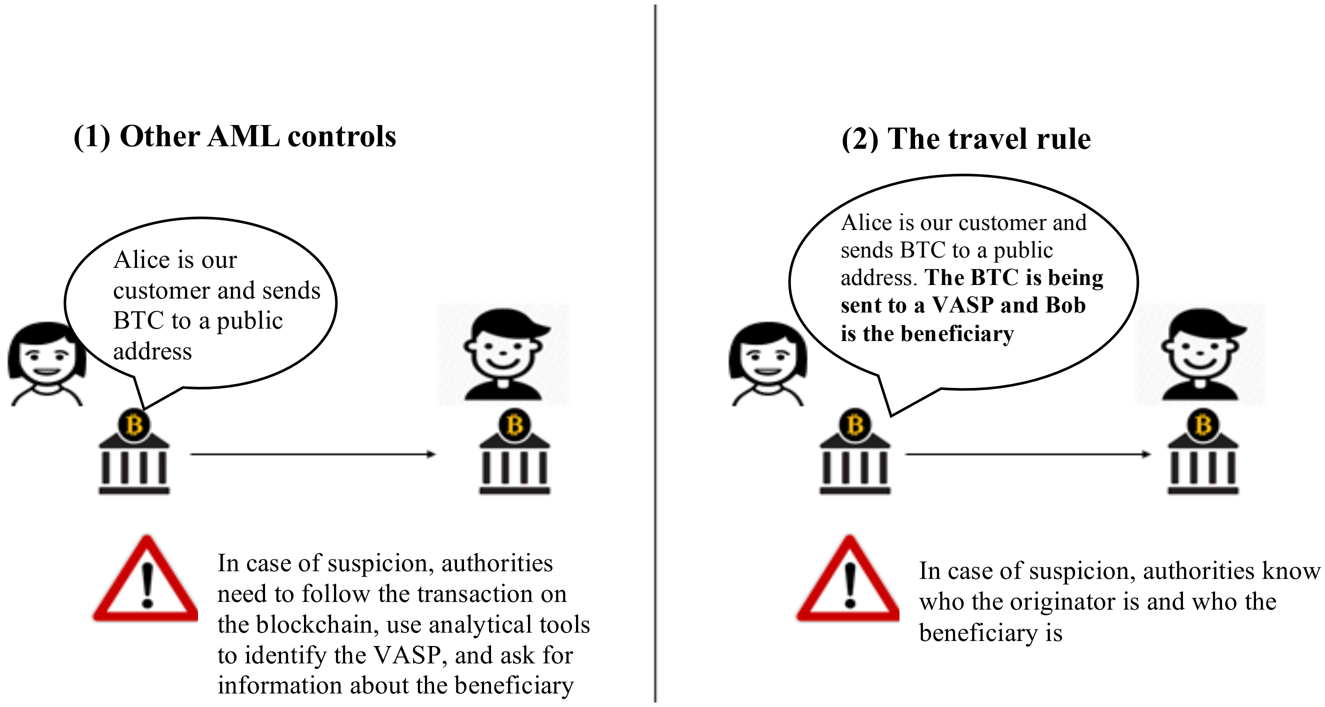

(1) Other AML controls
Alice is our customer and sends BTC to a public address
In case of suspicion, authorities need to follow the transaction on the blockchain, use analytical tools to identify the VASP, and ask for information about the beneficiary
(2) The travel rule
Alice is our customer and sends BTC to a public address. **The BTC is being sent to a VASP and Bob is the beneficiary**
In case of suspicion, authorities know who the originator is and who the beneficiary is

Figure 24: other AML requirements vs. travel rule

3.4.1 Virtual Assets (VA) and Virtual Asset Service Providers (VASPs)

The virtual asset market is fast-moving and quickly evolving. In order to keep pace with evolving trends, the FATF have brought a greater number of sectors in the scope, placing requirements on virtual assets (VA) and virtual asset service providers (VASPs).[183]

Virtual asset is the term the FATF uses to refer to crypto-assets and other digital assets. The definition does not only cover virtual currencies, but also other types of assets such as tokens.[184] The FATF uses the term virtual asset service providers (VASPs) to refer to businesses are subjected to the FATF recommendations. Simply said, a VASP is anyone who

[182] Rebora, *Coinmonks* 29 December 2019

[183] FATF (2019), p 6 recital 4

[184] The FATF defines virtual assets as *'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'*. FATF (2012-2020), p. 126/127

is intermediating in the virtual asset ecosystem. To provide flexibility in a rapidly evolving space, the FATF has introduced an activity based definition of a VASP.[185] Examples of VASPs are exchanges (both virtual currency-fiat exchanges and virtual currency- virtual currency exchanges), custodian wallet providers, and intermediaries that facilitate solely transfer of virtual assets.[186]

The FATF recommendations focus, thus, on placing obligations on intermediaries between users and the virtual currency ecosystem. For this reason, transactions without the use of VASP (e.g. peer-to-peer transactions) are not subjected to the FATF constrains. The lack of coverage of such transactions could leave a blind spot in the effectiveness of the travel rule (figure 25).[187]

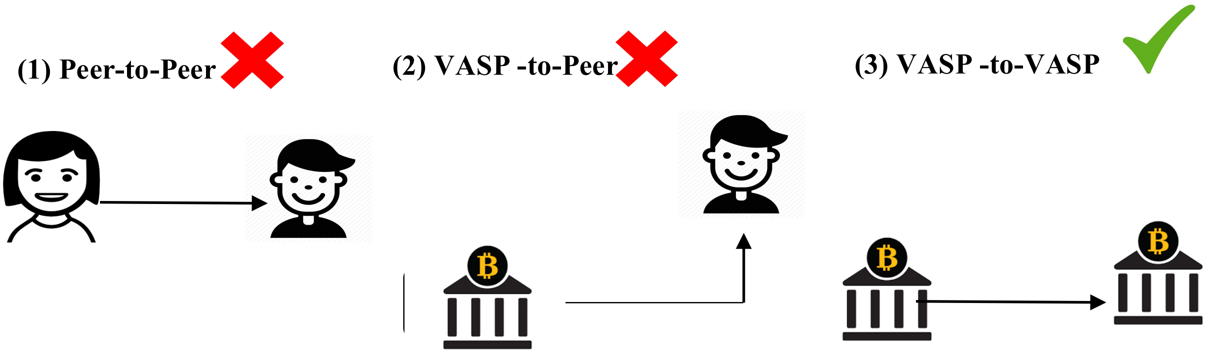


Figure 25: the travel rule applies between VASPs

By the same token, the FATF does not regulate the technology that underlies virtual currencies.[188] In this line of thinking, decentralized exchanges can be seen as a grey area. A

[185] The FATF defines a VASP as *'any natural or legal person who is not covered elsewhere under the Recommendations and as a business of conducts one or more of the following activities or operations for or on behalf of another natural or legal person: Exchange between virtual assets and fiat currencies; Exchange between one or more forms of virtual assets; Transfer of virtual assets; Safekeeping and/ or administration of virtual assets or instruments enabling control over virtual assets; Participation in and provision of financial services related to an issuer's offer and/ or sale of a virtual asset'* FATF (2012-2020), p. 126/127

[186] A comparison of the international AML/CFT standards on virtual assets with the European AML/CFT framework shows that AMLD5 already lags behind. AMLD5 only covers cryptocurrencies and therefore does not encompass other types of crypto-assets such as tokens. Second, AMLD5 only covers fiat-to-crypto exchanges and custodian wallet providers. Houben & Sneyers PE 648.779 2020, p. 47-48

[187] FATF (2019), p. 17, recital 47

[188] FATF (2019), p. 17, recital 48

decentralized exchange is an online platform of which each function related to trading is performed by the blockchain system itself, so that, decentralized exchanges may fall outside the scope of the FATF recommendations. On the other hand, when customers need to pay a fee in order to run the software, they may fall within the scope of VASPs. In that case, a decentralized exchange may facilitate exchange services or the transfer of value. Most decentralized exchanges ask for a fee, and fall therefore probably within the scope of the travel rule.[189]

3.4.2 Information that travels

The travel rule applies when carrying a transaction, domestic or cross-border[190], above a threshold of USD/EUR 1,000.[191] In such a transaction, information about the originator and the beneficiary has to 'travel' together to the receiving VASP.

For the purpose of achieving compliance, the sending VASP needs to obtain the following information of the originator: the name of the customer, the account number and unique identifiable information, either an address, national identity number or customer identification number or date and place of birth.[192] The travel rule also requires the receiving VASP to obtain the name of the beneficiary, and the account number, so that, the receiving VASP can share information of the beneficiary with the sending VASP. As a final point, information of the originator and information of the beneficiary has to be sent to the receiving VASP (see figure 26). [193]

[189] FATF (2019), p. 15-16, recital 40

[190] In case of cross-border transfers, countries may adopt a de minimis threshold, not higher than USD/EUR 1,000. In this case, VASP should obtain: the originator's name and account number, and; beneficiary name and account number FATF (2012-2020), p. 73 (5) and (7)

[191] FATF (2012-2020), p. 72 (3), p.71 (7)

[192] FATF (2012-2020), p. 73 (6)

[193] FATF (2012-2020), p. 73 (7)

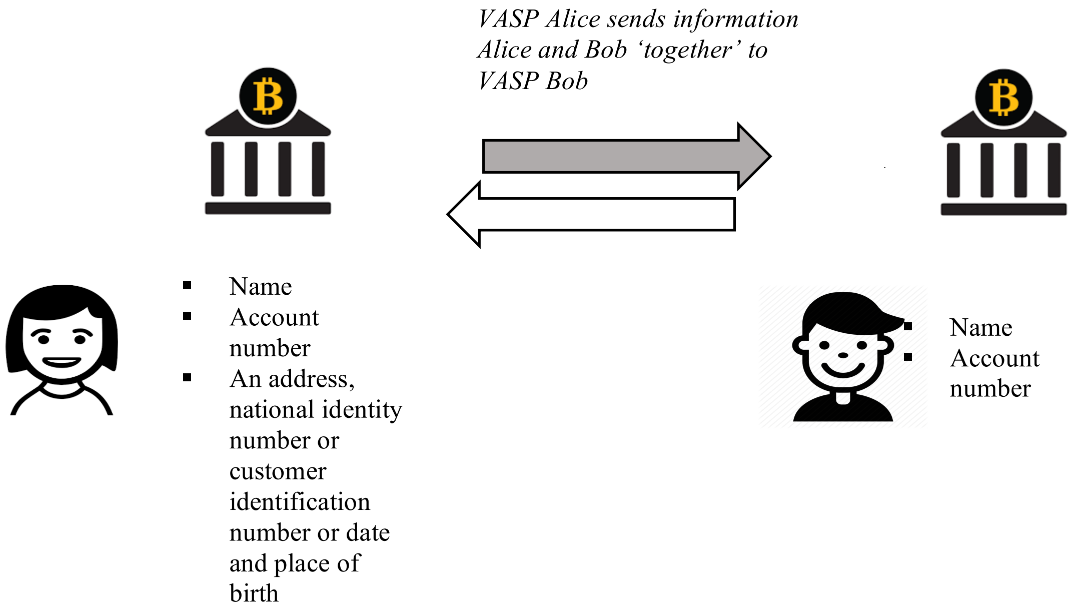

VASP Alice sends information Alice and Bob 'together' to VASP Bob
Name
Account number
An address, national identity number or customer identification number or date and place of birth
Name
Account number

Figure 26: travel rule information

3.4.2 Implementation of the travel rule

The FATF has set a 12-month review period for implementation of the travel rule, which ended in June 2020.[194] The 12-month review revealed that there has been less implementation of travel rule requirements for VASPs than other AML requirements. From the 32 jurisdictions that regulate VASPs, only 15 jurisdictions introduced travel rule requirements for VASPs. The reason for delay is generally attributed to the lack of adequate holistic technological solutions.[195]

The first challenge addresses the issue of transferring data cross-chain. The virtual currency ecosystem consists out of hundreds of independent blockchain networks and exchanges, each with their own technical standards and operating procedures.[196] In the last couple of months, progress has been made in the development of technological solutions to enable data transmission. Examples are Sygna bridge, TRISA, OpenVasp, Notabene, and Shyft. In line with the decentralization ethos that underpins virtual currencies, there is a general desire for

[194] According to Sian Jones, a regulatory consultant, the deadline June 2020 'is a bit of a myth' and the adoption of the travel rule, and the other FATF recommendations, could take years Partz, *Cointelegraph* 12 May 2020

[195] FATF (June 2020), p. 12 recital 43

[196] Milea, *Inbound FinTech* 21 October 2020

multiple potential solutions, rather than one centralized solution.[197] In order to transmit data effectively, different protocols –written in different programming languages- need to able to communicate.[198] An important development is the creation of a global messaging standard called IVMS101, also referred to as InterVASP. The messaging standard addresses the issue of data being captured in multiple languages, character sets and local conventions.[199] Most solution providers in the industry have standardized the messaging content around the InterVASP messaging format.[200]

The second challenge concerns the issue of counterparty identification. VASPs must be able to identify whether they are performing a transaction with another VASP. Whereas an International Bank Account Number (IBAN) can be attributed to a destination bank account with a given bank, the structure of a bitcoin address is simply a random generated selection of numbers and letters. In other words, there is no information tying the address to a particular identity or VASP (see figure 27).[201] By implication, the originating VASP also does not know whether the virtual asset destination address is owned by a VASP, by a non-VASP, or by a natural person.[202]

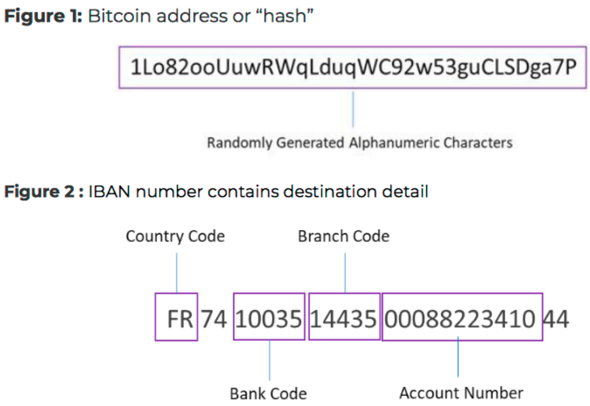


Figure 1: Bitcoin address or "hash"
1Lo82ooUuwRWqLduqWC92w53guCLSDga7P
Randomly Generated Alphanumeric Characters
Figure 2 : IBAN number contains destination detail
Country Code
Branch Code
FR 74 10035 14435 00088223410 44
Bank Code
Account Number

Figure 27: bitcoin address vs. IBAN[203]

[197] FATF (June 2020), p. 12 recital 42

[198] In September 2020, Sygna Bridge and TRISA have announced a proof-of-work concept to demonstrate interoperability between their systems. *Mono Vsione* 15 September 2020

[199] *Sygna* 2020

[200] Shin, *Unchained* 4 August 2020

[201] Shin, *Unchained* 4 August 2020, GDF April 7 2019, p. 4 and p. 6

[202] GDF April 7 2019, 6-7

[203] GDF April 7 2019, p. 4

Currently the only way of collecting a VASP counterparty's information is to contact the counterparty VASP directly and ask for it.[204] Another possible solution proposed in the virtual currency industry is the creation of a global list of VASPs (or GLOV) to store information such as name, contact details and protocols supported.[205] However, the creation of a global list brings challenges on its own such as how to ensure the accuracy and security of the information, determining who would have access to this information, and who would supervise the ones responsible for collecting information. These challenges need be addressed before a robust solution could be developed.[206]

The FATF stated in the 12-month review that it will continue monitoring the market and undertake a second 12-month review of the implementation of the revised FATF standards by June 2021.[207]

3.5 Conclusion

Virtual currencies confront regulators around the globe with significant challenges in ensuring that they are not used for money laundering. The travel rule aims to address the anonymity surrounding virtual currencies for the purpose of preventing and detecting money laundering. The increase of the amount information available about users transferring virtual currency, combined with blockchain technology, allows to monitor and record 'who' owns 'what' and 'when'.

[204] *Sygna* 2020

[205] Information on licensed and registered VASPs would need to be collected from each jurisdiction's list and accessed through central database (centralized) or through an API/ smart contracts which connect to each jurisdiction's list (decentralized).

[206] GDF April 7 2019, p. 5-6, FATF (2020), p. 16 recital 62

[207] FATF (June 2020), p. 2

Chapter 4 Is the FATF travel rule effective in the fight against money laundering?

4.1 Introduction

The travel rule has far-reaching consequences for users of virtual currencies, VASPs, and the virtual currency market as a whole. This chapter aims to answer the most important question in this thesis: *is the travel rule effective in the fight against money laundering via virtual currencies?* In the following pages, this chapter will discuss two main challenges that may negatively affect the travel rule's effectivity: transfers with unhosted wallets and the sunrise problem.

4.2 Unhosted wallets

The travel rule applies to transactions between VASPs. Transfers between peers (unhosted wallets) without the use of a VASP are thus not subjected to the travel rule, and other AML requirements. The exclusion of transfers via unhosted wallets easily allows for participants in the network to evade FATF travel rule.[208] For example, when Alice requests a transfer to a private/ unhosted wallet (transaction 1), Alice is then able to submit a transfer onwards to Bob's VASP (transaction 2), which will receive funds without Alice her personal information (figure 28 (3)). A significant point of concern, therefore, is that unhosted wallets are likely to become the preferred way of holding and transferring illicit virtual currencies.[209]

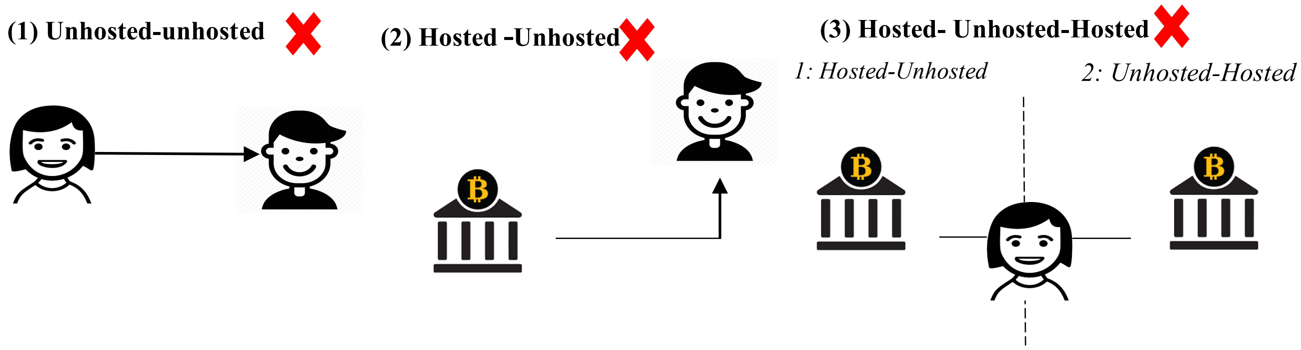


Figure 28: transactions that are not subjected to the FATF travel rule

[208] GDF April 7 2019, p. 8

[209] Shin, *Unchained* 4 August 2020, Fanusie, *Forbes* 30 October 2019

To prevent criminals from money laundering via unhosted wallets, the FATF subjects VASPs to apply a risk-based approach (RBA). The application of the RBA requires VASPs understand the money laundering risks associated with transactions, and allows VASPs to take appropriate mitigation measures given a certain level of risk.[210]

The initial risk assessment is performed on a national level. Yet, jurisdictions and VASPs should duly considers the money laundering indicators identified by the FATF.[211] In June 2019, the FATF issued *a guidance for a risk-based approach to virtual assets and virtual asset service providers*.[212] The guidance helps FATF member jurisdictions and VASPs to identify and mitigate risks associated with virtual currency activities while focusing, especially, on factors that further obfuscate transactions or complicate a VASPs ability to identify the customer, including the use of mixers and privacy coins.[213] To further assist VASPs in the application of an effective RBA, the FATF also issued an extensive report on red flag indicators in September 2020, all of which are specific to the nature of virtual currencies and their associated financial activities. Among other things, the FATF mentions indicators related to the size and frequency of transactions, to transactions patterns, to the level of anonymity and unusual behavior of sender and recipient.[214] A single indicator in a transaction does not necessarily indicate criminal activity, however, the presence of an indicator should encourage further monitoring, examination, and reporting where appropriate.[215]

While transactions with unhosted wallets are not subjected to the travel rule, the VASP itself is subjected to the FATF recommendations when it transacts with an unhosted wallet. The application of the RBA may allow transactions with unhosted wallet to be considered as riskier from an AML perspective. The FATF mentioned in the red flag report that such transactions are an indicator of suspicious behavior and, more importantly, in its Guidance, the FATF explicitly stated that for all transaction with a Non-VASP, the receiving VASP

[210] FATF (2012-2020), FATF (2019), p. 4

[211] FATF (2019), p. 4

[212] FATF (2019)

[213] FATF (2019), p. 12 recital 31, p. 28 recital 110, p. 36 recital 151

[214] FATF (September 2020), p. 5 ff.

[215] FATF (September 2020), p. 5, recital 10

should obtain the required originator information from the beneficiary customer.[216] Transactions outside the scope of the travel rule could therefore be subjected to various assessments, checks, and balances.[217] As a result, it will be more difficult for criminals (and legitimate users) to explain how they came into possession of the currency (see figure 29).[218]

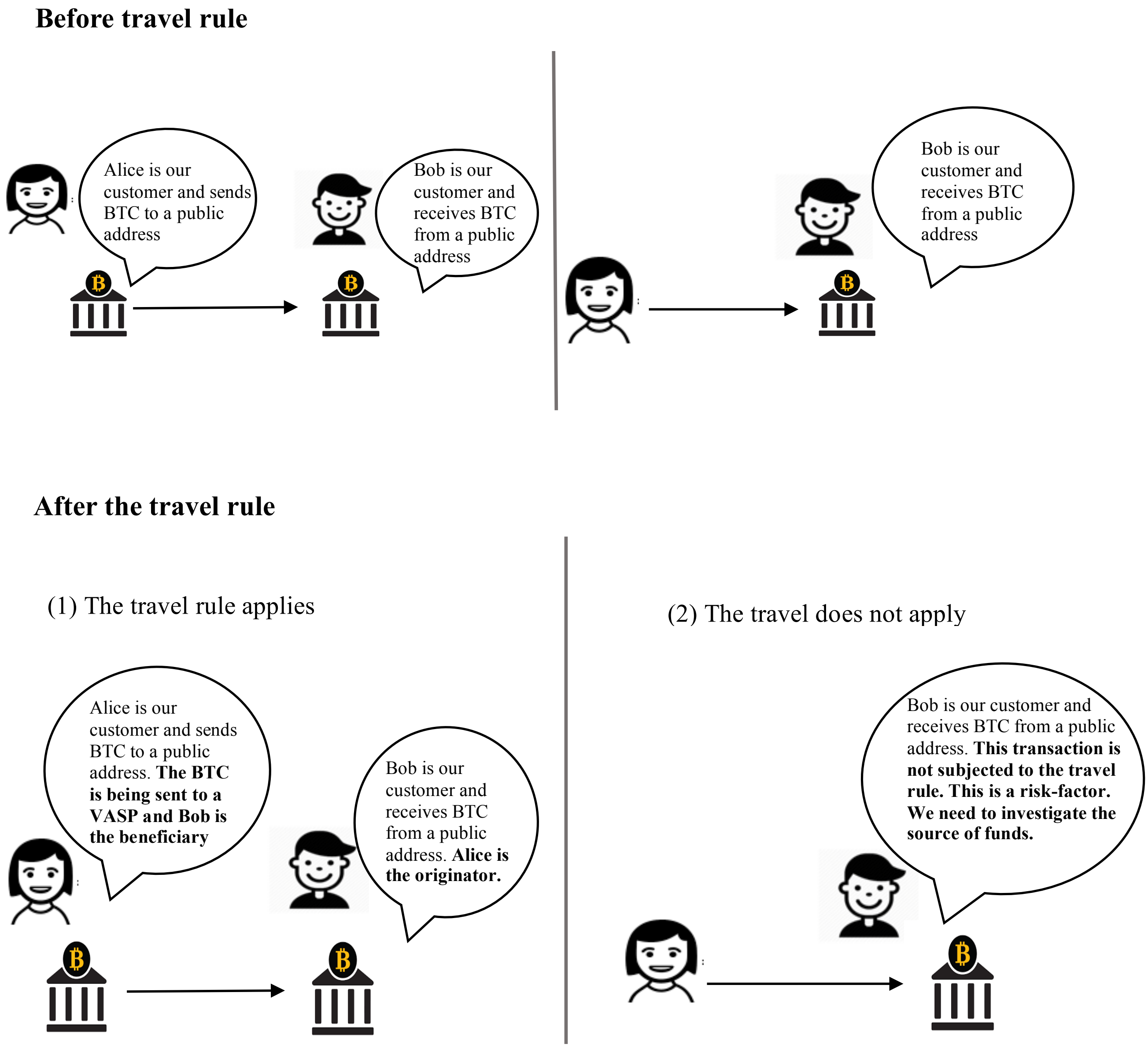

Before travel rule
Alice is our customer and sends BTC to a public address
Bob is our customer and receives BTC from a public address
Bob is our customer and receives BTC from a public address
After the travel rule
(1) The travel rule applies
(2) The travel does not apply
Alice is our customer and sends BTC to a public address. The BTC is being sent to a VASP and Bob is the beneficiary
Bob is our customer and receives BTC from a public address. Alice is the originator.
Bob is our customer and receives BTC from a public address. This transaction is not subjected to the travel rule. This is a risk-factor. We need to investigate the source of funds.

Figure 29: before vs. after travel rule

[216] FATF (September 2020), p. 10, FATF (2019), p. 30, recital 117

[217] FATF (September 2020), p. 5, recital 10

[218] FATF (2019), p. 30, recital 117

Potentially, transactions with unhosted wallets are also going to be subjected to new regulations. In the United States for example, the Financial Crimes Enforcement Network (FinCEN) issued a proposal to subject VASPs to a new set of rules on 18 December 2020.[219] When VASPs transact with an unhosted wallet, and a transaction-value larger than 3,000 dollars, it must verify the customer's identity, collect information about the name and address of the transacting counterparty, and retain records of the customer's transaction and the counterparty. Additionally, when the cumulative transaction-value exceeds 10,000 dollars within a 24-hour period, the proposed rule would require VASPs to submit a detailed report to FinCEN, including information about the name and address of the customer, and the transacting counterparty. If adopted, the rule would create significant identity verification requirements and obligations for recordkeeping and reporting.[220]

4.3 The sunrise issue

Another concern, the so-called 'sunrise issue', follows from the fact that the travel rule is going to be implemented country by country. [221] The implementation of the recommendations set by the FATF are extremely region-specific. Some jurisdictions take initiative while others wait for the development of holistic and scalable technological solutions.[222] A pressing concern is that criminals might create a shadow network of unregulated exchanges allowing them to launder money from countries that have not yet implemented the FATF recommendations. [223]

The sunrise issue remains prevalent until all jurisdictions have introduced the travel rule requirement and, as of today, a significant number of FATF members has not yet done so.[224] It is expected, however, that most jurisdictions will implement the revised FATF recommendations eventually, as the FATF regularly monitors its members. When a jurisdiction repeatedly fails to implement the recommendations, and is considered to be a

[219] U.S. Department of the Treasury, press release 18 December 2020

[220] U.S. Department of the Treasury, press release 18 December 2020, JJ, *Ciphertrace* 18 December 2020

[221] Shin, *Unchained* 4 August 2020

[222] FATF (June 2020), p. 12 recital 43

[223] Allison, *Coindesk* 21 May 2020

[224] FATF (June 2020), p. 12 recital 43, p.17 recital 66

global AML liability, the FATF may add the country to a high-risk monitoring list and, so, negatively affect a country's accessibility to the (worldwide) financial system.[225]

To address money laundering during the sunrise period, the FATF should give guidance on how regulated VASPs should deal with unregulated VASPs. [226] A regulatory push preventing regulated VASPs from dealing with unregulated VASPs might arise in the future. As such, the unregulated VASPs would be frozen out of a large part of legitimate liquidity. To mitigate the risks effectively, a coordinated approach across jurisdictions is desirable.[227]

4.4. No more money laundering via virtual currencies?

The travel rule is likely to be an effective means to combat money laundering. By increasing the amount of information available on users transferring virtual currencies, the travel rule improves the authorities' ability to 'follow the virtual currency'. [228]

However, the travel rule is not a panacea for a money laundering free world. Criminals will continue to explore new methods to launder money with and, ultimately, adapt to increased restrictions in the regulated sector.[229] To mitigate this problem, the FATF should continue to monitor market trends and gain an understanding of new ways in which technology can be abused by criminals.

Another challenge is that not every country in the world is a FATF member.[230] Examples of countries that are not a FATF member are South Jordan, Kazakhstan, Myanmar, Cuba, Panama, Croatia, Latvia, Lithuania, Estonia.[231] The above-mentioned countries are not subjected to any of the FATF recommendations but can still transact with countries located in

[225] *FATF*, High-risk and other monitored jurisdictions, Allison, *Coindesk* 21 May 2020, Ghoshray 2014-2015 (Volume 59 N.Y.L. Sch. L. Review) p. 528, 530

[226] Shin, *Unchained* 4 August 2020

[227] Allison, *Coindesk* 21 May 2020

[228] FATF (2012-2020), INR 15, p. 78

[229] HM Treasury December 2020, p. 4

[230] *FATF*, countries

[231] Eastern European countries who are a EU member state, could indirectly be subjected to the FATF recommendations, because the European Commission is a member of the FATF.

FATF jurisdictions. For example, an exchange in Panama that is not subjected to the travel rule can still transact with a VASP in France which is subjected to the travel rule. To address the risks of money laundering via non-FATF jurisdictions, VASPs should treat transactions from jurisdictions that lack (adequate) AML controls as riskier from an AML perspective.[232]

Furthermore, FATF member jurisdictions that do not want to implement the FATF recommendations will always remain, as will jurisdictions that do implement the recommendations but turn a blind eye on VASPs that do not have adequate controls in place.[233] For the purpose of achieving compliance, The FATF should continue to monitor its member jurisdictions closely. To combat money laundering, VASPs should treat transactions from such jurisdictions as riskier. [234]

4.4 Conclusion

This chapter argues that in time the global adoption of the travel rule will reduce the abuse of virtual currencies for money laundering. The exclusion of unhosted wallets is not likely to significantly impact the effect of the travel rule. The application of a risk-based approach allows transactions with unhosted wallets to be subjected to a greater level of AML scrutiny. Furthermore, the sunrise issue is likely to affect the travel rule short-term as it is expected that most countries will implement the travel rule. While the travel rule is likely to be effective in the fight against money laundering, money laundering via virtual currencies will remain an issue.

[232] FATF (September 2020), p. 17, recital 16

[233] *FATF*, High-risk and other monitored jurisdictions

[234] FATF (September 2020), p. 17, recital 16

Chapter 5 Conclusion

Recent innovation has rapidly changed the financial landscape. The emergence of virtual currencies, especially, has gave rise to a fundamental reinvention of how goods, services, and assets are exchanged.

A lack of effective oversight has contributed to the potential benefits of virtual currencies, such as low transaction fees and processing times. However, it also leaves unaddressed potential risks for exploitation. The most critical risks that demand a response are those related to anonymity, varying from complete anonymity to pseudo-anonymity.

Recently, the Financial Action Task Force (FATF) updated its recommendations. The update of the FATF in 2019 goes beyond the requirements posed by the EU AMLD5. To address the risks presented by (pseudo)anonymous transfers, the FATF subjects virtual assets service providers (VASPs) to the same regulations already in effect for financial institutions, including the travel rule. The travel rule requires VASPs to collect, store, and exchange originator- and beneficiary information with the receiving VASP. In combination with blockchain technology, this information ought to offer an effective and powerful set of tools for authorities to monitor and record the audit trail of suspicious transactions.

In this thesis, an answer is sought to the question of whether the FATF travel rule is an effective means in the fight against money laundering via virtual currencies. Two main concerns could possibly impact the effect of the travel rule.

The first concern is that the inclusion of virtual asset service providers (VASPs) will not address the issue of anonymity wholly. Virtual currencies can be transferred between peers (unhosted wallets) without the use of a VASP. Criminals might potentially use unhosted wallets to evade the travel rule.

To combat the risks of money laundering via unhosted wallets, the FATF requires VASPs to apply a risk-based approach (RBA). Transactions with an unhosted wallet are likely to be identified as ‘riskier’ from a money laundering perspective and are therefore likely to be under greater levels of AML controls, especially since the FATF explicitly stated that for transactions with a Non-VASP, the receiving VASP should obtain information about the originators’ identity from the beneficiary customer.

The second concern refers to the sunrise issue. Jurisdictions will implement the travel rule according to their own implementation deadlines and, so, a period will exist in which some jurisdictions have implemented the travel rule and others have not. Problematically, criminals may choose to operate from countries that do not have adequate travel rule regulation in place.

Most jurisdictions are expected to implement the revised FATF standards. In the end, no jurisdiction wishes to be added to the high-risk monitoring list and lower its accessibility to the financial system. To mitigate the risks of money laundering during the sunrise period, sufficient information is required of how regulated VASPs should treat VASPs located in jurisdictions without FATF standards. To prevent gaps in the regulatory framework, a coordinated approach is desirable.

In the coming months, it will become clear how jurisdictions will implement the travel rule and how VASPs will comply with the FATF standards. This thesis argues that the travel rule is an effective first step towards a more regulated virtual currency environment. The travel rule increases the amount of information about users transferring virtual currencies and, thus, helps to prevent and detect financial crime.

While the revised FATF recommendations, including travel rule, are likely to bring about a more harmonized and robust AML framework, money laundering via virtual currencies remains an issue that needs to be closely monitored. To combat this issue, the FATF should continue to assess its member jurisdictions, and closely monitor market trends as well as gain understanding of new ways in which technology can be abused by criminals.

Bibliography

Andrew, *Byzantine* 18 May 2018

Andrew, ‘Blockchain fundamentals #2: What are UTXOs?’, *Byzantine* 18 May 2018, medium.com

Albrecht, *Cryptoticker* 20 January 2020

J. P. Albrecht, ‘What is a Bitcoin mixer and how does it work?’, *Cryptoticker* 20 January 2020, cryptoticker.io

Allison, *Coindesk* 21 May 2020

I. Allison, ‘Crypto ‘Gray’ Markets Unintended Consequences of FATF Travel rule’, *Coindesk* 21 May 2020, coindesk.com

Antonopoulos 2014

A.M. Antonopoulos, Mastering Bitcoin, O’Reilly Media, Inc, Usa 2014, cyperpunks-core.github.io

Arslanian & Fischer 2019

H. Arslanian & F. Fischer, The Future of Finance, Palgrave Macmillan, 2019

***Bitpanda Academy* 2014**

‘What is double-spending and why is it such a problem?’, *Bitpanda Academy* 2014, bitpanda.com

Bryant, *The Startup* 25 September 2019

A. Bryant, ‘Using Instant Messenger to Explain the FATF Travel Rule for VASPs’, *The Startup* 25 September 2019, medium.com

Cawrey, *Coindesk* 5 March 2014

D. Cawrey, ‘How Economist Milton Friendman Predicted Bitcoin’, *Coindesk* 5 March 2014, coindesk.com

***Chainalysis* January 2020**

‘The 2020 State of Cypto Crime’, *Chainalysis* January 2020, go.chainalysis.com

***Coingecko* 2020**

‘Top Cryptocurrency Exchanges Ranking by Trust Score’, coingecko.com

***DNB, De Nederlandse Bank* 4 mei 2020**

DNB, ‘Toezichtkosten’, *De Nederlandse Bank* 4 mei 2020, dnb.com

DNB, *De Nederlandse Bank* 23 september 2020

DNB, ‘Het screenen van de tegenpartij bij een (inkomende en uitgaande) transactie’, *De Nederlandse Bank* 23 september 2020, toezicht.dnb.nl

***Elliptic* 18 September 2019**

‘Bitcoin Money Laundering: How Criminals Use Crypto (And How MSBs Can Clean Up Their Act)’, *Elliptic* 18 September 2019, elliptic.co

***Everbloom Crypto Exchange Blog* 7 June 2018**

‘What Are Decentralized Exchanges?’, *Everbloom Crypto Exchange Blog* 7 June 2018, medium.com

Fanusie, *Forbes* 30 October 2019

Y. Fanusie, The Travel Rule is Not Enough If Crypto Gets Adopted’, *Forbes* 30 October 2019, forbes.com

FATF

FATF, Fatf.org

FATF (2019)

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, www.fatf-gafi.org/ publications/ fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

FATF (June 2020)

FATF (2020), *12-month Review of the revised FATF Standards on VASPs,* FATF, Paris, France, www.fatf-gafi.org/ publications/ fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

FATF (September 2020)

FATF (2020), *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, FATF, Paris, France, www.fatf-gafi.org/ publications/ fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html

FATF (2012-2020)

FATF (2012-2020), *International Standards on Combating Money-Laundering and the Financing of Terrorism & Proliferation,* FATF, Paris, France, www.fatf-gafi.org/recommendations.html

Foxley, *Coindesk* 27 April 2020

W. Foxley, 'Netherlands AMLD5 regulations hurting bitcoin firms', *Coindesk* 27 April 2020, coindesk.com

Gatti, *The Cryptonomist* 4 August 2019

M. Gatti, 'The Byzantine Generals problem and Bitcoin's solution', *The Cryptonomist* 4 August 2019, en.cryptonomist.ch

GDF April 7 2019

Letter from Global Digital Finance, *GDF Input to the FATF public statement (the 'Public Statement') dated February 22*, 2019, April 7 2019

Ghoshray 2014-2015 (Volume 59 N.Y.L. Sch. L. Review)

Dr. Saby Ghoshray, 'Compliance Convergence in FATF rulemaking: The Conflict Between Agency Capture and Soft Law, 59 N.Y.L. Sch. L. Rev (2014-2015)

Groot & Leupen, *Het Financieele Dagblad* 22 September 2020

G. de Groot & J. Leupen, 'ING worstelt al jaren met ongrijpbaar Pools dochterbedrijf', *Het Financieele Dagblad* 22 September 2020 fd.nl

Groot & Leupen, *Het Financieele Dagblad* 25 September 2020

G. de Groot & J. Leupen, ‘Gelekte meldingen laten zien hoe het piept en kraakt bij banken’, *Het Financieele Dagblad* 25 September 2020, fd.nl

Hamacher, *Decrypt* 14 Jan 2020

A. Hamacher, ‘New money laundering regulations threaten crypto firms in Europe’, *Decrypt* 14 Jan 2020, decrypt.co

Harding, *The Guardian* 5 April 2016

L. Harding, ‘What are the Panama Papers? A guide to history’s biggest data leak’, *The Guardian* 5 April 2016, theguardian.com

Hardjono et al. 30 April 2020

T. Hardjono, A. Lipton & A. Pentland, *Building the New Economy* 30 April 2020, wip.mitpress.mit.edu

He 2016 (SDN/16/03)

D. He et al., ‘Virtual Currencies and Beyond: Initial Considerations’, *IMF Staff Discussion Note* January 2016 (SDN/16/03)

HM Treasury December 2020

HM treasury, ‘National risk assessment of money laundering and terrorist financing 2020’, HM Treasury December 2020, assets.publishing.service.gov.uk

Holzborn & Oleshchuk, *Orrick* 9 December 2019

T. Holzbom & O. Oleshchuk, Germany: The Implementation of the Fifth Anti-Money Laundering Directive in German Law – Thighten The Thight?, *Orrick* 9 December 2019, mondaq.com

Houben & Sneyers, PE 619.024 2018

Prof. Dr. Houben, R., Sneyers A., *Cryptocurrencies and blockchain, study for the Committee on Financial Crimes*, *Tax evasion and Tax avoidance,* Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, PE 619.024 2018

Houben & Sneyers PE 648.779 2020

Prof. Dr. Houben, R., Sneyers A., *Crypto-Assets – Key developments, regulatory concerns and responses*, Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020

International Finance Corporation 2019

International Finance Corporation, Anti-Money Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, International Finance Corporation 2019, ifc.org

JJ, *Ciphertrace* 18 December 2020

JJ, FinCEN Proposed Rule Change for Unhosted CVC Walelts, *Ciphertrace* 18 December 2020, ciphertrace.com

Kaminska, *Financial Times* 11 September 2019

I. Kaminska, 'Don't bet on decentralized exchanges becoming the new crypto frontier…', *Financial Times* 11 September 2019, ft.com

Kuskowski, *Forbes* 2020

P. Kuskowski, 'Travel Rule Requirements Need Not Block Private Bitcoin Wallets, *Forbes* 2020, forbes.com

Küfner, *Nakamo.to* 15 August 2018

R. A. Küfner, 'The Byzantine Generals problem', *Nakamo.to* 15 August 2018, medium.com

Lastra & Allen, PE 619.020 2018

R. M. Lastra, J.G. Allen, *Virtual currencies in the Eurosystem: challenges ahead,* Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, PE 619.020 2018

Laurence 2019

T. Laurence, Introduction to Blockchain Technology, Van Haren Publishing 2019

***Learn me a bitcoin* 2015**

G. Walker, *Learn me a bitcoin* 2015, learnmeabitcoin.nl

Lemereis *rtlnieuws* 25 February 2014

D. Lemereis, ‘De Grote Bitcoin-crisis: MtGox offline na ‘mega-hack’, rtlnieuws 25 February 2018, rtlnieuws.nl

Liu 2011

D. Liu, Next Generation SSH2 Implementation: Securing Data in Motion, Syngress 2011

M., B*itDegree* 11 September 2020

Laura M., ‘What is a smart contract and how does it work?’, *BitDegree* 11 September 2020, bitdegree.org

Madeira, *Cointelegraph* 29 February 2020

A. Madeira, ‘Defining Bitcoin: Money, Currency or Store of Value’, *Cointelegraph* 29 February 2020, cointelegraph.com

Madhavji, *Altcoin Magazine* 26 November 2019

A. Madhavji, ‘This is How Cryptocurrencies Stand To Help The 1.7 Billion Unbanked’, *Altcoin Magazine* 26 November 2019, medium.com

Madhavji & Tan, *Cointelegraph* 30 July 2020

A. Madhavji & A. Tan, ‘Comparing Money Laundering With Cryptocurrencies and Fiat’, *Cointelegraph* 30 July 2020, cointelegraph.com

Mandel, *BQT.io* 7 April 2019

E. W. Mandel, ‘Evolving to succeed, not just to evolve’, *BQT.io* 7 April 2019, medium.com

Marr, *Bernard Marr & Co*

B. Marr, ‘A short history of Bitcoin and Crypto Currency Everyone Should Read’, *Bernard Marr & Co*, bernardmarr.com

Martin, *Cointelegraph* 15 April 2020

J. Martin, ‘Dutch AMLD5 implementation leaves crypto companies footing the bill’, *Cointelegraph* 15 April 2020, cointelegraph.com

Miggiani, *Regulation Y* 14 June 2020

K. Miggiani, ‘AMLD5 and the EU May 2020 AML/CFT Action Plan – where do crypto assets fit into the emerging landscape?’, *Regulation Y* 14 June 2020, regulation-y.com

Milea, *Inbound FinTech* 21 October 2020

M. Milea, ‘How The Travel Rule is Reshaping Crypto’, *Inbound FinTech* 21 October 2020, blog.inboundfintech.com

Nakamoto 2009

S. Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, March 2009, bitcoin.org/bitcoin.pdf

Narayanan & J. Bonneau 2016

A. Narayanan & J. Bonneau, Bitcoin and Cryptocurrency Technologies, Princeton University Press 2016

O’Neal, *Cointelegraph* 13 October 2019

S. O’Neal, ‘Can Crypto Exchanges Ever Be Truly Decentralized?’ *Cointelegraph* 13 October 2019, Cointelegraph.com

Partz, *Cointelegraph* 12 May 2020

H. Partz, ‘FATF’s Deadline for Travel Rule Is a Bit of a Myth, Says Siân Jones, *Cointelegraph* 12 May 2020, Cointelegraph.com

Perryer, *European CEO* 11 March 2019

S. Perryer, ‘A costly affair: Why Europe is losing the fight against money laundering’, *European CEO* 11 March 2019, europeanceo.com

Rebora, *Coinmonks* 29 December 2019

A. Rebora, ‘The Use of Cryptocurrency for money laundering’, *Coinmonks* 29 December 2019, medium.com

Reuter & Truman November 2004

P. Reuter & E. M. Truman, Money Laundering: Methods and Markets, *Chasing Dirty Money* November 2004, piie.com

Shin, *Unchained* 4 August 2020

L. Shin, Why The Travel Rule is One of the Most of Significant Regulations In Crypto, *Unchained* 4 August 2020, unchainedpodcast.com

***Simply Explained* 13 November 2017**

‘How does a blockchain work – Simply Explained’, *Simply Explained* 13 November 2017, Youtube.com

Sygna 2020

‘A guide to the EU’s 5th Anti-Money Laundering Directive (AMLD5), Sygna 2020, sygna.io

Taçoğlu, *Binance Academy*

C. Taçoğlu, ‘Trustless’, *Binance Academy* 2020*,* academy.binance.com

***The World Bank* 19 April 2018**

‘Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows’, *The World Bank* Press release 19 April 2018, worldbank.org

***True Energy Crypto* 28 September 2017**

‘Banking On Bitcoin – Crypto Currency Documentary’, *True Energy Crypto* 28 September 2017, Youtube.com

U.S. Department of the Treasury, press release 18 December 2020

U.S. Department of the Treasury, The Financial Crimes Enforcement Network Proposes Rule Aimed At Closing Anti-Money Laundering Regulatory Gaps For Certain Convertible Virtual Currency and Digital Asset Transactions, U.S. Department of the Treasury, press release 18 December 2020, home.treasury.gov

Wallace, *Wired* 23 November 2011

B. Wallace, ‘The Rise and Fall of Bitcoin’, *Wired* 23 November 2011, wired.com

Williams-Grut, *Insider* 17 January 2018

O. Williams-Grut, ‘Here are all the theories explaining the crypto market crash’, *Insider* 17 January 2018, insider.com

Van Wirdum, *Bitcoin Magazine* 18 November 2015

A. Van Wirdum, Is Bitcoin Anonymous? A complete Beginner’s Guide’, *Bitcoin Magazine* 18 November 2015, bitcoinmagazine.com