TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Eduardo da Cruz Rodrigues e Silva

LEGAL FRAMEWORK OF INITIAL COIN OFFERINGS

Master's thesis
Programme Law, specialisation law and technology

Supervisor: Thomas Hoffmann, Assoc. Prof.

Tallinn 2018

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 19899 words from the introduction to the end of conclusion.

Eduardo da Cruz Rodrigues e Silva ……
(signature, date)

Student code: 177182HAJM
Student e-mail address: silva.ecr@gmail.com

Supervisor: Thomas Hoffmann, Assoc. Prof.:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence

……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The aim of this Master Thesis is to analyse whether there is legislation that applies to Initial Coin Offerings and, if not, whether there should be legislation on this area. The methods used are legal analysis based on academic sources and on the understanding of the law of both European and national level (Estonian). United States legal sources are also used to give a better understanding of a phenomenon that is global due to its use of the Internet and Blockchain.

The hypothesis that will be tested in this thesis is that ICOs are not regulated by the current legal framework and they need specific regulation in the future and present the main concerns and recommendable practices for regulation of ICOs.

The thesis will conclude that there are current applicable laws depending on the rights associated with the token and, besides that, there is a specific need for regulation to harmonize interpretation, avoid uncertainties and protect the token buyers.

Keywords: Initial Coin Offering, Token, Cryptocurrency, Smart Contract, Blockchain.

INTRODUCTION

The analysis of the legal framework applicable to Initial Coin Offerings is the topic selected for the elaboration of this Master thesis because it consists in the use of new technologies, especially Blockchain technology that was invented as the supportive technology for the decentralised record of transactions of Bitcoin, the first cryptocurrency.

This topic is very novel since the first ICO ever made took place in the year of 2013 and only in 2017 it reached a considerable magnitude when considering the value raised by start-ups that chose this financing mechanism.

Furthermore, the topic of regulation of ICOs is relevant in the present, especially after the sudden loss of value of Bitcoin, in the transition between 2017 to 2018, being alarming to many investors and crypto currency holders. This sudden price fall raised awareness for the possible lack of legal protection in crypto businesses and the real need for the regulators worldwide to take a position about cryptocurrencies and about ICOs. However, in order to regulate ICOs, a good understanding of this process is required.

Initial Coin Offerings are a new way of raising funds for start-ups that are in the field of technology and want to issue cryptocurrency (tokens) in exchange for those funds. ICOs are becoming a strong alternative in crowdfunding to the more traditional venture capital, angel investors and accelerators.

However there is regulatory uncertainty on how to classify them for purposes of Taxation or Anti-Money Laundering, for example. "As virtual currencies are a new phenomenon and as yet not widely spread in terms of market capitalization, there is almost no regulation of their transactions. They can be used as payment vehicles as well as for speculation purposes."[1]

There is a big scale of uncertainty on the regulation of ICO. Different jurisdictions have different approaches to this Fintech mechanism, with positions that go from support to complete ban, passing through jurisdictions that look to this topic with special caution.

The assessment of legal framework regarding Initial Coin Offering is an urgent matter because in practice, "as the ecosphere of Internet finance continues to mature, it will penetrate deeper into the everyday scenarios of its consumers, in turn posing a significant threat to the dominant position occupied by banks."[2]

[1] Sauer, B. (2016). Virtual currencies, the money market, and monetary policy. International Advances in Economic Research, 22(2), 117-130.

[2] Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. Financial Innovation, 2(1), 24.

It is certainly in everyone's best interest that the applicability of legislation is clear and efficient because this technologies that wish to eliminate the middle man are spreading and reaching a wide portion of the population.

The main aim of this Master's thesis is to highlight the main legal problems that originate with conducting ICO as well as by using its underlying technologies: cryptocurrencies, distributed ledger technology (or blockchain technology) and smart contracts.

The Hypothesis is: ICOs are not regulated by the current legal framework and they need specific regulation in the future.

The main question of the thesis will be answered in the following chapter and consist in knowing: What are the risks of ICOs? What is the legal value of a Token? What regulations already apply? What are the possible regulatory approaches?

Chapter 1 will include the introduction to the concept of an Initial Coin Offering as a crowdfunding mechanism and differentiate it from traditional Initial Public Offerings (IPOs).

After that, a distinction will be made between the coin issued by the Initial Coin Offering, the token, and the general cryptocurrencies, that generally are mined and/or have their own blockchain technology associated.

A general overview of distributed ledger technology and smart-contracts will take place as they are the supportive technologies behind the process of an Initial Coin Offering.

Chapter 2 will identify the legal problems and issues that originate from ICOs. It will contain a brief economical and extended legal perspective of the value of the token issued.

It will highlight the fraud and pyramid schemes that concern the raising of crypto or traditional fund process and identifies the general risks associated, as well as it contains a first approach to the applicability of existing legal framework to ICOs.

Chapter 3 will consider the legal framework of Estonia based on the anti-money laundering rules, civil law, with consideration to the applicability of sale or loan contracts to tokens or ownership protection.

The comparison with Initial Public Offerings will be established and analysed as well as the securities requirements, which constitute the main financial law approach to ICOs. Brief references are made to consumer protection and taxation issues.

Chapter 4 will show how ICOs are already being regulated by some jurisdictions and what are the perspectives and possible methodologies for the future of ICO regulations.

The possibility of ICOs being in the scope of a multitude of jurisdictions is also analysed from the context of Private International Law.

1. WHAT IS AN ICO

ICO stands for Initial Coin Offering. It is difficult to define what it exactly is because of its technological novelty and different uses that can be attributed. It can be looked as a mechanism for crowd funding, as normally the token issuer is still looking for funds to develop its platform and will allocate the raised funds for that purpose. However, the tokens issued (the coin offered) is so connected with cryptocurrencies and might have so many different functions and attribute different rights, that the definition of an ICO is very difficult to reach in a wide view. This is also a reason that will be further explained on why there is a need for regulatory clarification and the need for clear conceptual definitions.

Adhami et al. elaborated an analysis on enterprises choosing to conduct ICOs to develop their businesses. It is noted the similarity between ICOs and IPOs, which are Initial Public Offerings that consist on the issuance of company's share regulated by financial supervision authorities and which respect the registration of those issued securities and the elaboration of a prospectus, because of the characteristic that both institutional investors and small retail investors are reserved tranches of securities in the IPO case or tokens in the ICO case. The crypto offering is targeted to the community users, the project managers, bounties, which are rewards related to marketing and expansion of the community, and the crowd of the Internet. It is further added a very important characteristic of the ICOs that is the fact that the tokens may be sold on a secondary market, in exchange platforms that connect the sellers of the tokens that usually establish their own parameters of the sale, for example the minimum price they are willing to sell the token for, and the buyer that can choose from a set of predefined and accepted tokens and exchange them for cryptocurrencies. The indicated similarities between the ICOs and crowdfundings, include low protection of contributors, limited set of information available and no relevant track record for the proponents. The main difference is the fact that crowdfunding start-ups collect fiat money through traditional payment channels, while ICOs offer tokens and rely on cryptocurrency blockchains.[3]

"Crowdsourcing takes place when a profit-oriented firm outsources specific tasks essential for the making or sale of its product to the general public (the crowd) in the form of an open call over the internet, with the intention of animating individuals to make a voluntary contribution to the firm's production process for free or for significantly less than that contribution is worth to

[3] Adhami, S., Giudici, G., Martinazzi, S. (2017) Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings. *Social Science Research Network.*

the firm."[4] This idea of crowdsourcing that can be understood as a synonym to crowdfunding is very accurate for the raising of funds through an ICO because the rights associated with the token are very often the right to use the future to be launched platform which have a hypothetical value that is less valuable for the buyer than it is for the issuer that needs to develop its business idea. The statement cannot however be fully transposed to the ICO business because not all companies are profited-oriented, some are foundations, and there is almost always the possibility to exchange the token in secondary market which gives it an intrinsic speculative value.

In the traditional crowdfunding model, the "entrepreneur is usually unable to identify the consumers. The entrepreneur must then use some self-selecting device to induce high-paying consumers to reveal themselves."[5] This characteristic of finding the right crowd does not apply exactly to ICOs. It is true that a community is based around a product or service but other buyers are actually investors that try to find the most promising ideas and business plans, in order to by a token at discount or initial low price and expect that once the platform is operational the token price will raise because of demand.

The assessment of an ICO platform, product or service is done through reading the ICO Company's Whitepaper. This document shows once more the apparent similarity between ICOs and IPOs since it can be looked at as a prospectus in an IPO. Whitepapers are usually one of the documents that are disclosed in the token issuer website. Others documents are the Token Sales Agreement, that includes the legal definitions, conditions of sale and limitations of liability mainly, and simple version of the business plan description or even the results of Howey Test[6] for assessment of Securities. This test is used not only when the ICO has its jurisdiction in the United States of America but also when the company is planning to issue tokens to the American people.

The Whitepaper includes the problem that exists, the solution that the company presents which is the platform that is or will be developed, the allocation of funds, the allocation of tokens, the total supply of tokens, the used Blockchain, normally Ethereum Blockchain as explained further, the roadmap, and the description of the team behind the project.

ICOs make a strong effort to build a community around their platform through publications in Medium, discussions in forums and use of social networks, for example Twitter. This is done for the purpose of creating a network effect around the token. The ultimate goal could be that other

[4] Kleemann, F., Voß, G., Rieder, K. (2008). Un(der)paid Innovators: The Commercial Utilization of Consumer Work through Crowdsourcing. Science, *Technology & Innovation Studies, 4(1),* 5 - 26.

[5] Belleflamme, P., Lambert, T., Schwienbacher, A. (2014). Crowdfunding: Tapping the right crowd. *Journal of business venturing, 29(5),* 585-609.

[6] U.S. Supreme Court SEC v. Howey Co., 328 U.S. 293 (1946) *Securities and Exchange Commission v. Howey Co*

persons would start accepting the issued token as a mean of payments and eventually turn into a cryptocurrency. Even if this is not the main goal, the network effect calls users to the platform and increases the value of the token.

"Initially, the creator of a cryptocurrency is the only party that recognizes and accepts that cryptocurrency, which makes it difficult to persuade others to adopt it. However, as more and more users appear, the cryptocurrency becomes more attractive. (…) a large difference in quality (real or perceived) between the entrant and the incumbent may offset the discrepancy in the strength of the network effects. Whether this happens with new cryptocurrencies is an empirical question".[7]

1.1 Difference between token and Bitcoin

This thesis does not intend to conduct a study on Bitcoin but its relevance to the legal framework is very relevant because they are interconnected in the sense that most ICO launchers accept Bitcoin as payment for the tokens and almost all crypto exchanges include Bitcoin as an available currency, which is especially important in the tokens secondary market.

Nevertheless Tokens and Bitcoin are not the same. For the next chapters' legal considerations, it is essential to make a comparison and to establish the differences.

Bitcoin and other cryptocurrencies, altcoins or simply coin are backed by their own Blockchain. This means that the transactions of a specific coin is verified and saved in their own Blockchain, which is similar to a digital ledger. People are motivated to do this work by the grant of cryptocurrency associated with that Blockchain and by transaction fees.

"One of its most distinguishing features is that the registration of transactions is done through the so-called mining activity undertaken by certain entities. Such activity consists of solving a puzzle requiring high computational power, since registration of a block of transactions can only take place once the puzzle has been solved. Providing the right economic incentives to solve the puzzle is very important for the transactions to be registered on the underlying ledger."[8]

Bitcoins have a maximum limit that will ever be mined (slightly under 21 million coins). Every couple of years the creation of a new block in the Blockchain is rewarded with less bitcoins. Bitcoin's algorithm was built in a way that the incentive would transition from mined coins to only transaction fees when all coins are mined. Yet, "to date, transaction fees have primarily

[7] Halaburda, H. (2016). Digital Currencies: Beyond Bitcoin. *SSRN*
[8] Dimitri, N. (2017). Bitcoin Mining as a Contest. *Ledger*, *2*, 31-37.

been used to discourage overuse of the network with many small transactions (called penny flooding) and have never provided more than 1–2% of mining revenue. Fee values have primarily been determined by defaults configured in the reference client, with a small number of users opting to pay higher fees to have their transactions published more quickly."[9]

Tokens in an ICO are not mined; they are issued or allocated after the payment determined in the Token Sale Agreement. For that reason tokens can also be considered to be pre-mined. There is a total amount of tokens that will be available as in Bitcoin, but there are no miners, since ICO companies use a cryptocurrency Blockchain to save and verify the token transactions.

"In Bitcoin-like cryptocurrencies the mining process is usually a race among the miners to see who finds the proof first."[10] In ICOs, the terms and conditions for the sale of tokens are pre-determined and usually if there are tokens that are not sold, that amount is burned, meaning that they are sent to a frozen wallet and cannot be accessed.

Mining cryptocurrencies using proof-of-work requires an expensive amount of hardware and use too much energy. A proposed alternative is starting to be more used and it is called proof-of-stake. This means that the work of verification of transactions is not done via computational power but by ownership of virtual currencies. "Virtual mining offers two main benefits: first, it may be more difficult for an attacker to acquire a sufficiently large amount of digital currency than to acquire sufficiently powerful computing equipment. Second, by avoiding the consumption of real resources (*i.e.*, compute cycles), no real-world resources are wasted."[11]

1.2 Problems related with Bitcoin

Bitcoin has the largest market cap with an approximate value of $177,000,000,000[12] and the second biggest coin (Ethereum) has a market cap of around $84,000,000,000.[13]. These two coins are usually the medium of exchange for tokens during the ICO token sale, even though some issuing companies also accept fiat currency. The connection between cryptocurrencies and tokens is high due to this factor. This leads to the market prices and trust in cryptocurrencies to affect also the token market and the amounts raised during ICOs.

[9] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015) Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *Security and Privacy (SP), IEEE Symposium on 2015*, IEEE, 104-121.

[10] Biryukov, A., Khovratovich, D. (2017). Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger, 2*, 1-30.

[11] Bonneau (2015) *supra nota* 9

[12] https://coinmarketcap.com/

[13] *Ibid.*

Cryptocurrencies have been all over the news with allegations of being a Ponzi or a pyramid scheme and also due to the high volatility of their prices. However, there are some problems in the present that are either a limitation or a real issue that influence the ICO ecosystem. Those problems are Bitcoin's transaction limits, the favouring of anonymity and the connection with criminal activities.

"Each transaction is at least 250 bytes. Dividing 1 million by 250, we see that each block has a limit of 4000 transactions, and given that blocks are found about every 10 minutes, we're left with about 7 transactions per second, which is all that Bitcoin network can handle. (…) It's quite low compared to the throughput of any major credit card processor. Visa's network is said to handle about 2000 transactions per second around the world on average and is capable of handling 10000 transactions per second during busy periods."[14]

The main problem that originates from the transaction limit is the fact that miners fees raise with higher demand. This way "small casual transactions are starting to shift to alternative networks, because it's impossible to support small transactions when each transaction costs $20 in fees".[15] If a person wants to buy 50 euros worth of tokens during an ICO, that transaction will probably not happen when transaction fees are so high. This can have a huge impact in the total funds raised even though cryptocurrencies would be thriving at that time.

Cryptocurrencies, in general, favour anonymity of ownership. The coins and tokens are stored in wallets and to make a transaction it is only needed an address that is the public key. Public keys are used to encrypt the transfer and are randomly generated with each transfer. The anonymity of cryptocurrencies creates legal problem since it makes it very difficult to establish taxable persons that do not declare earnings. Besides that, payments for illicit products or services find a way to be possible by using cryptocurrencies.

In order to prevent these problems, it is necessary to create linking techniques that would allow a fast de-anonimization, especially when required by governmental institutions and courts. Multi signature wallets are wallets controlled by three or more people and from which the funds can only be transferred when a majority gives authorization. "New linking techniques may also arrive. For example, multi-signature addresses have an unintended negative effect on privacy since the multi-sig structure in a change address can be matched to the sending address even if the keys involved change."[16]

[14] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press

[15] https://arstechnica.com/tech-policy/2017/12/bitcoin-fees-rising-high/

[16] Bonneau (2015) *supra nota* 9

The tokens issued by the ICO legal entity are also anonymous. Even if the company requires KYC questionnaire to be filled by the buyer and verification of data received, the tokens can easily become anonymous when exchanged in the secondary market for cryptocurrencies. People can buy tokens after the ICO is completed. For this reason, exchange platforms are important players in the crypto market and an important subject of regulation as further explained.

Regarding the problem of criminality and Bitcoins, Böhme et al. indicate three classes of criminal concerns about Bitcoin that are Bitcoin-specific crime, money laundering, and Bitcoin-facilitated crime. The first Bitcoin related crime consist in attacks on the currency and its infrastructure like Bitcoin theft, attacks on mining pools, and denial-of-service attacks on exchanges to manipulate exchange rates. These are difficult crimes to deal with due to their novelty, lack of clarity on which agency and jurisdiction are responsible, technical complexity, procedural uncertainty, and limited resources. The second Bitcoin-related crime makes money laundering more difficult to trace especially because of funds that are transferred through mixers, with mixing records concealed from the public. The third Bitcoin-specific crime is the easy way to pay for unlawful services and product as happened with Silk Road. It is specified that criminal tend to use cryptocurrencies because of the anonymity that it gives, the certainty that transfers cannot be changed and to be a technological alternative to cash for long distance payments.[17]

1.3 Altcoins

One of the characteristics of virtual currencies is the fact that most of them are associated with their own Blockchain. However, this is not the only indicator. Cryptocurrencies like Bitcoin and Ethereum can be called altcoins and their value is not dependent in a specific product or underlying asset but rather on their acceptance by natural and legal persons. But why are altcoins created? “Coins are invented to address specific issues such as high computation cost of PoW (proof-of-work), to increase the number of transactions per second, to increase the block size, to ensure that the ledger is not as transparent, to accommodate more efficient use of smart contracts, and so on.”[18] Tokens are sometimes described as currencies or cryptocurrencies. The following are two possible interpretations of the meaning and value that is attributed to tokens.

[17] Böhme, R., Christin, N., Edelman, B., Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29(2)*, 213-38.

[18] Chuen, K., David, L. E. E., Guo, L., & Wang, Y. (2017). Cryptocurrency: A New Investment Opportunity? *The Journal of Alternative Investments*, 20(3).

"A currency is a token of value that can be earned and deployed. A currency stores value and is transmissible. This generalized definition supports the claim that there can be many nonmonetary currencies that are conceived in the same structure. For example, reputation is a unit of value that can be earned and deployed in certain situations; it is a nonmonetary currency in the sense that it is a proxy for status or some kinds of tasks that a person can do."[19] Another view is that "cryptocurrency tokens are given to investors as a proof of future cash flow, payments, or potential future exchange, or the right to participate, vote, build blocks or purchase. On top of the future cryptocurrency benefits, the network effect of cryptocurrency may be a crucial factor in its valuation, for the associated technology and perceived value of the cryptocurrency by the public."[20]

For the purposes of Initial Coin Offering, the most relevant cryptocurrency is Ethereum because most companies choose to issue their tokens according to the ERC20 standard and the smart-contract functionality of the Ethereum platform. The ERC20 tokens means that all the wallets that support it can be used to receive the tokens issued after the token sale. Ethereum has its value because of the acceptance that Ethereum platform has seen from the ICO community and because Ethereum coins are used as the fuel for the transaction. The fees that are paid for the use of Ethereum Blockchain are paid in the native coin. The smart contracts and the tokens are programmed in Solidity, which is Ethereum programming language. "Ethereum's blockchain records contracts, which are expressed in a low-level, byte-code like, Turing-complete language. Essentially, a contract is a program that runs on every node in the Ethereum system. Ethereum contracts can store data, send and receive ether payments, store ether and execute an infinite range (hence Turing-complete) of computable actions, acting as de-centralized autonomous software agents. Ethereum can implement quite complex systems that are otherwise implemented as altchains themselves."[21]

The innovation brought by this altcoins will be further analysed in the end of this chapter. The most important innovative idea associated with this platform is in the words of Randolph Robinson the idea of programming code as Law. "This idea of code as law comes to life on the Ethereum platform, which allows nodes on the network to send and receive self-executing and enforcing smart contracts. Once launched, these contracts cannot be stopped. (…) These

[19] Swan, M., *Blockchain: Blueprint for a New Economy*, Sebastopol, O'Reilly
[20] Chuen (2017) *supra nota* 18
[21] Antonopoulos, A. M. *Mastering Bitcoin, Unlocking Digital Cryptocurrencies,* Sebastopol, O'Reilly

unstoppable, self-executing smart contracts present significant regulatory and law enforcement challenges because Ethereum participants interact pseudonymously."[22]

1.4 Blockchain technology in ICO

Blockchain is the technology included in the Bitcoin protocol and that has been replicated by other altcoins. One of the main characteristics is automation. "Based on the features of being trust-free and democratized, blockchain technology has enabled business transactions with strangers without the need for a trusted intermediary; meanwhile, software can automate such of the transaction process, allowing contractual promises to be enforced without human involvement."[23] Blockchain technology is the main reason why cryptocurrencies have real value because the transactions are verified in this digital ledger. Blockchain technology can be independent from cryptocurrencies and its use is being tested in other areas: "the enthusiasm for blockchain-based solutions has raised so high to be considered indispensable to the future of precision medicine ecosystem, improving data security, data sharing, interoperability, patient engagement by wearable sensors, AI-based diagnostics and much more."[24] In fact, blockchain technology is very important for businesses that require a stable, verifiable and secure ledger or record of transactions. "There are many nonfinancial service related opportunities where Blockchain may prove viable and beneficial. This includes other industries such as auditing, gambling, and authentication for event tickets and luxury goods."[25]

This chapter will show the essential value that Blockchain gives to ICOs.

Iansiti et al. have highlighted the five principles on how the Blockchain works. Those principles are: distributed database, peer-to-peer transmission, transparency with pseudonymity, irreversibility of records and computational logic. Blockchain is distributed because no one controls the entire database; the parties verify the records of its transaction partners directly. Storage and forwarding information is conducted between peers and not through a central node. Even though every transaction is visible to anyone with access to the system, users can choose to remain anonymous or provide proof of their identity to others. Transactions cannot be changed because they are linked to every transaction record that came before them. Blockchain

[22] Robinson, R. (2017). The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings. *SSRN*

[23] Sun, J., Yan, J., Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation, 2(1),* 26.

[24] Furlanello, C., De Domenico, M., Jurman, G., & Bussola, N. (2017). Towards a scientific blockchain framework for reproducible data analysis. *arXiv preprint arXiv:1707.06552*.

[25] Fanning, K., Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance, 27(5),* 53-57.

transactions are tied to computational programming code, which means that the transactions can be automatically triggered between nodes.[26]

The tokens issued after the ICO is completed are secured as a transaction mean by being verified in the Blockchain. "Storing certificates on the Blockchain is a cost-effective way of storing and securing vital information."[27]

The qualification of the token will be further explained in the next chapter, but a general consideration to all cryptocurrencies, altcoins or tokens is the fact that they are in their core, a data file consisting in a binary sequence. Blockchain technology guarantees that this data file are not copied and remain authentic and trusted and that has a very positive effect for ICOs. "Blockchain technology allows a network of economic agents to agree, at regular intervals, on the true state of shared data. (…) Before Bitcoin, any form of digital cash, like other digital goods, could be easily copied and double spent, making the system worthless in the absence of a central clearinghouse. Crypto tokens solve this problem by allowing for the creation and exchange of scarce, digital assets without the negative effects stemming from assigning market power to a third-party."[28]

As previously referred, most ICOs use the Ethereum platform that includes Ethereum Blockchain for the issue of their tokens. Ethereum has the "technology to allow for the writing of smart contracts. Such a contract could, for example, make payment conditional on an observable action or quality of a good or service sold, allow parents to give their kids pocket money while at the same time limiting what their children could spend it on, etc."[29]

Blockchain has developed the importance of a decentralized network of nodes that guarantee the sustainability and security of the technology. "Nodes are the connected network formed between computers that the Blockchain clients use, and in this process their computers perform the validation on transactions and they relay the information. Every time a computer joins the Blockchain network, a copy of the Blockchain is downloaded."[30]

Blockchain technology might constitute a risk to ICOs because a research has shown that "with reference to adoption, businesses should realize that the blockchain system is not yet at an optimum maturity level and should conduct extensive feasibility studies before

[26] Iansiti, M., Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95(1),* 118-127.
[27] Sá Soares, D., (2016) *Electronic Government, 15th IFIP WG 8.5 International Conference, EGOV 2016 Guimarães, Portugal, September 5–8, 2016 Proceedings*, s. l., Springer
[28] Catalini, C., Gans, J. S. (2016). Some simple economics of the blockchain (No. w22952). *National Bureau of Economic Research.*
[29] Halaburda, (2016) *supra nota* 7
[30] Botos, H. M. (2017). A Blockchain Intelligence Analysis. *Res. & Sci. Today,* 13, 42.

implementation."[31] Initial coin offering are based in experimental and not fully tested technologies that definitely present some challenges. Besides Blockchain, the other technology is the smart contracts.

1.5 Smart contracts

There are some questions about the legal definition of smart contracts and what exactly are the legal effects and/or if it is a contract at all.

"Smart contracts are programs that can establish and enforce fiduciary relations between parties (in the case of The DAO fund, to have the ability to submit transactions, including transferring money), decentralised applications or Dapps are smart contracts that include some sort of frontend or user interface. Initial Coin Offerings (ICOs) are token sales by which some of these DAOs and Dapps raise funds."[32]

The legal definition and effects of a smart contract are not the only problems that smart contracts raise. "A smart contract (or contract for short) is an autonomous agent stored in the Blockchain, encoded as part of a creation transaction that introduces a contract to the Blockchain. Once successfully created, a smart contract is identified by a contract address; each contract holds some amount of virtual coins (Ether), has its own private storage, and is associated with its predefined executable code."[33]

Raskin differentiates "Strong smart contracts have prohibitive costs of revocation and modification, while weak smart contracts do not. This means that if a court is able to alter a contract after it has been executed with relative ease, then it will be defined as a weak smart contract. If there is some large cost to altering the contract in a way that it would not make sense for a court to do so, then the contract will be defined as strong."[34] This shows that there is not a single legal approach to smart contracts and this is one of the main difficulties also when dealing with the tokens: there is not a single definition, conditions and effects regarding smart contracts or tokens in the way we are used to with the traditional classifications and list of regulated property rights or contracts.

[31] Wang, H., Chen, K., Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, 2(1), 12.
[32] Venegas, P. (2017). Initial Coin Offering (ICO) Risk, Value and Cost in Blockchain Trustless Crypto Markets. *SSRN*
[33] Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 254-269. ACM.
[34] Raskin, M. (2016). The Law and Legality of Smart Contracts. *SSRN*

The problems associated with The DAO have shown the fragility of all software that is the imperfections in the programming code, the discovery of bugs and the susceptibility of being attacked. "Unfortunately, expressive programming languages are hard to reason about. An ambitious smart contract called The DAO suffered a theft of an estimated $50 million thanks to a litany of security problems. (Ultimately, this theft was reversed by a networkwide "hard-fork" upgrade.)"[35]

Jaccard presents a case by case approach on the legal problems of smart contracts based on the analysis of what they represent and the applicable law. It is analysed that a smart contract might represent data, a legal contract, property or a right. Very similar considerations will be made regarding the value of the tokens. Data itself most of the times does not have legal value or produce effects. However, the collection of data in a large number has a legal impact when it constitutes big data. Data can be protected by copyright laws when there is an intellectual effort of the creator of that data, which makes it a literary work. It is suggested that a classification of property right on data would be a good solution because it allows same effects as in property rights to apply. The smart contract can have data representing virtual or digital property. This might also not attribute legal effects when in most countries virtual property does not have juridical value. An example given is that ownership of a bitcoin can mean the right to access to the data that is Bitcoin. The main legal consequences are that it is very difficult to legally justify ownership of virtual or digital assets or values and the only way to protect this kind of property would be by claiming an eventual contractual right, it would then constitute an asset subject to tax law and in case of bankruptcy, it can be compensation for the creditors. Data can be considered as a legal contract because it is an imitation of contract content and the structure and functioning of a corporation. Jaccard proceeds with the analysis of smart contract representing property. If representing property, the smart contract is called a token and it may represent any physical asset/property. When representing a thing, the token smart contract can be equivalent to a Title. Property rights have *numerus clausus*, which means that it is essential to determine the qualification as property according to the law of the relevant jurisdiction because the private parties do not have the liberty to define what property is. At this point there is a major conclusion that smart contracts do not have legal effect if they do not represent property.[36]

Smart contracts have some limitations, specifically because of their lack of flexibility and integration of external factors. "Smart contracts are most efficient for contracts that can be

[35] Luu, (2016) *supra nota* 33
[36] Jaccard, G. (2018). Smart Contracts and the Role of Law. *SSRN*

reduced to simple "if-then" statements, as their terms are easy to convert to computer code and can be executed automatically."[37]

Another legal problem that can be associated with smart contracts is the assessment of the applicable law and jurisdiction. "Courts are accustomed, however, to dealing with difficult jurisdictional issues relating to contracts being formed over the Internet. Jurisdictional problems in the case of smart contracts can be avoided by the inclusion of the appropriate choice of law and jurisdiction clauses incorporated into the code by reference to the corresponding paper contract."[38]

Another issue is the understanding of programming language that is used to code a smart contract. Cuccuru raises some very interesting question for which answers can be extremely complex or difficult to agree upon: "Is computer language enforceable before a court should something go wrong in the self-execution phase? How to prove mistakes or fraud in automatic enforcement, assuming that judges cannot easily understand nor interpret code lines? Is code language actually interpretable, as it is supposed to eliminate the ambiguities of natural (legal) language, *i.e.* the very precondition of hermeneutics?"[39]

Overall, automation of the process and certainty of the action done, as proof, if there are no mistakes in the code, are very positive aspects. Nevertheless, "when the society is still experimenting with smart contract, regulators thinking how to regulate this new technology, it is dangerous to transfer from traditional contract to smart contract without any supplementary measures. It is also unrealistic to allow smart contracts to get rid of all third party intermediaries."[40]

[37] Cohn, A., West, T., Parker, C. (2017). Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids. *GEO. L. TECH. REV.*, 1, 273-284.

[38] Connor-Green, D. S. (2016). Blockchain in Healthcare Data. Intell. Prop. & Tech. LJ, 21, 93.
Couture, W. G. (2018). The Risk of Regulatory Arbitrage: A Response to Securities Regulation in Virtual Space. 74 *Wash. & Lee L. Rev. Online* 234

[39] Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology, 25(3),* 179-195.

[40] Hsiao, J. I. (2017). Smart Contract on the Blockchain-Paradigm Shift for Contract Law. *US-China L. Rev*., 14, 685.

2. IDENTIFICATION OF LEGAL ISSUES

Tokens raise legal issues because of the uncertainty of their classification. Tokens have different values and effects from case to case what makes it very difficult to establish a single concept that would describe the token.

Due to the lack of legal definitions worldwide, normally tokens are categorized as commodity/utility, security or as a currency/protocol. However, even with this standard categorization of the tokens it is sometimes difficult to consider them. It can be argued that token is not a utility because it lacks the magnitude of origin. Even though a token has characteristics of fungibility, there is only one issuer. Therefore, a token cannot be considered equivalent to gold or oil, which are examples of the commodities market.

It is also difficult to consider tokens as a currency. In fact, even altcoins with their own blockchain might not be considered currencies because there is no central authority, the price is too volatile and is not backed or guarantee its value. Tokens have a much more limited network of actual and potential users and are very often a means of payment used only within the issuer's platform.

The qualification of the token that brings the most immediate and effective legal consequences is the token as a security. This would mean that the financial authorities for supervision of economic activities would have in their scope the supervision of the issuance of tokens as any other issuance of a security. The applicability of securities legislation for an ICO would bring the same characteristics and legal effects of an IPO to the token issuing company. This means that a prospectus has to be released, the economic control over the company is done according to a different set of rules that the ICO companies normally want to avoid and limitations would be imposed on the acquirers of the tokens, which would consist mostly in accredited investors.

To be considered a security, the token has to be a document or an instrument that represent a proprietary right over an underlying asset. The United States approach on tokens as assets differs because of the Howey Test that determines the characteristics of a security as an investment that depends on the efforts of a third party.

According to the European perspective on securities, most tokens would not qualify as a security because there is no underlying asset. "Attributes of digital and physical goods can also be tracked on a distributed ledger as they move through the economy, increasing our ability to verify their integrity, provenance, manipulation and status over time. This is particularly powerful when immutable properties of a good can be reliably recorded on a blockchain, *i.e.*

when a unique, digital fingerprint can link ownership of a blockchain token to the underlying asset."[41]

2.1 Value of the Token

A token is a virtual asset. It does not have a physical dimension and consists in a data file composed by a binary code that has its value derived from natural and legal persons accepting it as a title or as means of payment. Besides that, there is a value in the fact that this data cannot be double spent since it is registered in the Blockchain.

This chapter will analyse if tokens can be considered e-money, how the value of the token is influenced and what are the rights associated to them.

It is widely accepted that cryptocurrencies in general, and therefore tokens in particular, cannot be considered e-money. This means that an ICO or token sale is not the issue of a digital representation of money; it is a contract of sale.

"A widely held view is that money should serve three distinct functions: it should be generally accepted as a medium of exchange; it should be a unit of account so that we can compare the costs of goods and services over time and between merchants; and it should be a store of value that stays stable over time."[42]

The European Union legislation on e-money establishes that electronic money means monetary value that is electronically stored as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer.[43]

The European approach is narrower than the previous general idea presented. It does not require the money in electronic format to be accepted by a large number of people but it is enough that one other person that not the issuer accepts it. A token can easily fit in this condition from the moment that a service accepts it as a mean of payment besides the platform service that normally is the same legal person that developed the ICO.

In the directive, it is used the term monetary value. Store of value, for this purpose would have the same meaning. A token is not a monetary or store of value due to its high volatility. The

[41] Catalini (2016) *supra nota* 28

[42] Peters, G., Panayi, E., Chapelle, A. (2015). Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. *SSRN*

[43] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267, 10.10.2009, p. 7–17

directive presents also the condition that the value of the issued e-money is the fact that the customer has a claim against the issuer that this digital representation of money could be used for payment transactions through the issuer. The e-money would also have to be redeemed back into money. The token from ICO is bought and in the possession of the buyer or investor or in some third party wallet. Besides that, the token usages are explained in the Whitepaper and are limited to the proposed to-be-developed products and platforms. Therefore a token does not fit in this requirement of being a claim towards the issuer for payment transactions.

Tokens have a specificity that is the fact they are traded after the end of the ICO. This has raised questions about the intent of the buyer. On one side there is the community that is formed around the product but on the other side there are the investors that speculate on the price of the token, investing in an early stage of the ICO and selling it in the exchange platforms when the price is rising. In early stages of an ICO the price can have discounts around 50% in the first week, with this rate decreasing week by week.

Conley determines the value of crypto-tokens based on four elements that can have different proportion on the valuation. He clearly states that no two tokens are exactly alike. Still, most combine four basic elements in different proportions. Those elements are transactional currency, profit share, voting control and proof-of-stake. The token price has an element of transactional currency specially when there are big sophisticated investors that hold a substantial percentage of tokens. This means that if one decides to sell all his tokens, the price will drop because there is a sudden increase of supply. A negative consequence of the token price fall is that other investors, big or small unsophisticated investors will perceive the decrease as a loss of confidence in the proposed product and platform and will probably try to sell their tokens while they are still profitable. Another price influence for tokens is the existence or not of profit share. “A major reason for the volatility seen in crypto-token prices is that there is nothing that ties down their value if they are only used as a medium of exchange.” Because token issuers want to avoid securities regulations, the lack of profit sharing leads to uncertainty about the platform value and the utility of the tokens that are dependent on a future, uncertain event, the completion of the underlying project of the ICO. In traditional companies with shares, the profit of the company is invested on the company itself, increasing its value and consequently increasing the value of shares, or it is distributed between the shareholders which is a reason for investors to hold the shares and not sell them. The other traditional characteristic of a share is the voting control. This is more commonly associated with the tokens than the profit distribution. “Token owners might get to vote over fees for some subset of services or on some of the details of the protocols. They might be allowed to approve new stakeholders, new projects wishing to joining the platform, or

even set the direction of future development. Unfortunately, when any aspect of control is separated from profit sharing, serious incentive problems are created. Voters vote in their own interests. They may choose fees or protocols that maximize their own return but harm the ecosystem as a whole." The last indicated characteristic that influences the token price are the situation when token holder assume a position of proof of stake. "Token holders are apparently being asked to pay for the privilege of contributing their efforts to maintain the platform." This can have serious influence on the price because the token holder need to have a predetermined amount of tokens to qualify as a verifier or give is input to the platform. This could work when a company has a very strong basis and is economically successful.[44]

The previous are reasons why the token price is so volatile and a risk investment. However there is a fundamental characteristic that gives the idea of token an intrinsic value that is just further increased with the development of the platform. The tokens are considered to have value because they are accepted by other natural and legal persons as means of payment. This is more a reason for value increase associated with the development of the platform than the intrinsic value of the token itself. The fact that tokens are binary data file means that they are a virtual product and can be copied. The possibility of being copied would remove all the value that a product like this could have. Blockchain technology gives the token its value of being the only code available for transaction because if someone would attempt to copy the binary data, the transaction involving the copy would never be approved and verified by the blockchain because the real token is already hashed from the previous blocks.

A main legal issue that will be further developed regarding token is the applicability of property law to the token. It is essential to assess if ownership is possible and what are the consequences if the answer is negative.

2.2 Fraud and Ponzi scheme issues

ICOs are often accused of being fraudulent platforms for raising money in a way that the entire project is only a scam or the financial return and promises constitute a Ponzi scheme.

Scams in ICOs can either come from inside or outside the organising team. When it comes from outside it is normally related with fraud and inducing investors to send their funds to a mirror site of the original ICO platform. These kinds of scams are included in the general cyber security

[44] Conley, J. P. (2017). Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings (No. 17-00008). *Vanderbilt University Department of Economics.*

related problems and will not be analysed in this thesis. When the scam comes from inside the platform the case will most likely be subject to criminal law under Division 2, Offences against All Types of Property from the Estonian Penal code, especially when there is proprietary damage for purpose of significant proprietary benefit by causing a misconception of existing facts. This is the crime of fraud[45] and might be the case of ICO scams.

"There exist altcoin developers who have conducted outright scams via Initial Coin Offerings, with the creators disappearing after crowdsourcing bitcoins from the community. (…) Meanwhile, some altcoins have also been created with illegitimate aims such as stealing users' personal details or bitcoin private keys through the installation of malware and trojans onto altcoin wallets."[46]

Ponzi schemes are also an issue in ICOs. Pyramid schemes in the sense of bringing more investors to benefit the earnings of the inviter are non-existing. The Ponzi schemes in the classical sense also do not entirely apply, as a scheme for investing money with clear promise of unrealistic profits. The Ponzi scheme possibility in ICOs is in a fine line that separates a scheme from an elaborate marketing strategy. "Still, it is foreseeable that, as Ethereum consolidates its position as a platform for smart contracts and as a cryptocurrency, criminals will exploit it to host their scams. Besides the growth of traditional Ponzi schemes accepting ether, we expect a second wave of Ponzi schemes, but very likely they will be less recognizable as such than the ones collected in this survey. For instance, they could mix multi-level marketing, token sales, and games, to realize complex smart contracts, which would be very hard to correctly classify as Ponzi schemes or legit investments"[47]

The Ponzi schemes are a real threat to the ICO market because the existence of few can lead to the lack of trust from investors in the global token issuing market. Just by studying the Whitepaper and searching about the team might not be enough to clearly conclude for a Ponzi scheme.

The main reasons that make Ponzi schemes appealing for criminals in an ICO are related with the technological advancements that are possible, particularly by using blockchain and smart contracts technology. It is easy to be anonymous in the blockchain and management of smart contracts and therefore move the funds without anyone's authorization. This happens because cryptocurrencies and token wallets are identified by a cryptographic public key and not by

[45] Karistusseadustik, RT I 2001, 61, 364, § 209

[46] Elendner, H., Trimborn, S., Ong, B., Lee, T. M. (2016). The cross-section of crypto-currencies as financial assets: an overview (No. 2016-038). *SFB 649 Discussion Paper*.

[47] Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. (2017). Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. *arXiv preprint arXiv:1703.03779*.

names. Another legal issue rises here, should crypto and blockchain related businesses be oblige to perform KYC (Know Your Customer) procedures and in which conditions?

Besides the anonymity aspects there is also a problem with legal enforcement. Since there are no central authorities backing blockchain or the correct application of smart contracts it turns out very complex for a court to have the necessary elements of proof to decide in a case like this. It is important to note that there hasn't been any relevant judicial case in Europe related with these issues.

Blockchain has a positive and negative side in relation with fraud prevention. "Blockchain systems are very effective in preventing objective information fraud, such as loan application fraud, where fraudulent information is fact-based. However, for subjective information fraud, such as rating fraud, where the fraudulent information is not easily verified, blockchain systems are not effective in all scenarios."[48] A way that ICOs try to combat fraud within the platform is by attributing reputation tokens functionality. It means that tokens can be earned by activity and have to be collected to become a trustworthy member of the platform.

Finally, "investors may gain a false sense of trustworthiness from the fact that the code of smart contracts is public and immutable, and their execution is automatically enforced. This may lead investors to believe that the owner cannot take advantage of their money, that the scheme would run forever, and that they have a fair probability of gaining the declared interests."[49]

2.3 Are ICOs regulated?

The first part of the research hypothesis states that ICOs are not regulated. To determine the truthfulness of this statement it is necessary to know if the existing laws are applicable to ICOs. The difficulty to answer to this question comes from the fact that the tokens do not attribute the same rights even though they are all qualified as tokens. This makes it complex to create a specific legislation that would apply to tokens in general.

Adhami shows the rights attached to tokens. "(In) 68.0% of the cases ICO contributors are rewarded through an exclusive access to the services offered by the platform project. Tokens may be used as a currency in commercial transactions in 20.9% of the cases (assessment based mostly on the project's intention to create a new blockchain instead of relying on an existing one). Governance rights are granted in 24.9% of the ICOs while profit rights are offered in

[48] Cai, Y., Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation, 2(1),* 20.

[49] Bartoletti (2017) *supra nota* 47

26.1% of the cases. It is important to notice that each token may assume multiple roles and grant different rights to the holders and this adds to the difficulty of pinpointing the type of financial security that may be compared with."[50]

The token that gives the right to access to services is a right to claim for services in the future since the platform is normally not completed yet and there are no certainties about which other services will join the platform. This right raises the biggest question regarding tax law. The main issue is the qualification of the token issuance as part of the services to be offered, meaning if this consists in a supply of services or if there is a supply of goods for VAT taxation purposes.[51]

When the token gives rights of governance and voting to the token holders, the main uncertainty is the application of the regulations that apply to Initial Public Offerings and if the token can be qualified as a security. For that analysis, it will be considered the Securities Market Act. The tokens do not always give governance and voting rights cumulatively to the investors, therefore it has to be clear whether one of those rights by itself allows the comparison with securities.

Finally, when the token represents currency in commercial transactions, as seen before, do not follow under the definition of currency or e-money. Here the main regulatory concerns have to do mainly with the origin of funds which might be regulated by the Anti-money laundering legislation.[52]

The core legal analysis of tokens includes also considerations on classical civil law, both property law and contract law.

The property act will determine the ownership conditions for tokens and their possible qualification as securities. The Law of Obligations Act will determine if a Token Sale or ICO is legally regulated as to the definition[53], the format[54], the validity[55] of a contract and the requirements to be a contract of sale[56].

[50] Adhami (2017) *supra nota* 3

[51] Käibemaksuseadus, RT I 2003, 82, 554, § 1

[52] Rahapesu ja terrorismi rahastamise tõkestamise seadus, RT I, 17.11.2017, 2

[53] Võlaõigusseadus, RT I 2001, 81, 487, § 8. (Definition of contract (1) A contract is a transaction between two or more persons (parties) by which one party undertakes or the parties undertake to perform an act or omission.)

[54] Võlaõigusseadus, RT I 2001, 81, 487, § 11. (Format of contract (1) A contract may be entered into orally, in writing or in any other form if no required format is provided for the contract by law.)

[55] Võlaõigusseadus, RT I 2001, 81, 487, § 12. (Validity of contract (1) The validity of a contract is not affected by the fact that, at the time of entry into the contract, performance of the contract was impossible or one of the parties did not have the right to dispose of the thing or right which is the object of the contract.)

[56] Võlaõigusseadus, RT I 2001, 81, 487, § 208. (Definition of contract of sale (1) By a contract of sale of a thing, a seller undertakes to deliver an existing thing, a thing to be manufactured or produced or a thing to be acquired in the future by the seller to the purchaser and to allow the transfer of ownership to the purchaser, and the purchaser undertakes to pay the purchase price for the thing to the seller in cash and to take delivery of the thing.)

2.4 Overall Risks

The European Securities and Markets Authority have issued a statement that has been followed by the European national financial authorities and that indicates the specific areas and problems that make ICO investments very risky. Four main factors are identified in the statement.

First, an ICO can be happening in an unregulated space, vulnerable to fraud or illicit activities. Due to this fact, there are clear suspicions that a token offering event can be used by some issuers for purposes of money laundering. The anonymity and lack of regulatory supervision contribute for that risk. If the ICO is out of the scope of EU and national legislation, then the investors and buyers are not protected by consumer rights or the right to information for example.

Secondly, there is a high risk of losing all of the invested capital. The fact that ICOs are a way of crowdfunding and the product or service proposed is not yet completed because of needed funds. This leads to the risk that the product or service will never be fully developed, because of need for more funds or due to disagreements between the founders. Highly associated with this aspect and condition to lose the invested capital is the devaluation of the token in the market or the non-acceptance of tokens in the exchanges at all.

Another risk presented in the statement is the inadequate information. The Whitepapers are all different in the sense that there is no mandatory structure applicable. It is pointed out that many times investors cannot assess the entirety of the risks just by reading this document that is most cases in not checked by a trusted third party; it is incomplete and can be misleading.

The final warning is related with the flaws in the technology. ICOs are based on blockchain technology which is a very recent technology that has not been tested in larger scale. Technology flaws related with cybersecurity, for example hacking and fraud, and cryptography, for example loss of private keys, present serious risks for the loss of the capital invested by the token holders.[57]

Xu has identified the possible cybersecurity threats to the blockchain technology: the 51% attack, account takeover, digital identity theft and hacking. In a possible 51% attack "the dominant node can outpace all other nodes, manipulate the blockchain, insert fraudulent transactions, double-spend funds, or even steal asset from others." Nowadays this is not realistic because the miners are organized in groups and the biggest has around 20% of computational power. Besides that, the cost would be considerably high and there are no incentives to do so. The identity theft is the most critical of the risks. "If one's private key is acquired or stolen, no

[57] ESMA50-157-829, 13 November 2017

third party can recover it."[58] This means that the access to the wallet is not possible anymore. In an identity theft case, the control of a private key of other person allows the crypto currency value to be transfer to a different address and since the private keys are generated specifically for each transaction, the person that was stolen cannot recover the crypto funds; the transaction is irreversible.

The next chapter consists on the legal analysis of the problems raised and presents the reasoning for concluding the thesis hypothesis.

[58] Xu, J. J. (2016) Are blockchains immune to all malicious attacks? *Financial Innovation* 2 (1), 25

3. LEGAL FRAMEWORK

Estonian legislation has one act that specifically regulates virtual currency activities and has some definitions. Virtual currency means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or a payment transaction.[59] This definition is wide enough that almost any token could be included in its scope. The division previously presented between currency tokens, security tokens and utility tokens are qualifications of tokens that do not find legal grounds as a definition by itself but are concepts that have been used to differentiate the legal effects and applicable rules to them. According to this definition, a token is virtual currency when it is transferable, preservable or tradable. Tokens are always transferable in the sense that they can be send from one wallet to another wallet. Tokens are also preservable by cryptographic means. The tokens are protected by private keys that, in principle, only the token holder has knowledge of. The tokens are tradable from the moment a crypto currency exchange accepts to trade them. It is very usual that tokens are tradable, even though it only happens after the ICO is concluded.

Secondly tokens are virtual currencies when natural or legal persons accept them as a payment instrument. This is the most important part of the definition for ICOs because when the token issued is only accepted by one person, the platform that will be developed with the funds raised, then the token is not a virtual currency because to be so it has to be accepted as a payment instrument by two or more persons. The requirement that the token would not be a legal tender is more of a description then a requirement.

Only two kinds of services are in the scope of the anti-money laundering act: providers of service of exchanging a virtual currency against a fiat currency and providers of virtual currency wallet service.

A possible definition for exchanges is the provision of "services to buy and sell cryptocurrencies and other digital assets for national currencies and other cryptocurrencies. Exchanges play an essential role in the cryptocurrency economy by offering a marketplace for trading, liquidity, and price discovery."[60]

On the other side, a wallet "is a software program that is used to securely store, send and receive cryptocurrencies through the management of private and public cryptographic keys. Wallets also

[59] Rahapesu ja terrorismi rahastamise tõkestamise seadus, RT I, 17.11.2017, 2, §3 9)

[60] Hileman, G., Rauchs, M. (2017). Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*.

provide a user interface to track the balance of cryptocurrency holdings and automate certain functions, such as estimating what fee to pay to achieve a desired transaction confirmation time."[61]

An essential provision in the law is the reference to private keys. In a wallet service provider, keys are generated for customers or customers' encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies.[62] The private key allows the token or virtual currency holder to encrypt the data file in order to send it to the wallet address of the recipient that has the public key.

This Cryptocurrency benchmark study presents interesting number about third parties holding private keys. It is more often that exchange platforms hold private keys of their customers. This happens in 73% of the exchanges. On the other hand, only 15% of wallets hold private keys, while 12% ask the customers whether they prefer to keep control of the private key or trust it to the wallet service provider.

The providers of payment services are not directly included under the anti-money laundering regulation in Estonia because to provide these services, the companies open virtual wallets for their clients in order to manage the transaction just like a bank. This way, companies are in control of the private keys that are necessary to control the funds and make the transaction requests.

When a company holds private keys, it means that the wallet is a custodial wallet, in opposition with software wallets that are provided by companies that do not control the wallet's activity and therefore cannot access the funds. "Compared to traditional financial services, custodial wallet providers that provide VC wallets to their users can be seen as financial institutions that provide bank or payment accounts to their customers. When such fund transfers are done between financial institutions, this is regulated by the Fund Transfer Regulation. However, the same transfer in VCs – trough VC wallets held by VC wallet providers – is unregulated."[63]

Even though the European Union is trying to harmonize anti money laundering regulation with the 5th AML directive, it will still be possible for companies to go forum shopping for the best jurisdiction.

"The decentralised nature of the currency means that there is limited effect any single jurisdiction can have on the operation currency itself, and the focus is on companies providing services in the field. Given the borderless nature of Bitcoin, however, it is difficult to see how

[61] *Ibid.*
[62] Rahapesu ja terrorismi rahastamise tõkestamise seadus, RT I, 17.11.2017, §3 10)
[63] Commission Staff Working Document Impact Assessment, Accompanying the document Proposal for a Directive of the European Parliament and the Council, SWD(2016) 223 final

regulators can prevent companies taking advantage of regulatory arbitrage, by setting up in jurisdictions with less restrictions."[64]

However, the provision of services within the European space can be limited to those companies that choose a jurisdiction outside European Union because they would not be able to provide services for nationals of EU countries without an appropriate license.

3.1 Existing legal framework for ICOs

It is not possible to say exactly what the law applicable to ICOs are. Since each token has different rights associated and represent different claims towards the issuing company and no law was developed in the European context to specifically regulate ICOs, it is only possible to make an assessment case by case.

"Depending upon how the promise is expressed, and upon the structure of the ICO and governing jurisdiction, a contract or partnership (or possibly even a trust) relationship may possibly arise. The important point is that issuing the commitment to the public and accepting the consideration on this basis is legally relevant conduct. The people who make those promises are bound by their commitments; and breach will result in liability."[65]

In this chapter, it will be presented the range of legislation that might be applicable, taking into consideration what the tokens that have been issued normally represent to the buyers.

In Estonia there is no Act regulating crowdfunding or a specific legal provision that establishes the proceedings and legal effects of the crowdfunding process to which an ICO could be comparable.

In the United States there is the JOBS act[66] (Jumpstart Our Business Startups Act) also known as the Crowdfunding Act that opens the possibility for unaccredited investors, or the general public, to invest in the fund raising by obtaining shares or similar rights with special rules for the issuance of securities, by making the whole procedure simpler and more accessible.

3.1.1 Civil Law

With cryptocurrencies, there is typically no issuer to which a claim can be made against. On the same note, however, a cryptocurrency cannot be said to typically represent a tangible asset. It is,

[64] Peters (2015) *supra nota* 42

[65] Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L. (2018). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *SSRN*

[66] Congress Bill, H. R. 3606 (112th): Jumpstart Our Business Startups

therefore, unclear which set of rules should have precedence, or if all the rules are equally applicable.

In the US, most case law have treated bitcoin as money for securities law purposes with many of the general requirements for securities, including investment contracts, and commodities futures being applicable. However, that is not to say that any cryptocurrency would receive similar treatment, as the individual cryptocurrency may differ materially from bitcoin. Indeed, the IRS treats bitcoin, and likely cryptocurrencies with similar features, as property for tax law purposes. To this end, it would seem that both the SEC and CFTC have jurisdiction with regard to ICOs, and it is unclear which set of rules should have precedence, or if all rules are equally applicable. Many further contradictions may arise in the future, and parties must take legal advice in all specific cases.[67]

Cryptocurrencies present this big challenge resulting from their nature that is the difficulty to qualify them as object of ownership, which consequently influences the applicability of the characteristic performances of sale contracts and general property law. "As a matter of law, the investor probably does not own any bitcoins, at least not in the sense of having title to personal property corresponding directly to bitcoins. What the investor has is simply a contract right against the operator of the website-what was classically, at common law, called a chose (*i.e.*, thing) in action. This sort of right is meaningfully different from having possession of personal property. For one thing, it is subject to a risk of default-if, for example, the website becomes insolvent"[68]

The Estonian Law presents some civil challenges for the qualification of the legal effects arising from the tokens issued after the initial coin offering. The main issue is the qualification of tokens as property or not. Tokens are a digital asset because they consist in binary data format and have associated the right to be used. According to the General Part of the Civil Code Act, a thing is a corporal object.[69] Tokens are not things because they are not corporal or, in other words, physical objects. Nevertheless, tokens are an object for property law. Objects are things, rights, and other benefits.[70] Tokens can be considered either a right or a benefit, depending on the terms of use, therefore, tokens are objects. The main problem is that ownership is full legal control by a

[67] Enyi, J., Le, N. (2017). The Legal Nature of Cryptocurrencies in the US and the Applicable Rules. *SSNR*
[68] Bayern, S. (2014). Dynamic common law and technological change: the classification of Bitcoin. Wash. & Lee L. Rev. Online, 71, 22.
[69] Tsiviilseadustiku üldosa seadus, RT 2002, 35, 216, §49. (1)
[70] Tsiviilseadustiku üldosa seadus, RT 2002, 35, 216, §48.

person over a thing[71] and ownership is created only in the cases provided by law[72]. This way, in general tokens cannot be owned according with this approach.

Different acts in Estonian law present different definitions of property. For purposes of the Money Laundering and Terrorist Financing Prevention Act, property means any object as well as the right of ownership of such object or a document certifying the rights related to the object, including an electronic document, and the benefit received from such object[73]. This definition could apply to tokens because it refers to an object.

The Income Tax Act has an extensive definition of property by presenting a definition based in examples: Income tax is charged on gains from the sale or exchange of any transferable and monetarily appraisable objects, including real or movable property, securities, registered shares, contributions made to a general or limited partnership or an association, units of investment funds, rights of claim, rights of pre-emption, rights of superficies, usufructs, personal rights of use, rights of commercial lessees, redemption obligations, mortgages, commercial pledges, registered securities over movables, or other restricted real rights, or the ranking thereof, or other proprietary rights (hereinafter property). Tokens can also fit in this definition because they can be considered transferable and monetarily appraisable objects, rights of claim.

The main problem for the token holders are the contracts from the Law of Obligations Act that might not receive protection in cases when credit, loans or collateral transactions are made with tokens or virtual currencies in general. In a contract of sale the seller undertakes to deliver a thing there is a transfer of ownership to the purchaser done in exchange for the price[74]. Here is used the concept of thing but as opposite to credit or loans, there is a norm of equivalence of effects that states that the provisions of this Act concerning the sale of things apply to the sale of rights and other objects.[75] This is can be understood as ownership is created only in the cases provided by law. Even though a token cannot be owned by itself, it can be the object of a sale contract.

[71] Asjaõigusseadus, RT I 1993, 39, 590, §68. (1) LPA
[72] Asjaõigusseadus, RT I 1993, 39, 590, §68. (3) LPA
[73] Rahapesu ja terrorismi rahastamise tõkestamise seadus, RT I, 17.11.2017, §3. 2)
[74] Võlaõigusseadus, RT I 2001, 81, 487, §208. (1)
[75] Võlaõigusseadus, RT I 2001, 81, 487, §208. (3)

3.1.2 Financial Law

If a token is considered to be a security for purposes of the Securities Market Act,[76] then the registration requirements and the issuance of a prospectus are mandatory under the risk of facing criminal proceedings for non-compliance.

"At its heart, ICOs have formed as an alternative way of raising capital to the Initial Public Offer (IPO) which is a heavily regulated process which serves as a distinct barrier to many companies. This has led to competing arguments: that IPOs shouldn't be as complicated, therefore ICOs help to balance out regulations; or that IPOs are a barrier for a reason, and that ICOs can only be seen as an abuse of the system. (…) ICOs embrace some of the elements of anarcho-capitalism, which perturbs regulators because the ICOs feel they are outside the regulators' remits."[77]

From the European and Estonian perspective, the determination of a token as security is narrower than in the United States because there is a list of financial instruments that are securities and the main aspect to consider when assessing the legal qualifications of a token is if it gives governance rights and/or profit rights to the token holder. In the United States, due to the interpretation that is currently done by the SEC and the courts using the Howey Test, the conditions that the buyer of the token is making an investment for profits depending on the activities and efforts of a third party might seem easier to interpret but is also open to wider and more variable understanding.

On a further financial law application interpretation, "Currency Tokens are characterized by the fact that one token reflects a right in another currency, either crypto or otherwise. For instance, 1 Token could reflect the value of 1 USD, 1 EUR or 1 ETH. The ICO merely translates a currency into bits and bytes. Around the globe, regulators have implemented rules for payment services. Some regulators have held that those rules could apply to cryptocurrencies."[78]

One condition that would make the token to be a security is related with investment funds. The funds raised might be considered assets in an investment pool if those assets are used to further investments. This situation is analysed from the business model of the platform behind the ICO and should be found in the Whitepaper.

"Under the European Alternative Investment Management Framework (…) the central concept that determines the AIFMD's scope is the alternative investment fund (AIF). The AIFMD uses the term 'alternative' in a somewhat misleading way to include all collective investment undertakings that are not governed by the UCITS framework and raise capital from a number of

[76] Väärtpaberituru seadus, RT I 2001, 89, 532, §2
[77] Flood, J., Robb, L. (2017). Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings. *SSRN*
[78] Zetzsche (2018) *supra nota* 65

investors, with a view to investing it in accordance with a defined investment policy for the benefit of those investors. While equity token ICOs are likely to meet those criteria, the determination of whether there is a discretionary third party fund management and a defined investment policy must be assessed on a case-by-case basis."[79]

Hacker et al. present three formal requirements to determine the applicability of the initial public offering rules from the EU securities regulation regarding prospectus to the initial coin offerings. The formal characteristics are transferability, standardization and negotiability on capital markets. The transferability is clear from the definition from Art. 2(a) of the Prospectus Directive: securities mean transferable securities as defined in the Directive 93/22/EEC. That definition says that transferable securities are shares in companies and other securities equivalent to shares in companies, bonds and other forms of securitized debt which are negotiable on the capital market and any other securities normally dealt in giving the right to acquire any such transferable securities by subscription or exchange or giving rise to a cash settlement with the express exclusion of instruments of payment. Tokens are transferable on secondary markets, the exchange platforms which would meet the requirement of transferability but the tokens that are qualified as instrument of payment would be automatically excluded from the definition of securities. "For those issuers attempting to circumvent EU securities regulation, this presents a technical workaround that could be economically attractive in financing schemes that seek to establish extremely stable and long-lasting relationships between product users. Such a scheme is rare, but not unheard of. For example, the tokens issued in one of the largest ICOs so far, the EOS token sale, "will become fixed (non-transferable) on the Ethereum blockchain within 23 hours after the end of the final EOS Token distribution period which will occur on June 1, 2018." Once they are fixed, EOS tokens therefore likely are not securities." The requirement of negotiability means the practical possibility of the token's ownership to be transferred. It is not connected with the possibility to agree on the price or to negotiate the sale of tokens. "The European Commission has offered guidance concerning the interpretation of negotiability. According to their Q&A document, "if the securities in question are of a kind that is capable of being traded on a regulated market or MTF [multilateral trading facility], this will be a conclusive indication that they are transferable securities". Regulated markets and multilateral trading facilities are technical terms defined under the MiFID regime, to which Art. 2(1)(j) of the Prospectus Directive refers. The former includes only authorized marketplaces for financial instruments functioning in accordance with Title III of MiFID, for example stock exchanges.

[79] Zetzsche (2018) *supra nota* 65

Similarly, MTFs are marketplaces for financial instruments characterized by bringing buying and selling interests together." Finally, standardization is perhaps the most interesting point when analysing the applicability of the securities legislation to the initial coin offerings. Standardization means that the set of securities would be the ones present in the law and that tokens would fit in the definition of one class of securities. The tokens are not sufficiently standardized to be considered a security for purposes of MIFID that tells that 'transferable securities' means those classes of securities which are negotiable on the capital market. This definition states the existence of classes of securities. However, it is also states the existence of "other securities equivalent to shares in companies". "The issued units must share a number of characteristics so that they can be considered a class. Most importantly, the claims represented by the units must not be individually negotiated with investors. Second, it is argued that, from a functional perspective, non-standardized issued units cannot be easily traded on a capital market as standardization is necessary to reduce search costs for investors. One popular definition therefore holds that units must be defined by common characteristics so that it is sufficient to refer to the type and number of units to trade them."[80]

There is an indication what similar rights to shares can be from a Commission working paper: "The pre and post trade transparency requirements currently only apply to shares admitted to trading on a regulated market. A number of instruments that are similar to shares are outside the scope of MiFID transparency requirements. These instruments from an economic point of view are equivalent to shares and share many characteristics with the equity markets, including liquidity, types of investors, etc. Hence most market participants and regulators are of the view that it would be beneficial to subject these markets to transparency requirements."[81] Those instruments that are similar to shares are further exemplified in the comments with the reference to depositary receipts, exchange traded funds and certificates issued by companies. Tokens do not fit in the scope of similar rights to shares.

It can be strongly argued that tokens are a very similar instrument to payment instruments. Since it is so difficult to consider the so called utility tokens as securities or prepayment of services, it can be considered that those tokens are similar to payment instruments.

"Similar conclusions could be reached for bitcoin spin-offs such as bitcoin gold or bitcoin cash that are primarily designed for payment purposes. The CJEU also explicitly held that bitcoin is

[80] Hacker, P., Thomale, C. (2017). Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. *SSRN*

[81] Commission Staff Working Paper Impact Assessment Accompanying the document Proposal for a Directive Of The European Parliament And Of The Council on Markets in financial instruments [Recast] and the Proposal for a Regulation Of The European Parliament And Of The Council on Markets in financial instruments {COM(2011) 656 final} {SEC(2011) 1227 final}

neither a security conferring a property right nor a security of a comparable nature. However, the decision concerned the VAT treatment of bitcoins, not securities regulation; the list of securities in Art. 135(1)(f) VAT Directive, which the CJEU interpreted, differs from the one in MiFID. It lacks, for example, the reference to equivalents of shares in other entities, and to other forms of securitized debt. Therefore, some uncertainty persists as to whether the court would reach a similar conclusion under EU securities regulation."[82]

One of the classes of securities that have a big role outside the regulated market is the derivatives. Most tokens can be considered derivatives when they are an instrument that represents a patrimonial right over an underlying asset. The asset does not have to be a physical thing, it can also be a right to use. These tokens are traded in the secondary market and can potentially fall under EMIR regulation[83] on OTC derivatives, central counterparties and trade repositories and qualify for the obligation of clearing, reporting and risk mitigation of OTC derivatives. "If the Emir clearing obligation were applied to blockchain derivatives, the advantages of the technology - speed, cost, transparency - would be immediately cancelled out. If blockchain derivatives are somehow considered out of the scope of the Emir clearing obligation, it is entirely possible that a significant portion of the market would move to blockchain transactions and the regulation itself would become redundant."[84]

"It is crucial that any discussion about FinTech companies and activities, and the possible challenges they may pose to financial stability, does not lose sight of the heterogeneity of the industry in question and acknowledges the need to look beyond the diversity and interconnected nature of these services."[85]

3.1.3. Consumers Rights

ICOs are being constantly characterized as very risky investments by different governmental authorities and analysts. The main legal problem that it raises is the consumer protection regarding the information given in the Whitepapers and the marketing that is made as well what liabilities can be charged to the ICO launching company and what warranties the buyer has.

The ICO event can be considered as a distance contract because under the Consumer directive, any contract concluded between the trader and the consumer under an organised distance sales or

[82] Hacker (2017) *supra nota* 79

[83] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ L 201, 27.7.2012, p. 1–59

[84] Leonard, C. (2016). Blocking the Blockchain. *Int'l Fin. L. Rev.*, *35*, 58.

[85] Minto, A., Voelkerling, M., & Wulff, M. (2017). Separating apples from oranges: identifying threats to financial stability originating from FinTech. *Capital Markets Law Journal*, 12(4), 428-465.

service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded.[86] This means that the consumers would have the right to withdrawal from the contract without giving any reason or incurring in any costs. This is a big risk for companies and definitely a liability that they try to avoid through their terms and conditions and token sale agreements.

"Further, if ICO participants are consumers, private international law will limit the discretion with which ICO backers can determine the applicable law. Under most private international law regimes, contracts between commercial entities and consumers are subject to the consumer protection laws in force in the consumer's country of residence, or at least the rights granted in that jurisdiction are upheld. (…) Thus, as a common denominator, since ICOs are offers to the public (*i.e.* consumers) by some commercial enterprise, where a consideration is required in order to participate, the general consumer protection legislation of the relevant country will apply."[87]

Zetzsche also makes very interesting consideration about the fact of an ICO being or not conducting a commercial activity, which will also be relevant for purposes of tax law. The question that is difficult to answer in this aspect is if the sale of the token in return for a promise of a future action that might or might not happen, depending on the development of the platform, is enough to consider that there is a business relationship or commercial activity. This is a specially pertinent is a situation when the company issuing the token is not a private limited company but rather a foundation, non-profit organization or a trust, in the Anglo-American system of law.

The token buyers often face similar risks independently of which token they are considering to acquire. Besides the obvious, and probably major, risk of legal uncertainty in relation to the legal effects and protection of the consumers towards an ICO, Kaal et al. identify the following consumer risks: the intangibility of the product or the non-existence of a product at all, the early liquidity despite little information, the inexistence of liquidity preference and the option of developing an open source code for the platform. Tokens normally do not have any tangible product associated with the sale and only a promise of future product is given to investors. Because the ICO market is still starting, only few companies could deliver the promised product.

[86] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88

[87] Zetzsche (2018) *supra nota* 65

This is a factor that might raise trust issues. Regarding the liquidity issue, “unlike any prior financing vehicles, ICOs provide the highest possible liquidity for investors. (…) ICO investors typically invest - and the token exchange - on very limited information which increases volatility of the tokens and the entire cryptocurrency market.” [88] The fact that the innovations and promised product are done by using open source code option of licensing allows improvement of the code but at the same time it can be copied and used by anyone. Finally, in the case of the ICO projected business model being terminated or ran out of funds and the company is declared bankrupt, the tokens do not give any liquidity preference to their holders.

3.1.4 Anonymity (AML and KYC)

The Anti-money laundering legal considerations and requirement for conducting know your customer diligences was already referred in the beginning of this chapter as applicable to virtual currencies. However, the tokens are not necessarily virtual currencies within the meaning of the definition in the law. Virtual currencies need to be accepted by legal or natural persons. Sometimes tokens are accepted as means of payment by only one legal person which is the developer of the platform.

In abstract, tokens have a big risk of being used for money laundering because their holders can be anonymous and it is very difficult to know the origin of the tokens since they can be tradable for other cryptocurrencies without involving fiat currency trade. The multiplicity of addresses and possibility to make multiple transactions that would make it very difficult to track the origin of the funds are characteristics that enhance the risk. “The owners themselves are not identified by name on the ledger, but rather by a set of letters and numbers representing their public cryptocurrency address. Anyone can freely create as many wallets as he or she desires, at practically zero cost, without providing any identifying information. This relatively high level of anonymity makes it difficult for regulators to identify individuals who use the protocol for illicit value transfers. It should be noted, however, that most cryptocurrencies are not completely anonymous, but rather are pseudonymous. For example, if the identity of some wallet owners is known, it is theoretically possible to use these known nodes in the system to build a "transaction graph" that tracks each particular cryptocurrency.”[89] However this theoretically possible way to build a transaction graph would require high volume of resources, time and money which might

[88] Kaal, W., Dell'Erba, M. (2017). Initial Coin Offerings: Emerging Practices, Risk Factors, and Red Flags. *SSRN*
[89] Marian, O. (2015). A conceptual framework for the regulation of cryptocurrencies. *U. Chi. L. Rev. Dialogue, 82*, 53.

affect the efficiency of controlling tokens and virtual currencies in the course of investigation. This is why it is recommendable that AML rules would apply as preventive measures.

AML rules should be enforced against the trade market and payment service providers. "Some services used for third party payment or trade require identifying information beyond the public wallet key. However, the exchanges do not have much incentive to reveal user information unless forced by the IRS. Generally speaking, the group of retailers that have begun accepting Bitcoin could also reduce anonymity of public keys should customer privacy be breached, but even with transactions tying users' personal information to public keys anonymity can be kept intact through the use of multiple keys."[90] By licensing exchange platforms and wallet private key holders (payment service providers included), the law is providing preventive measures for the prevention of money laundering practices.

It is a challenge for the blockchain technology to allow the correct performance of KYC combined with the anonymity characteristic and the respect for the General Data Protection Regulation. There are however some technical solutions already in place. "Corda and the Ethereum blockchain have similarities, but the former is – in its essence – the combination of a distributed database and a Java Virtual Machine, enabling parties on the network to execute bilateral transactions involving sensitive information that is not revealed to the public. These kinds of solutions could offer new approaches to providing distributed but private document exchange between customers and financial institutions that include storage possibilities for larger documents."[91]

3.1.5 Tax law

The taxation of tokens is a difficult area of law because the states have a special power in the enforcement of taxation because interpretation can be applied retroactively and the interests charged on legal and natural persons that are infringing their tax obligations are very high.

There is no clear obligation on taxation of virtual currencies. In fact, the exchange of virtual currencies is vat exempt according to the *Hedqvist* case[92] from the ECJ. However, tokens are not virtual currencies in the sense that they bring rights attached.

[90] Pittman, A. (2016). The Evolution of Giving: Considerations for Regulation of Cryptocurrency Donation Deducations. *Duke L. & Tech. Rev., 14*, 48.

[91] Moyano, J. P., Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering, 59(6)*, 411-423.

[92] Judgment of the Court (Fifth Chamber) of 22 October 2015, *Skatteverket v David Hedqvist, Case C-264/14*

"Some tokens are sold with no power in the holder to compel the seller to repurchase the tokens and with no sharing of profits. Thus, they may be viewed as prepayments for future services. In other words, all the proceeds of the ICO could be taxable income."[93]

This is a situation where it is not certain if the token is a prepayment of future hypothetical services or an exchange of virtual currencies.

For the token to be considered the prepayment of a future service, it needs to be considered a voucher for tax purposes. However, in the *Hedqvist* case it is very clearly stated that "it must be recalled that a supply of services is effected 'for consideration' within the meaning of Article 2(1)(c) of the VAT Directive, and is therefore subject to VAT, only if there is a direct link between the services supplied and the consideration received by the taxable person (judgments in *Loyalty Management UK and Baxi Group, C-53/09 and C-55/09, EU:C:2010:590*, paragraph 51 and the case-law cited, and *Serebryannay vek, C-283/12, EU:C:2013:599,* paragraph 37".

It seems difficult to establish the direct link between the provider and the services that is normally not the same company that conducts the ICO and even if it is, there are no services ready yet because they are not even developed. Besides that, the token is built in a way that ideally would turn itself to be a virtual currency. If the fees are low and it offers comparative advantages to other tokens, that token issued will start to be accepted by other persons as means of payment, which can be possible immediately upon their listing in an exchange platform. It would probably be more reasonable to treat an ICO as an exchange of virtual currencies. The token is the object of an agreement between the parties that makes it the accepted means of payment for a future transaction. The buyers are not acquiring tokens with the perspective to use the services that the Whitepaper says that it can be used.

In respect to income tax, tokens are likely to be in that scope because in most countries they are considered as digital assets and are or have a similar statute to property.

"Some tokens also allow a holder to demand repurchase of the token by the issuer. Although the amounts issuers receive for these tokens may have to be refunded, those amounts are received by their issuers under a "claim of right." Under that doctrine, amounts received by a taxpayer, over whom the taxpayer has full dominion, can be included in the taxpayer's income."[94]

Income tax is determined by the individual or by the company accordingly with the respective tax residence.

[93] Shakow, D. J. (2017). The Tax Treatment of Tokens: What Does It Betoken?. *SSRN*
[94] *Ibid.*

3.2 Possible approach for regulation

There is a strong need for regulation because businesses using virtual currencies and start-ups funding themselves is growing at a fast pace. Bitcoin has seen a huge growth in popularity and there is an economic and social perspective that the legislator has to take into consideration. The spreading of influence of virtual currencies and the associated fear of missing out that has driven so many people to acquire the most different classes of digital assets should be enough indicators that crypto transactions are legally relevant. This is not anymore a small effect invention.

"As every cryptocurrency is managed in an individual "Wallet" of the owner the provider should aim for a solid compliance program including compliance policies, client identification forms, due diligence and reporting as it is the case in traditional banking activities. (…) A lot of legitimate new clients may think that if the cryptocurrencies are asking for such regulations they are so significant that I should also start using them. And with an increased market share any regulations are also affecting the whole economy."[95]

In the next and final chapter it will be shown the current approaches and existing or drafted legislations as well as the possible solutions that the legislators can follow. In the European Union it can be more difficult for a country alone to take the necessary steps because law like the Value Added Tax or Financial Market legislations are developed in a supra national level. Also due to the global effect of cryptocurrencies, it can be better to take those core measures at a supra national level.

"One approach for regulators would be to completely exclude Bitcoin-economy transactions from regulation, just as forwards and private investment funds are excluded from the CEA and the Investment Company Act, respectively. Another approach would be to exempt Bitcoin-universe transactions from most applicable regulation, while still imposing requirements and prohibitions relating to recordkeeping, reporting, and fraud. The latter approach would be similar to how private company securities, commodity trade options, and certain over-the-counter securities markets are regulated."[96]

Bitcoin and the crypto businesses that appeared after, including in a large scale the business model of ICOs include a very interesting sense of in-built justice and consequent enforcement. "It is necessary to assess whether the Bitcoin system has autonomous jurisdiction to enforce. This is probably the most innovative aspect of Bitcoin: in systems such as escrow, the delivery of

[95] Breu, S., Seitz, T. G. (2017). Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society. *SSRN*

[96] Brito, J., Shadab, H., Castillo, A. (2014). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. *Colum. Sci. & Tech. L. Rev., 16*, 144.

the decision coincides with its coercive enforcement. Bitcoin adjudicators decide the dispute by simply directing the flow of money to the prevailing party: hence, the possibility of non-compliance is automatically ruled out."[97]

Very often, the tokens holders that have enough reputation tokens are given the role of arbitrators or mediators of conflicts that might appear relating the platform transactions. In fact, escrow mechanisms and multisignature wallets that require the majority of private key's owners' authorization to proceed with the payment have brought justice solutions that have been for a long time object of regulations, contracts and disputes in the traditional judicial system.

[97] Ortolani, P., (2016) The Three Challenges of Stateless Justice *Journal of International Dispute Settlement, 7(3), 596-627*

4. ICOS NOW AND THEIR THE FUTURE

The cyberspace as a digital world has been seen for some time as an unregulated space. Nowadays the regulation of cyberspace has been happening more often but there are still opposing views in this topic.

Lessig has been an advocate for the regulation of the cyberspace prior to this new legislative approach to the internet. "No doubt this particular mix of views will continue to puzzle some. How can I believe in regulation and yet be so skeptical about government? But it doesn't take much imagination to understand how these apparently conflicting views can go together. I take it we all believe in the potential of medicine. But imagine your attitude if you were confronted with a "doctor" carrying a vial of leeches. There's much we could do in this context, or at least, that is my view. But there's a very good reason not to want to do anything with this particular doctor."[98]

This chapter will present some of the concerns and recommendable practices for regulation of ICOs in the context of the cyberspace regulation trend.

4.1 Private international law

Besides the legal analysis to determine if the existing legislation of a country is applicable or not to an ICO, Initial Coin Offerings present the problem of which country´s law should be applicable. Normally, the choice of jurisdiction is made in the contract for the sale of tokens or token sale agreement. However, the nature of this fundraising technique and all the technologies associated with it can bring some relevant questions in the field of Private International Law.

The innovative technologies underlying an ICO are responsible for the most of the legal uncertainties since they bring possibilities and solutions not existing and therefore non-regulated before. Two of the main aspects are on one hand the extensive possibility of token buyers and investors from all around the world because the ICO have easy access to enter into the token sale agreement and on the other hand the fact that ICO transactions made through smart contracts are recorded and made possible through a decentralized public blockchain, normally Ethereum, that does not have a geographical limits. The data is stored all over the network of miners in the form of information that is encrypted and hashed in the different nodes.

[98] Lessig, L. (2006), Code: Version 2.0, New York, Basic Books A Member of the Perseus Books Group

Barsan points the most relevant issues on ICOs regarding conflict of jurisdiction and conflict of laws. A distinction is made between two stages of an ICO. First, there is the invitation to treat that is based on the information provided in the White Paper. At this stage there is no contractual relation between buyer and seller because the investor might decide not to buy tokens. In this scenario, the tort law can apply, especially related to the pre-contractual duties.

The other scenario is when the investors already bought tokens and might suffer damages because of the information that was presented in the White Paper. In that situation, the activity of the ICO issuing company can fulfil the conditions to be considered a fraud, under criminal law, and give origin to nullity of the contract and payment of damages according to the applicable tort law. In a situation when the tort law rules apply to the factual events, the courts that have jurisdiction are the ones where the harmful event took place. This poses a new challenge related with the place where the damage occurred. It is possible to say that the damage took place on the wallet of the token buyer. This constitutes a problem because a token wallet is a digital product that is dependent on the blockchain and therefore decentralised, when the wallet in case is a software wallet. In case of a custodial wallet, the place where the damage took place can be associated with the headquarters of the company that offers the wallet service.

Another question raised by Barsan is to know if contract law applies at all to a token sale event or ICO. A sale contract has the consideration for the good being money. In the ICO case, cryptocurrencies are not considered money and most ICOs do not accept fiat currencies during the token sale but only cryptocurrencies, Ethereum and Bitcoin most of all. Since cryptocurrencies are not money because they are not issued by a centralised governmental institution and are not a legal tender of any country, cryptocurrencies can be qualified as goods themselves. This way, a token sale would simply be a barter agreement where tokens are exchanged for cryptocurrencies. Another limitation for a token sale agreement to be considered a typical sale contract is that the goods that are being sold generally have to be tangible and tokens do not have that characteristic. It is concluded that it seems difficult to apply contract law to a token sale. Even if there are question on whether there is a typical sale contract with the characteristic legal obligations and rights, generally the principles of contractual law are applicable. Since there is a clear and inseparable connection between the White Paper and the sale of tokens, there will always be a situation where pre-contractual liability applies under Rome I regulation. When contractual law legal basis cannot be found for liability actions, tort law will apply in situation where damage was produced. Non-contractual liability cannot be excluded in contract by limitation of liability. The applicable law is the one from the jurisdiction where the damages occur. This solution still has the problem of determining the place where the

damage happened. This article defends that a similar case[99] can serve as analogy for determining the wallet has the place where the harmful event occurred. The *Kolassa* case held that according to Brussels Recast, the court where the harmful event occurred has jurisdiction, especially if that was the jurisdiction of the investor's bank account where the loss happened.

However, token holders are not considered investors because the offer is made to the public. Consequently, the token holder that qualifies as a consumer would see the law of its residence to apply to the contract when no law is chosen. Nevertheless, there is an exception that excludes the regime for consumer contracts in Rome I regulation: "rights and obligations which constitute a financial instrument and rights and obligations constituting the terms and conditions governing the issuance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units in collective investment undertakings in so far as these activities do not constitute provision of a financial service."[100] This means that tokens qualified as securities, financial instruments of units in investment funds are not object to conflict of law rules applicable to consumers.[101]

4.2 Regulatory actions

Countries from all around the world that have seen the rise of ICOs in their jurisdiction have started to take action. The approach is very different. It goes from issuing guidelines and recommendations until completely forbidding ICOs or creating specific laws with rules for the ICO procedure and clarification of concepts. There is a regional tendency of legally consider ICOs. If in western and central Europe it is more visible the adoption of guidelines, in Eastern Europe there has been the first steps to regulate ICOs and from Asia there is a bigger tendency to forbid ICOs.

Germany has followed the example of the United States, France and the Netherlands and the German Federal Financial Services Supervisory Authority has issued a statement on ICO and Token Regulation that concludes that the existing laws apply to ICOs, especially the ones related with banking regulation, payment service providers and, above all, securities regulatory requirements. The German securities' legislation has a specific class of securities that are units of account and is a class that is not stated in MIFID II or in other European countries. Therefore,

[99] Judgment of the Court (Fourth Chamber) of 28 January 2015. *Harald Kolassa v Barclays Bank plc*.
[100] Article 6 4. (d) of the Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) OJ L 177, 4.7.2008, p. 6–16
[101] Barsan, I. (2017). Legal Challenges of Initial Coin Offerings (ICP). *Revue Trimestrielle de Droit Financier (RTDF) (Quarterly Review of Financial Law), n° 3, 54-65*

the issued tokens are more likely to be considered a security in Germany than in other countries of Europe.

Switzerland released Guidelines for enquiries regarding the regulatory framework for initial coin offerings in February 2018 that shows the different categories of tokens and indicates conditions that might qualify the tokens under the scope of different legislative acts. In the previous year, the Swiss Financial Market Supervisory Authority started an investigation of an undisclosed number of ICO launching companies to assess the accordance of their activities with the legal framework existing in the country.

Gibraltar was the first country in Europe that created a regulation specifically for Blockchain. The regulation uses the legal term for Blockchain that is Distributed Ledger Technology and even though no clear reference or definitions are made regarding ICOs, the issuing companies fall within the scope of the regulation because of the use of Distributed Ledger Technology for record keeping of the tokens.

"The Chinese context is important because ICOs has raised nearly $400 million from about 100,000 investors prior to the ban. However, more recent statements from Chinese regulators have stated that the ICO ban is intermittent, pending a more systematic regulatory framework."[102]

South Korea has taken a similar approach to China by forbidding ICOs in its jurisdiction because of the lack of regulations that would protect the investors.

Russia and Belarus are jurisdictions were legislative action was pursued in respect to ICOs. In the case of Russia, there is a federal law project on digital financial assets. In this law it is possible to find definitions of distributed ledger technology, cryptocurrencies, mining and validation activity, smart contracts and tokens that are qualified as a digital financial asset. This federal law establishes a procedure for the issuance of tokens and imposes a maximum amount of contribution possible for non-accredited investors.

Belarus issued a presidential decree that includes similar definitions and creates a favourable framework for the issuance of Tokens. The innovative aspect of this regulation is the clarification on tax issues, by exempting token associated transactions from taxation for the period of the next five years.

[102] Chohan, U. (2017). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. SSRN

4.3 Future perspectives and proposed framework

One of the main questions regarding the future of cryptocurrencies in general and more specifically about Initial Coin Offerings is the problem of combining and harmonising the development of these new technology applications and the regulation scope of those new applications of the most diversify sectors of social interactions, namely the financial sector.

The issue of whether or not regulation hinders innovation has generally led the regulators to take precautions before regulating ICOs. "Bitcoin is a belief that innovations need to be encouraged and allowed to flourish rather than being shut down. (…) Regulators appear to be heeding these warnings and to be working to understand virtual currencies before they regulate. (…) This is generally a laudable position to take, as regulators certainly do not want to be accused of constricting innovation and job growth. However, this guiding principle should not blind them to important structural risks embedded in new technologies, particularly when these new technologies are attracting significant investment and attention from prominent business and policy leaders."[103]

As shown in previous chapters, the main reasons for an urge in regulation of ICOs is connected with the prevention of money laundering and scams but also the governmental need of taxation. An efficient regulation on the use of cryptocurrencies and tokens requires a deep knowledge of the context and possible consequences of such regulation projects. In today's political perspective, there is also caution taken when facing technology regulation because a good legal framework for financial technology start-ups and other larger corporations is a distinctive factor of economical attraction of a country.

When there is a lack of clear legal framework, there is the risk of regulatory arbitrage. "Regulatory arbitrage exploits the gap between the economic substance of a transaction and its legal or regulatory treatment, taking advantage of the legal system's intrinsically limited ability to attach formal labels that track the economics of transactions with sufficient precision."[104] ICO companies will choose the jurisdictions of which can have some comparative advantage with other ICOs and will modulate their issued token to specific legal regimes. This is a situation that can lead to adverse consequences in the future of the company. For example, regarding the avoidance of the token being considered a security: "Securities regulation furthers two general policy goals when applied to transactions: ensuring that investors have sufficient information when making investment decisions and deterring fraud. The requirement that securities offerings

[103] Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. NYUJ Legis. & Pub. Pol'y, 18, 837.

[104] Fleischer, V. (2010). Regulatory arbitrage. *Tex. L. Rev.*, *89*, 227.

either be registered or exempt from registration furthers the former purpose, and the securities fraud prohibitions, including private rights of action, further the latter. Not surprisingly, compliance with the securities laws is costly, which motivates parties to structure transactions in order to avoid application of the securities laws."[105] However, the consequences of avoiding this costly procedure f registering a security and releasing a prospectus has downsides when tax issues and consumer protection will start applying to those ICO companies.

A concern for future regulation that has not been amongst the top areas to regulate is the ICO company incorporation. The funds that are raised in cryptocurrency are stored in a crypto wallet that is not certain to whom it belongs to. Even though the contributions are addressed to the company, it is not certain if the public address is owned by the company, by an individual or by the different founders in the form of a multi-signature wallet. "All proceeds from the token sale go to the organization or group of developers selling the tokens. The nature of these organizations runs the gamut. Some are organized as traditional business entities or not-for profit foundations. Others are not formally organized - they consist of a loosely connected group of developers, and the proceeds from the token sale are distributed to those individuals."[106]

Cryptocurrencies have fees that sometimes are too high to justify small everyday transactions. "Most people seem to prefer to have their assets and liabilities denominated in the same currency. This reduces their risk in terms of their own currency, which is not trivial given the volatility of exchange rates. (…) It is hard to see the U.S. dollar being replaced by Bitcoin or other private digital currencies for everyday transactions. (…) Remittances are very expensive. Bitcoin definitely has the capability of disintermediating banks and payments processors in such uses. Regulation raises major unresolved hurdles. (…) The ability to evade capital controls may well be a very important effect of Bitcoin and similar private digital currencies."[107]

There is a general positive view that coins and tokens will contribute to a direct relation between service providers and product sellers and consumers by eliminating the traditional intermediaries. The token platforms can be seen as intermediaries but at the same time they are mostly connecting platforms run by a software and smart-contracts that give businesses a bigger audience and market for their activities and give consumers more options and security when getting some product or service. "The future of cryptographic currencies overall is even brighter than the future of bitcoin. (…) Many human activities that previously required centralized

[105] Couture, W. G. (2018). The Risk of Regulatory Arbitrage: A Response to Securities Regulation in Virtual Space. *74 Wash. & Lee L. Rev. Online 234*

[106] Rohr, J., Wright, A. (2017). Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets. SSRN

[107] Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability, 17*, 81-91.

institutions or organizations to function as authoritative or trusted points of control can now be decentralized. The invention of the blockchain and consensus system will significantly reduce the cost of organization and coordination on large scale systems, while removing opportunities for concentration of power, corruption and regulatory capture."[108]

The decentralized verification of transactions as well as the activity rewards or reputation tokens favour the trust in the system.

Jesse, Deokyoon et al. concluded for the need of more research on Blockchain technology and presented some suggestions for research that should be pursued and adopted in related technological fields of Blockchain before regulations are adopted.

The suggestions are to "continue to identify more issues and propose solutions to overcome challenges and limitations of Blockchain technology"; "to be ready for pervasive use of Blockchain technology, scalability issues such as performance and latency have to be addressed" and; to "develop more Blockchain based applications beyond Bitcoin and other cryptocurrency systems. Blockchain technology is applicable for other solutions such as smart contracts, property licensing, voting etc."[109]

To conclude it is essential that collaboration between the regulators and the industry is conducted in order for the most efficient and constructive legal understanding of the initial coin offering procedures to be better achieved. "We know that new disruptive technologies are just around the corner whether they are autonomous vehicles, smart contracts on blockchain platforms, ambient artificial intelligence systems in our homes and cars, or something yet to be envisioned. How do we prepare to regulate technology we do not really understand yet? We argue that this can be achieved by creating a collaborative, flexible, nimble process of regulation that involves all industry and regulatory stakeholders."[110]

The Collingridge dilemma is easily adapted to the regulation of ICOs. It states that "on the one hand, at the early stages of technological development, there is insufficient information regarding potential harms and benefits, but on the other hand, in later stages it can be very difficult, if not impossible, to alter the status quo once the technology has matured, diffusion has taken place and it has become an innovation."[111] This means that the answer for the question of whether ICOs should be regulated or not depends in part on the existing knowledge about the

[108] Antonopoulos, *supra nota* 21

[109] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

[110] Armitage, A., Cordova, A. K. (2017). Design-Thinking: The Answer to the Impasse between Innovation and Regulation. SSRN

[111] Collingridge, D. (1980), *The Social Control of Technology*, Pinter referenced in Butenko, A., & Larouche, P. (2015). Regulation for innovativeness or regulation of innovation? *Law, Innovation and Technology*, *7*(1), 52-82.

underlying technology and the evidence of adverse effects originating from the issuance, trade and usage of tokens. At the present, the intermediate moment of the Collingridge dilemma seems to be happening.

Concluding that there is a need for regulation of ICOs, there are two main questions: what are the most important legal issues to be solved with the new legal framework; and if a law should be specifically created for regulating ICOs or if the existing ones should be amended.

It must be clear whether tokens can be considered property, a digital asset for example, and therefore be legally protected by ownership rights, or if the token is considered a right or a contractual position. It is not possible to consider ownership of tokens when it is not specified in property law because of the principle of *numerus clausus*. This is an important issue to be regulated because if a token is not a thing or under and therefore not under the classification of ownership, then the token is in fact a security. Token as a financial instrument, not dependant of any particular form, that has a patrimonial right attached. This creates the situation where there would be securities within and outside the scope of MIFID ii, which would present difficulties to exactly determine under which category of security the token would be.

It would be very positive to include the ICO tokens under the category of property. This can be done either by a more inclusive definition of "thing" that would include objects besides physical things or by creating special law for ICO that would create a new property category: the digital assets.

The uncertainty regarding property law does not affect the possibility of the token to be the object of a contract of sale because, according to the Law of Obligations Act of Estonia, the sale of things applies to the sale of rights and other objects.

However, the consumer sale, as stated in the Law of Obligations Act of Estonia, is only applicable to the sale of a thing on the basis of a contract of sale where a consumer is sold a movable by a seller. For consumer protection to apply to ICO sale of tokens, it would be required for the ICO to be considered a consumer service. It does not seem correct to include the ICO under service because the service will only start when the proposed platform is operational. For consumer protection to apply for the sale of tokens as a good, the classification of a digital asset is once more relevant.

The income tax in Estonia is charged on gains from the sale or exchange of any transferable and monetarily appraisable objects. It does not present reason for dispute that tokens are, indeed, a monetarily appraisable object, since one of the main characteristics associated with the token is the possibility to sell it for other virtual currencies and, therefore to money, in the sense of fiat currencies.

With respect to the financial nature of the services to be provided by the ICO company using their token, there are two matters to be addressed in a regulatory level.

First, it is necessary to establish the equivalence or not of tokens, depending on their rights, and virtual currencies in general to fiat money. This is a position that has to be taken on the political level because the issuance of money is a highly governmental centralised activity and, in case of the European Union, even a supranational centralised activity.

Secondly, and only when that decision is adopted, the financial crypto activities that are similar to the traditional banking/financial activities can see the same regulations being applied.

Right now, it is not possible to consider a token lending-like financial service to the regulated by the Law of Obligations Act as a loan agreement or credit agreement. The reasons are similar with the problem regarding property law and with the concept of money as legal tender. Loan agreement have as legal object a sum of money or a fungible thing, while a credit is only a sum of money. Therefore, the rules applicable to credit institutions are not applicable to financial activities based on tokens.

In the cases provided by law, provisions concerning things apply to rights.[112] A special law regulating ICOs and the tokens issued can create the equivalence between the token as a patrimonial right originating from a contract to the provisions concerning things.

Due to the multiplicity of rights that can be associated with a token and the consequent extensive number of legal acts that already apply or should apply, a law should be specifically created for the creation of a legal framework for ICOs.

Besides the previous suggested changes, the following legislative actions should be pursued to complete the proposed framework.

When classifying a token as a security especially as an instrument that confers similar rights to a share, would be important to limit the extent to which a token can be a similar right to a share. The exclusive attribution of one right (*e.g.* governance right) might not qualify the token as similar to share when all the other rights are missing (*e.g.* profit distribution or company's ownership).

The issue of knowing if non-accredited investors can or not participate in an ICO depends also on the rights that are given with the token. A limitation of participation for non-accredited investors would only be acceptable when the token is purely a security, *i.e.* not a hybrid of a virtual currency or a token with utility associated. The legal framework for ICOs could, nevertheless, establish a facilitation mechanism of investment for non-accredited investors with

[112] Tsiviilseadustiku üldosa seadus, RT I, 20.04.2017, 21, § 49 (2)

the knowledge of the risk associated with the token. A monetary limit in this case would be understandable. If the token has utility elements, is a cryptocurrency or a hybrid, obligations could be established for the future service provider to comply with the main promises presented in the White Paper, by allowing the respective Token holders to easily access the progress done by the company or, for example, to establish parameters that would show, more clearly, adhesion to the roadmap timelines. An obligation to redeem tokens could be created for the case of purely utility tokens that have the characteristics of a pre-sale of services.

A limit of sales for a non-security token does not seem reasonable, as people are not usually limited for the acquisition of goods or services. However, warning about the risks associated with the token, in particular the price volatility, should always be included in the sale agreement.

In order to legitimise the ICO procedure, further measures could be adopted. That would include regulation of crypto exchanges, by requiring more AML and KYC procedures, defining standards for accepting tokens in the exchange lists that would be objective and not depending on the token issuer paying the exchanges a determined sum of money, and demanding the necessary efforts to ensure cybersecurity and data and privacy protection.

One final legal measure to adopt is to regulate the control of the raised funds. Who exactly is the holder of the cryptocurrencies collected during the ICO has to be clear. There has to be predefined authorised holders that could be a wallet account in the ICO company's name or an escrow. The possibility for the individuals that launched the ICO to hold the funds in their private wallets can be considered a risk factor that facilitates scams and frauds.

The existence of such legal framework for ICOs can create conditions for fully compliant ICOs that present the clear steps and duties of an ICO launching company while ate the same time protecting investors and consumers. Such specifically created law would enable the country enabling it to be the chosen law for the ICO procedure.

While a legal framework for ICOs is not developed, interpreting existing laws based on substance over form is only adequate when form is not closed or determined (*e.g.* in the case of qualifying a token as a similar right to a security). Definitions have to be respected or there is the risk of making interpretation *contra legem*, which is prejudicial and hinders technological advancements as ICOs are an example.

CONCLUSION

The aim of this Master's thesis is to highlight the main legal problems that originate with conducting ICO as well as by using its underlying technologies: cryptocurrencies, distributed ledger technology (or blockchain technology) and smart contracts. The existence of legal uncertainty in damaging for start-up companies that wish to be innovative and also for buyers and investors that are not fully protected when dealing with cryptocurrencies, which consists on distance juridical relations that include a big diversity of legal effects from different jurisdictions because ICOs are a global market.

The answers to the questions that were developed during this thesis can be summarised as follows:

What are the risks of ICOs? ICOs issue a token that can only be used in the future when the platform will be developed and operational. This creates high volatility of the token price. Some ICOs have been proven to be a fraud. The risk of being a fraud is higher when there is not much information about the team behind the project. Cryptocurrencies in general and tokens are not backed by any governmental agency and depend only on the fact that individuals recognise its value. The fact that legal protection for crypto holders is not certain increases the general risk.

What is the legal value of a Token? Tokens are classically divided into cryptocurrency token, in the sense that there is no service associated with the token besides the possibility of using it as a medium of exchange, utility tokens, which are categorised as such because of the specific usage of a platform through the payment of fees for access or because they are the internal currency for products and services and security tokens, that have the characteristics of securities has set in the law and are mostly associated with the expectation of distribution of profit, governance rights or ownership of a company or the tokenisation of a commodity. It is not always easy to clearly determine under which categories the tokens can be qualified due to the different possible combinations of rights and value that can be associated with a token. A complex issue is the fact that the token can be considered a hybrid token.

What regulations already apply? Some law might indeed be applicable, from financial law (banking law and securities law) to consumer protection law and tax law or anti money laundering law. An important condition to assess the applicability of existing laws is the proximity that tokens have to government backed/fiat currencies. This is visible in the required licenses for crypto exchanges against fiat currency as well as e-money requirements. If a token is

merely a digital representation of value of a fiat currency and is established at par value, the e-money regulations apply.

What are the possible regulatory approaches? It is possible to adopt specific regulations on ICOs that establish an appropriate legal framework for conducting this mechanism of crowdfunding but it is also possible to clarify existing laws and create definitions or adapt existing ones in order to bring certainty to the concept of tokens. Some countries have already adopted a legislative approach to Initial Coin Offerings.

There is certainly a legal vacuum in the regulation of tokens and ICO since they are not specifically regulated but it is not necessarily the Wild West that some analysts present it to be.

However, the multiplicity of ICO applicable regulations, which depends on its value, and the risks associated to cryptocurrencies, in the most general idea of this concept, leads to a very high degree of legal uncertainty for ICO launchers, for the buyers or investors and for the governmental authorities responsible for the supervision of the financial system.

Facing so much uncertainty on the applicable laws on this level, it is expectable that the same uncertainty and questions would take place at the court level. Therefore the present is moment to prevent court decisions that would be contradicting. It is an option to wait for case law at the European level to bring some light to ICO but it would be more effective to prevent potential harm and help to create a positive business flow.

Important conclusions that were reached in this thesis is that contrary to cryptocurrencies that have a stronger currency and alternative means of payment characteristic associated, tokens have a closer relation with property law, in the sense that they can be considered as a new form of (digital) asset in most cases. However, some jurisdictions, including Estonia have the perspective of property law based on the object as a physical thing. It is certain that the law can create equivalent effects to not physical things but this has not been done so far in relation with tokens.

Nevertheless, some tokens might be virtual currencies with the same function of pure cryptocurrencies working as a mean of payment.

The fact that the principle of private autonomy allows for the parties to agree upon the contractual claims and obligations that do not have to be typified in the legislation does not mean that it should be the way to face ICOs. Mostly because of the wide reach that token issuance has worldwide and because contractual clauses for the token generation event include very often clauses that are standard terms.

The principle of private autonomy does not solve the problem of the lack of form for characteristically performances or the importance to have clear regulations for banking activities or securities issuance.

In conclusion, to answer the research hypothesis there is indeed some laws that are applicable to ICOs but there is a need for specific regulation for harmonization in the European level and for clarification in both European and national level of regulations.

These conclusions are relevant for the determination of a need for regulation and for highlighting the economic and legal risks associated with the tokens and to establish the conceptual distinctions and different approaches between tokens and cryptocurrencies,

Further research possibilities include micro comparison between legal arrangements and macro comparison of applicable laws to ICOs in different jurisdictions.

LIST OF REFERENCES

SCIENTIFIC BOOKS

1. Antonopoulos, A. M. Mastering Bitcoin, Unlocking Digital Cryptocurrencies, Sebastopol, O'Reilly

2. Lessig, L. (2006), Code: Version 2.0, New York, Basic Books A Member of the Perseus Books Group

3. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press

4. Sá Soares, D., (2016) Electronic Government, 15th IFIP WG 8.5 International Conference, EGOV 2016 Guimarães, Portugal, September 5–8, 2016 Proceedings, s. l., Springer

5. Swan, M., Blockchain: Blueprint for a New Economy, Sebastopol, O'Reilly

SCIENTIFIC ARTICLES

1. Adhami, S., Giudici, G., Martinazzi, S. (2017) Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings. *Social Science Research Network.* SSRN

2. Armitage, A., Cordova, A. K. (2017). Design-Thinking: The Answer to the Impasse between Innovation and Regulation. SSRN

3. Barsan, I. (2017). Legal Challenges of Initial Coin Offerings (ICP). *Revue Trimestrielle de Droit Financier (RTDF) (Quarterly Review of Financial Law), n° 3, 54-65*

4. Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. (2017). Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. *arXiv preprint arXiv:1703.03779.*

5. Bayern, S. (2014). Dynamic common law and technological change: the classification of Bitcoin. *Wash. & Lee L. Rev. Online*, *71*, 22.

6. Belleflamme, P., Lambert, T., Schwienbacher, A. (2014). Crowdfunding: Tapping the right crowd. *Journal of business venturing*, *29*(5), 585-609.

7. Biryukov, A., Khovratovich, D. (2017). Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger*, *2*, 1-30.

8. Böhme, R., Christin, N., Edelman, B., Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213-38.

9. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015) Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *Security and Privacy (SP), IEEE Symposium on 2015*, IEEE, 104-121.

10. Botos, H. M. (2017). A Blockchain Intelligence Analysis. *Res. & Sci. Today, 13*, 42.

11. Breu, S., Seitz, T. G. (2017). Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society. *SSRN*

12. Brito, J., Shadab, H., Castillo, A. (2014). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling. *Colum. Sci. & Tech. L. Rev.*, *16*, 144.

13. Butenko, A., & Larouche, P. (2015). Regulation for innovativeness or regulation of innovation?. *Law, Innovation and Technology*, 7(1), 52-82.

14. Cai, Y., Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, *2*(1), 20.

15. Catalini, C., Gans, J. S. (2016). *Some simple economics of the blockchain* (No. w22952). National Bureau of Economic Research.

16. Chohan, U. (2017). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. *SSRN*

17. Chuen, K., David, L. E. E., Guo, L., & Wang, Y. (2017). Cryptocurrency: A New Investment Opportunity? *The Journal of Alternative Investments*, *20*(3).

18. Cohn, A., West, T., Parker, C. (2017). Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids. *GEO. L. TECH. REV.*, *1*, 273-284.

19. Conley, J. P. (2017). *Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings* (No. 17-00008). Vanderbilt University Department of Economics.

20. Connor-Green, D. S. (2016). Blockchain in Healthcare Data. *Intell. Prop. & Tech. LJ*, *21*, 93.

21. Couture, W. G. (2018). The Risk of Regulatory Arbitrage: A Response to Securities Regulation in Virtual Space. *74 Wash. & Lee L. Rev. Online 234*

22. Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology*, *25*(3), 179-195.

23. Dimitri, N. (2017). Bitcoin Mining as a Contest. *Ledger*, *2*, 31-37.

24. Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, *17*, 81-91.

25. Elendner, H., Trimborn, S., Ong, B., Lee, T. M. (2016). *The cross-section of crypto-currencies as financial assets: an overview* (No. 2016-038). SFB 649 Discussion Paper.

26. Enyi, J., Le, N. (2017). The Legal Nature of Cryptocurrencies in the US and the Applicable Rules. *SSNR*

27. Fanning, K., Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, *27*(5), 53-57.

28. Fleischer, V. (2010). Regulatory arbitrage. *Tex. L. Rev.*, 89, 227.

29. Flood, J., Robb, L. (2017). Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings. *SSRN*

30. Furlanello, C., De Domenico, M., Jurman, G., & Bussola, N. (2017). Towards a scientific blockchain framework for reproducible data analysis. *arXiv preprint arXiv:1707.06552*.

31. Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, *2*(1), 24.

32. Hacker, P., Thomale, C. (2017). Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. SSRN

33. Halaburda, H. (2016). Digital Currencies: Beyond Bitcoin. SSRN

34. Hileman, G., Rauchs, M. (2017). Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*. SSRN

35. Hsiao, J. I. (2017). Smart Contract on the Blockchain-Paradigm Shift for Contract Law. *US-China L. Rev.*, *14*, 685.

36. Iansiti, M., Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118-127.

37. Jaccard, G. (2018). Smart Contracts and the Role of Law. SSRN

38. Kaal, W., Dell'Erba, M. (2017). Initial Coin Offerings: Emerging Practices, Risk Factors, and Red Flags. SSRN

39. Kleemann, F., Voß, G., Rieder, K. (2008). Un(der)paid Innovators: The Commercial Utilization of Consumer Work through Crowdsourcing. *Science, Technology & Innovation Studies*, *4*(1), 5 - 26. http://www.sti-studies.de/ojs/index.php/sti/article/view/81

40. Leonard, C. (2016). Blocking the Blockchain. *Int'l Fin. L. Rev.*, *35*, 58.

41. Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 254-269. ACM.

42. Marian, O. (2015). A conceptual framework for the regulation of cryptocurrencies. U. Chi. L. *Rev. Dialogue*, 82, 53.

43. Minto, A., Voelkerling, M., & Wulff, M. (2017). Separating apples from oranges: identifying threats to financial stability originating from FinTech. *Capital Markets Law Journal*, 12(4), 428-465.

44. Moyano, J. P., Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, *59*(6), 411-423.

45. Ortolani, P., (2016) *The Three Challenges of Stateless Justice Journal of International Dispute Settlement*, 7(3), 596-627

46. Peters, G., Panayi, E., Chapelle, A. (2015). Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. SSRN

47. Pittman, A. (2016). The Evolution of Giving: Considerations for Regulation of Cryptocurrency Donation Deducations. *Duke L. & Tech. Rev.*, *14*, 48.

48. Raskin, M. (2016). The Law and Legality of Smart Contracts. *SSRN*

49. Reyes, C. L. (2016). Moving beyond bitcoin to an endogenous theory of decentralized ledger technology regulation: an initial proposal. *Vill. L. Rev.*, *61*, 191.

50. Robinson, R. (2017). The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings. *SSRN*

51. Rohr, J., Wright, A. (2017). Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets. *SSRN*

52. Sauer, B. (2016). Virtual currencies, the money market, and monetary policy. *International Advances in Economic Research*, *22*(2), 117-130.

53. Shakow, D. J. (2017). The Tax Treatment of Tokens: What Does It Betoken?. *SSRN*

54. Sun, J., Yan, J., Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, 2(1), 26.

55. Venegas, P. (2017). Initial Coin Offering (ICO) Risk, Value and Cost in Blockchain Trustless Crypto Markets. *SSRN*

56. Walch, A. (2015). The bitcoin blockchain as financial market infrastructure: A consideration of operational risk. *NYUJ Legis. & Pub. Pol'y, 18*, 837.

57. Wang, H., Chen, K., Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, *2*(1), 12.

58. Xu, J. J. (2016) Are blockchains immune to all malicious attacks? *Financial Innovation 2 (1)*, 25

59. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

60. Zetzsche, D. A., Buckley, R. P., Arner, D. W., Föhr, L. (2018). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. SSRN

ESTONIAN LEGISLATION

1. Asjaõigusseadus, RT I 1993, 39, 590,

2. Karistusseadustik, RT I 2001, 61, 364

3. Võlaõigusseadus, RT I 2001, 81, 487

4. Väärtpaberituru seadus, RT I 2001, 89, 532

5. Tsiviilseadustiku üldosa seadus, RT 2002, 35, 216

6. Käibemaksuseadus, RT I 2003, 82, 554

7. Rahapesu ja terrorismi rahastamise tõkestamise seadus, RT I, 17.11.2017, 2

8. Tsiviilseadustiku üldosa seadus, RT I, 20.04.2017

EU AND INTERNATIONAL LEGISLATION

1. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) OJ L 177, 4.7.2008, p. 6–16

2. Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ L 201, 27.7.2012, p. 1–59

3. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267, 10.10.2009, p. 7–17

4. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304, 22.11.2011, p. 64–88

OTHER COUNTRIES' LEGISLATION

1. Congress Bill, H. R. 3606 (112th): Jumpstart Our Business Startups (USA)

OTHER COURT DECISIONS

1. U.S. Supreme Court SEC v. Howey Co., 328 U.S. 293 (1946) *Securities and Exchange Commission v. Howey Co*

2. Judgment of the Court (Fifth Chamber) of 22 October 2015, *Skatteverket v David Hedqvist*, Case C-264/14

3. Judgment of the Court (Fourth Chamber) of 28 January 2015. *Harald Kolassa v Barclays Bank plc*.

OTHER SOURCES

1. https://coinmarketcap.com/

2. https://arstechnica.com/tech-policy/2017/12/bitcoin-fees-rising-high/

3. Commission Staff Working Paper Impact Assessment Accompanying the document Proposal for a Directive Of The European Parliament And Of The Council on Markets in financial instruments [Recast] and the Proposal for a Regulation Of The European Parliament And Of The Council on Markets in financial instruments {COM(2011) 656 final} {SEC(2011) 1227 final}

4. Commission Staff Working Document Impact Assessment, Accompanying the document Proposal for a Directive of the European Parliament and the Council, SWD (2016) 223 final

5. ESMA 50-157-829, 13 November 2017