# UNIVERZITA KARLOVA

## Právnická fakulta




**Teodora Drašković**


# Blockchain na evropské úrovni

Diplomová práce


Vedoucí diplomové práce: JUDr. Tereza Kunertová, LL.M., Ph.D.

Katedra: Katedra evropského práva

Datum vypracování práce (uzavření rukopisu) : 31. srpna 2018

# CHARLES UNIVERSITY

## Faculty of Law




**Teodora Drašković**


# Blockchain at the European Level

Master's Thesis


Master's Thesis Supervisor: JUDr. Tereza Kunertová, LL.M., Ph.D.

Department of European Law



Date of completion (manuscript closure): 31 August 2018

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce má 225 692 znaků bez příloh, včetně poznámek pod čarou a mezer.

I declare that this master's thesis is a result of my independent work and that all the used sources have been duly cited. I further declare that this master's thesis has not been used to obtain any other or the same academic degree.

I further declare that the text of this master's thesis itself has 225 692 characters without annexes and including footnotes and gaps.

Teodora Drašković

V Praze dne / In Prague on

## Poděkování

Ráda bych poděkovala JUDr. Tereze Kunertové, LL.M., Ph.D. za trpělivost, čas, podporu a cenné rady a komentáře, které mi během psaní této diplomové práce poskytla.

Mé poděkování rovněž patří mé rodině za veškerou inspiraci, pomoc a podporu, které mi poskytovali během celého studia.

## Acknowledgment

I would like to thank JUDr. Tereza Kunertová, LL.M., Ph.D. for the patience, time, support and valuable advice and comments that she has provided me with during the writing of this master's thesis.

I would also like to express my thanks to my family for all inspiration, help and support that they have provided to me in the course of my studies.

## Content

## Introduction

According to statistical reports, in June 2018 the word Bitcoin was the 54th most searched keyword on Google[1], while in 2017, it was the second most-searched global news term.[2] Cryptocurrency community is experiencing a boom of attention and it is not reaching only a narrow group of enthusiasts anymore. More importantly, the attention is increasingly drawn towards the underlying technology of blockchain and its potential utilization without limitation to the financial sector solely. The technological development was largely left unchecked for the most part of the decade since its introduction in 2008, however, over the last couple of years and with unexpected spikes of value of cryptocurrencies and security scandals, the attention of national regulators has been sparked and the global discussion as to where in the legal system we should place blockchain and cryptocurrencies has begun. Upon discovering that the European Commission was launching a blockchain observatory program[3] and study[4], I decided to base my master thesis on the topic of blockchain technology within the EU regulatory framework. My main motivation was to explore a new and largely undiscovered area of modern technology from the legal point of view. Due to its complexity and many differing approaches of national jurisdictions, I considered the assessment at the European level and internal market as the best and most useful approach for conducting a complex analysis. For this purpose I used legal analysis and comparative methods.

The aim of this thesis is to provide a basic overview of how the technology works and all major areas where the deployment of blockchain might be subject to already established regulatory requirements. Given the short and revolutionary history of the blockchain technology, there are only scarce literature and source materials available. Most of the undertaken assessments are either of highly technical nature, or focus on a narrow scope of blockchain's features or relating legal fields. This thesis, therefore, seeks to implement the

---

[1] R. Hudgens, '*The 100 Most Popular Google Keywords [Infographic]*' (2018), available at: https://www.siegemedia.com/seo/most-popular-keywords, last accessed 17.8.2018.

[2] J. Koetsier, '*Bitcoin Is The Second Most-Searched Global News Term Of 2017*' (2018), *available at:* https://www.forbes.com/sites/johnkoetsier/2017/12/13/bitcoin-is-the-second-most-searched-global-news-term-of-2017/, last accessed 17.8.2018.

[3] See '*EU Blockchain Observatory and Forum*' (2018), available at: https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum, last accessed 17.8.2018.

[4] See '*Study on opportunity and feasibility of a EU blockchain infrastructure*' (2017), available at: https://ec.europa.eu/digital-single-market/en/news/study-opportunity-and-feasibility-eu-blockchain-infrastructure, last accessed 17.8.2018.

particular aspects of legal research into a coherent and comprehensive outline which might serve as a first step for necessary further research on the legal side of decentralized ledgers. As I am very interested in this topic, I would like to conduct more research in the future, in order to be able to assess the presented legal concerns and fields in more depth and, simultaneously, to provide thorough legal assessment in other areas of blockchain development which could not be included in this master's thesis, namely, e.g. in the public sector for eGovernment purposes or supply chains.

This master's thesis is divided into four chapters. The first Chapter provides an introduction of EU primary law in respect of the EU's competence to act in the area of blockchain technology. Then, basic description of blockchain technology is laid down in Chapter two, while more detailed and technical information is included in Annexes I - IV of this master thesis. Subsequently, in Chapter three, regard is given to cryptocurrencies and smart contracts and their potential utilization concepts and solutions. Lastly, Chapter four assess ten particularly interesting aspects of blockchain technology which, under certain circumstances, might be viewed as advantages or potential issues that need to be overcome for future mass deployment of blockchain.

*"I am pro-technology that improves the lives of many people in any way possible, and I think the blockchain has the potential to do that."*

Melanie Swan

"*It will take time for the idea of decentralized trust through computation to become a part of mainstream consciousness, and until then, the idea creates cognitive dissonance for those accustomed to centralized trust systems*."

Andreas Antonopoulos

## 1. EU Competence in Respect of Blockchain Technology

The EU was established by the Member States with the intention to fulfill the envisioned goals such as monetary and customs union, free movement of goods, services, persons and capital, common policies in e.g. agricultural sector, cooperation in judicial affairs, etc.[5] Thus, the EU can only act on the basis and within the limits of powers and competences[6] attributed to it by the sovereign Member States.[7] The so-called principle of conferral has been one of the fundamentals of the European integration from the beginning.[8] Currently, it is enshrined in Article 5(1) of the TEU and further defined in Article 5(2) of the TEU: "*Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.*" Per this principle, every legal document of the EU has to have a legal basis; otherwise, it would be an act *ultra vires*, i.e. beyond the limits of attributed competence.

[5] See K. Lenaerts, P. Van Nuffel, R. Bray, N. Cambien, *European Union Law* (3rd ed., Sweet & Maxwell 2011), p. 106-111.

[6] While some national jurisdictions differ between the notion of power and competence (e.g. the Czech Republic), the EU law generally does not distinguish between the two; therefore, this thesis will hereinafter understand the notion competence as encompassing the term power as well. See P. Svoboda, *Úvod do evropského práva* (5th ed., C.H. Beck 2013), p. 46.

[7] M. Tomášek, V. Týč and coll., *Právo Evropské unie* (2nd ed., Leges 2017), p. 147; P. Craig, G. de Búrca, *EU law: text, cases, and materials* (6th ed., Oxford University press, 2015), p. 74; K. D. Borchardt, *The ABC of EU law* (6th ed., EU Publications Office 2011), p. 38, H. C. H. Hofmann, '*General principles of EU law and EU administrative law*' in C. Barnad, S. Peers (eds), *European Union Law* (2nd ed., Oxford University Press 2017), p. 197-198; R. Shütze, *European Union Law* (1st ed., Cambridge University Press 2015), p. 224-225.

[8] M. Tomášek, V. Týč, op. cit. no. 7, p. 147-150; L. TIchý, R. Arnold, J. Zemánek, R. Král, T. Dumbrovský, *Evropské právo* (5th ed., C. H. Beck 2014), p. 68-70.

Nevertheless, the delimitation of competence limits and consequently, the particular legal basis is not always clear.[9] For this reason, the legal theory distinguishes between three types of the EU competence: (i) expressly attributed competence, (ii) implicitly attributed competence and (iii) subsidiary/supplementary competence.[10] While the CJEU does not step in to define EU's competence and its limitations very often, an example of such definition of limitation might be the *Tobacco Advertising* case[11] where the Court held that the interpretation of Article 114 (then 95) of the TFEU cannot be extended so as to allow any action on the EU level, solely based on the internal market pretense.[12]

The first group encompasses all instances when the treaties expressly authorize the EU (and/or any of its institutions) to carry out a specified task. [13] Articles 3 to 6 of the TFEU serve as an example. Implicitly attributed are the competences which are reasonably necessary for the exercise of an expressly attributed competence[14], i.e. all competences that are enshrined within but not explicitly enumerated in the treaties. A usually provided example is the external competence of the EU which might be necessary if the matter requires international negotiation and agreement.[15] In the pre-Lisbon era, the principle of implied international competence was set down by the CJEU's ERTA doctrine[16] and following case law. While the doctrine was subsequently codified in Article 5(2) TFEU, there is presently still considerable discussion as to the scope of its interpretation.[17] Finally, the notion of subsidiary competence refers to situations when the treaties only set forth specific goals which should be achieved within the Union, however, they do not stipulate the EU's competence. In

[9] K. Lenaerts and coll., op. cit. no. 5, p. 113-117.

[10] P.Svoboda, op. cit. no. 6, p. 51-52; K. Lenaerts and coll., op. cit. no. 5, p. 122-123.

[11] Case-380/03 *Germany v European Parliament and Council* [2006] ECLI:EU:C:2006:772.

[12] See also P. Craig, G. de Búrca, op. cit. no. 7, p. 76; J. Snell, *The internal market and the philosophies of market integration* in C. Barnard, S. Peers (eds), op. cit. no. 7, p. 317-319.

[13] P. Svoboda, op. cit. no 6, p. 54; L. Tichý and coll., op. cit. 8, p. 74; K. Lenaerts and coll., op. cit. no.5, p. 113.

[14] M. Tomášek, op. cit. no. 8, p. 149; P. Craig and G.de Búrca, op. cit. no. 7, p. 76; K. Lenaerts and coll., op. cit. no. 5, p. 120-121.

[15] P. Svoboda, op. cit. no. 6, p. 54-55.

[16] The ERTA doctrine follows from the CJEU's judgment Case C-22/70 *Commission v Council* [1971] ECLI:EU:C:1971:32. See also T. Verellen, '*The ERTA Doctrine in the Post-Lisbon Era: Note under Judgment in Commission v Council (C-114/12) and Opinion 1/13*' (2015), 21 Colum. J. Eur. L. 383, [online] last accessed 17.8. 2018; M. Hodun, *Doctrine of Implied Powers as a Judicial Tool to Build Federal Policies*.

[17] The discussion namely relates to notion of "largely covered area" and was stirred once more with CJEU's partially contradicting approaches which might be observed namely in its reasoning in C-114/12 *Neighboring rights* [2014] ECLI:EU:C:2014:2151 and in CJEU, Opinion 1/13 (Grand Chamber) [2014] ECLI:EU:C:2014:2303. See also T. Verellen, op. cit. no. 16.

order to overcome such gaps, Article 352(3) of the TFEU provides for a blanket authorization of EU institutions.[18]

The second categorization of EU competences is based on the extent and nature of the competence, i.e. the amount of competence that is transferred from the Member States to the EU. Firstly, in the exhaustive list of specified areas, the EU has the exclusive competence, i.e. in such areas, the EU is the primary actor and Member States can only adopt legal acts if specifically authorized or instructed by the EU.[19] The areas of Union's exclusive competence are enumerated in Article 3 TFEU as follows: (i) customs union; (ii) competition; (iii) monetary policy for eurozone members; (iv) conservation of marine biological resources under the common fisheries policy; (v) common commercial policy and (vi) conclusion of international agreements relating to areas of EU's exclusive competence.

Secondly, in a majority of areas the EU has a so-called shared competence with Member States which can be either pre-emptive (Member States can adopt legally binding acts only in areas where the EU decided not to or ceased to continue exercising competence[20], thus, respective competences of Member States and the EU exclude one another), or non-pre-emptive (EU's competence cannot prevent Member States from exercising their competence in the particular matter, e.g. humanitarian aid or research). The non-exhaustive list of shared competences is provided in Article 4 TFEU and it includes e.g. internal market, consumer protection, area of freedom, security and justice, etc. The primary instrument of shared competence is harmonization under Article 114 TFEU[21]. At this point it should be emphasized that the borderline between exclusive and shared competence can in some cases be particularly blurry. For instance, taking the customs union as a representative of the exclusive competence and the internal market as matter falling within shared competence, "*it may be difficult to decide whether a case is concerned with the customs union, tariffs, quotas, and the like, or whether it is really 'about' discriminatory taxation. There can in addition be*

[18]M. Tomášek and coll., op. cit. no. 8, p. 149-150; P. Svoboda, op. cit. no. 6, p. 55, P. Craig and G. de Búrca, op. cit. no. 7, p. 91-93, R. Schutze, op. cit. no. 7, p. 231-234; L. Tichý and coll., op. cit. no. 8, p. 75-76; K. Lenaerts and coll., op. cit. no. 5, p. 122-123.

[19] K. Lenaerts and coll., op. cit. no. 5, p. 124-127; P. Craig and G. de Búrca, op. cit. no. 7, p.78; M. Tomášek and coll, op. cit. no. 8, p. 154; R. Schütze, op. cit. no. 7, p. 237-238.

[20] P. Craig and G. de Búrca, op. cit. no. 7; p. 84; K. Lenaerts and coll., op. cit. no 5, p. 127-130.

[21] J. Snell, op. cit. no. 12, p. 315; R. Schütze, op. cit. no. 7, p. 229.

*disputes as to whether an act falls within common commercial policy or the internal market*."[22]

Last type of competence distribution is the supporting, coordinating, or supplementary action which allows the EU to only assist Member States when exercising their primary competence, thus excluding harmonization[23]. The included areas are specified in Article 5 TFEU and they include e.g. health sector, tourism or education matters.[24]

Apart from the above established scope, the Member States are the sole bearers of competence (so-called retained power), such as citizenship rules, security or direct taxation; however, when exercising their retained powers Member States are obliged to act in compliance with the EU law[25] and principle of sincere cooperation enshrined in Article 4(3) TEU[26].

Together with the conferral principle, the subsidiarity principle enshrined in Article 5(3) TEU and proportionality principle embedded in Article 5(4) TEU should also be taken into account when exercising competence within the EU territory[27]. Adherence to the subsidiarity principle is monitored mainly by national parliaments and requires the EU to act within areas of shared competence solely if the envisioned goal can be better attained at the EU level.[28] The proportionality principle consists of two parts which should be attained by every legal act adopted on the EU territory: the legal act must be appropriate for the intended objective, and necessary, i.e. there are no other instruments which could achieve the objective.[29] Therefore, while the subsidiarity principle applies only in the areas of shared competence, proportionality principle is applicable to exclusive and coordinating competenceS as well.

As follows from the assessment in this thesis below, blockchain technology is not easy to categorize in terms of appropriate regulation and consequently, the exercise of competence, especially in respect of cryptocurrency. Given the individual secondary legislation that has

---

[22] P. Craig and G. de Búrca, op. cit. no. 7, p. 79.

[23] P. Craig and G. de Búrca, op. cit. no. 7, p. 86; M. Tomášek and coll., op. cit. no. 8, p. 156: Specific type of coordinating action relates to coordination of economic and employment policies under Article 5 TFEU. See also R. Schütze, op. cit. no. 7, p. 241-243.

[24] P. Craig and G. de Búrca, op. cit. no. 7, p. 86.

[25] P. Svoboda, op. cit. no. 6, p.58, P. Craig and G. de Búrca, op. cit. no. 7, p. 86.

[26] H. C. H. Hofman , op. cit. no. 7, p. 197-198; K. Lenaerts and coll., op. cit. no. 5, p. 147-155.

[27] M. Tomášek and coll., op. cit. no. 8, p. 157-158.

[28] P. Craig and G. de Búrca, op. cit. no. 7, p. 96, 97; L. Tichý and coll., op. cit. 8, p.74-75; K. Lenaerts and coll., op. cit. no. 5, p. 131-140.

[29] H. C. H. Hofman, op. cit. no. 7, p. 203-204; P. Svoboda, op. cit. no. 6, p. 48; K. Lenaerts, op. cit. no. 5, p. 141-147.

been considered and in some instances already applied to cryptocurrencies and other blockchain technology, it follows that they are likely based in shared competence, particularly the internal market which aims at establishment and promotion of four freedoms of movement – pertaining to goods, services, persons and capital.[30]

Provided that cryptocurrency is qualified as a payment instrument or a financial instrument for investment purposes, it would be subject to the free movement of capital and payments under Articles 63 – 66 TFEU. While the notion of capital is not defined in the EU primary law, the CJEU has provided some guidance in this matter and stated that investment instruments and securities do fall within its scope.[31] As follows from section 3.1.1 of this master thesis, the EU institutions have refused to accept cryptocurrencies as means of payment and instead, refer to it as means of exchange. However, they have considered that in some cases, especially in terms of ICO, cryptocurrencies may qualify as financial instruments and thus capital.

There are particularly two issues which might pose obstacles. First concern relates to any regulation of blockchain at the EU level – if adopted, it might lead to *de facto* extension of EU law to a global range due to the decentralized nature of blockchain and possible global distribution of nodes within the network. This will be crucial namely with respect to capital and payments, as the freedom of movement encompasses movements to third countries.[32] Secondly, cryptocurrencies might be difficult to balance in terms of competence, as the free movement of capital might clash with monetary policy of eurozone, should one of eurozone Member States accept a cryptocurrency as a legal tender.[33] An ECB representative has expressed doubts in the past stating that only euro can be accepted as legal tender within the eurozone. In this regard, a regulation on the EU level, including legal qualification and delimitation of competences might be appropriate to prevent potential conflicts.

---

[30] See e.g. L. Tichý and coll., op.cit. no. 8, p. 320-328; K. Lenaerts and coll., op. cit. no. 5, p. 202-204.

[31] See J. Snell, op. cit. no. 12, p.447-449; M. Tomášek and coll., op. cit. no. 8, p. 239-240; L. Flynn, *Free movement of capital* in C. Barnard and S. Peers (eds), op. cit. no. 7, p.448-452; R. Schütze, op. cit. no. 7, p. 659-660.

[32] See J. Snell op. cit. no. 12, p. 449, 454-456; M. Tomášek and coll., op. cit. no. 8, p. 239-240; L. Flynn, op. ci. No. 31, p. 454-456.

[33] See K. Darrah, '*Estonia pushes ahead in race to issue first state-backed cryptocurrency*' (2018), available at: https://www.worldfinance.com/markets/estonia-pushes-ahead-in-race-to-issue-first-state-backed-cryptocurrency, last accessed 17. 8. 2017. In relation to the legal tender, within the eurozone, the closest Member State to a state-backed cryptocurrency, and potentially a crypto legal tender, is probably Malta which has already enacted some crypto regulation. Please see section 3.1.5 of this master thesis.

Blockchain-based currency and related payment services can also potentially qualify as services falling under the Articles 56 – 62 of the TFEU.[34] Especially complicated will be the determination of providers of such services[35], given the decentralized nature of the blockchain network. In the event that financial institutions opt for some form of blockchain technology and cryptocurrency, which might be the case especially with respect to closed/permissioned blockchains, the providers using this technology might also wish to enjoy the freedom of establishment under Articles 49 – 55 of the TFEU.[36]

Finally, cryptocurrencies might also be categorized as commodity which would namely entail application of Articles 28 of the TFEU and following provisions ensuring free movement of goods.[37] As cryptocurrencies might share some aspects with commodities, especially gold, prohibition of import and export restrictions under Articles 34 and 35 TFEU would also be applicable, however, it is not entirely clear whether such restrictions would even be technically feasible due to the decentralized nature of cryptocurrencies and the fact that they do not respect geographical borders.

It follows that unless the EU considers blockchain and cryptocurrency a matter falling in the scope of monetary policy of eurozone or common commercial policy, which are both unlikely, the blockchain technology will be a matter of shared, and likely pre-emptive, competence. In accordance with section 3.1.1 of this thesis, it also follows from the approach of the EU institutions which do not seem to express the view that harmonization, let alone unified regulation on the basis of exclusive competence is necessary. Such conclusion, however, is dependent on the fact that no (eurozone) Member State, so far, has tried to claim a cryptocurrency as its legal tender. Given the additional layers which could be built on top of blockchain and cryptocurrency level, such as smart contracts and decentralized applications, it should also be noted that the presented conclusion might differ; the assessment of applicable primary and secondary provisions will be subject to the particular purpose and use of blockchain technology and related instruments (e.g. in respect of intellectual rights, see section 3.2.4 of this thesis).

---

[34] See J. Snell, op. cit. no. 12, p. 450-452; M. Tomášek and coll., op. cit. no. 8, p. 218-221; C. Barnard, J. Snell, *Free movement of legal persons and the provision of services* in C. Barnard and S. Peers (eds), op. cit. no. 7, p. 408-412.

[35] See M. Tomášek and coll., op. cit. no. 8, p. 221.

[36] See J. Snell, op. cit. no. 12, p. 450-452; M. Tomášek and coll., op. cit. no. 8, p. 231-234; C. Barnard, J. Snell, op. cit. no. 34, p. 404-407.

[37] M. Tomášek and coll., op. cit. no. 8, p. 212.

## 2. What is Blockchain and How Does It Work?

Blockchain is a new type of information technology[38], essentially consisting in a *decentralized trustless and transparent public ledger* which records any and all transactions validated by pre-defined consensus among computers participating in the ledger. Many consider blockchain as the new tier Internet[39], in the sense that it provides for a new way of network connection and potential interoperability, allowing open and censor-free access to information to everyone.

Public ledgers are nothing new; humanity has found use for them long before the first computer was invented. Their fundamental purpose is keeping track of information that the society deems important or valuable, namely an individual's rights and/or obligations. Over time, public databases were put in place to record ownership and asset transactions, to register corporations, patents or even domain names. With each public ledger a particular renowned institution was entrusted with its maintenance. Every transaction, i.e. every change of the record had to be wired through this trusted institution in order to ensure the integrity and accuracy of the recorded data. The reason for this is commonly referred to as the *Byzantine General's Problem*[40] which describes a situation where multiple independent persons do not trust each other, nevertheless, must communicate and cooperate towards a common goal. So far, the only way to effectively eliminate possible "treasonous" attacks aiming to disrupt and prevent consensus among independent entities – the generals, has been to cooperate via an independent and generally trusted third person, i.e. a bank, a state body or another kind of institution charged with control and coordination.

Blockchain may eliminate the need for the trusted intermediary. As a decentralized network based on asymmetric cryptography, blockchain ledger is comprised of equal nodes

---

[38] M. Swan, *Blockchain: Blueprint for a New Economy* (1st ed., O'Reilly Media, 2015), p. 92.

[39] Ibid, p. X; A. Wright, P. de Filippi, '*Decentralized Blockchain Technology and the Rise of Lex Cryptographia*' (2015), SSRN [online] available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, p. 18-19, last accessed 19.8.2018.

[40] A. Wright, P. de Filippi, op. cit. no. 39, p. 6: „*This problem questioned how distributed computer systems could reach consensus without relying on a central authority, in such a way that the network of computers could resist an attack from ill-intentioned actors. It posits that three divisions of the Byzantine army are camped outside an enemy city in hopes of conquering it. An independent general commands each division and, in order to plan an attack, they need to decide upon a common course of action. Yet, the generals can only communicate with one another through a messenger, and there is a traitor in the group who is actively trying to prevent the generals from reaching an agreement by either tricking them into attacking prematurely or concealing some relevant information so that the generals cannot plan a coordinated attack.*"

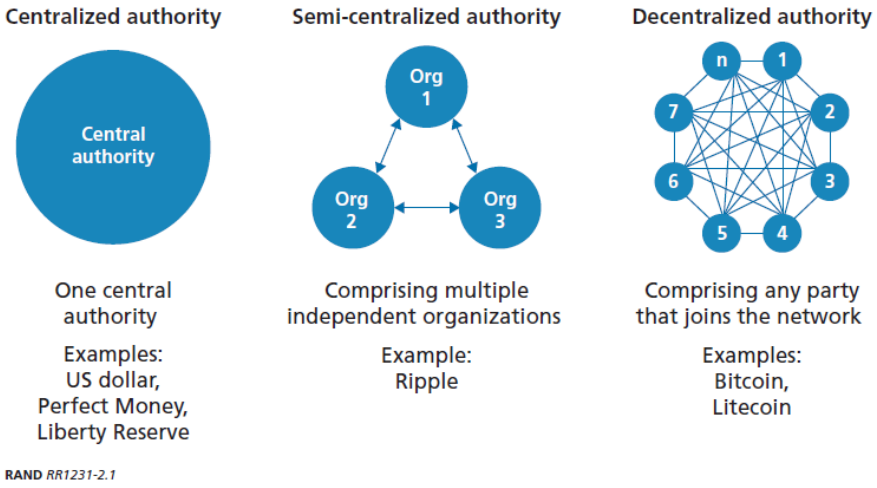
which, while using different methods of validation, verify and approve transactions, record them in a block of transactions and subsequently add the block to the chain in exchange for a reward. To be registered in the ledger of transactions, the transaction needs to be firstly accepted as true and validated by a pre-defined number of remaining nodes of the network. The transaction is true or legitimate, if e.g. "*the request comes from the authorized person, the house seller has not already sold the house, and the buyer has not already spent the money*[41]". For this determination, two major mathematical methods have been developed – the *proof-of-work* and *proof-of-stake*.

After the transaction is recorded in the ledger, it is permanent. Unless some unpredictable and unusual circumstances arise, such as a hacker attack, the data can never be amended or erased from the blockchain ledger. All other nodes in the network use the updated version of the blockchain for verification of new transactions which makes the ledger transparent. Based on blockchain technology, two persons living in different parts of the world who have never met and do not even know each other's names and other information, can safely trade and transfer monetary value in exchange of delivery of goods and services, or any other kind of transaction, without having to rely on any intermediary or centralized institution, e.g. a bank or PayPal. For detailed information relating to the technical features of blockchain transactions, see **Annex I. - Detailed Description of Blockchain Technology** of this thesis.

[41] P. Boucher, S. Nascimento, M. Kritikos, '*How blockchain technology could change our lives*' (2017), EPRS, Scientific Forensic Unit (STOA), p. 5.

*Figure 1* below shows differences between possible network structures.

**Figure 1: Virtual Currencies Have Varied Authority Structures**




*Source: J. Baron, A. O'Mahony, D. Manheim, C. Dion-Schwarz, National implications of Virtual Currency (1st ed., RAND Corporation 2015)*

# 3. Fields of Application of Blockchain Technology on the European Market

## 3.1. Cryptocurrencies and Financial Services

The idea of a decentralized trustless record of transaction information which is shared by everyone was brought forward for the first time in connection with digital currency by Satoshi Nakamoto in his paper from 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*[42]. The mystery behind the author is yet to be solved, even though it is now generally assumed that Satoshi Nakamoto serves as a pseudonym for a group of program developers who brought forth a "blue print" and manual for establishing a digital transaction system with its own digital currency, independent of any of the so-called *fiat currencies*, such as US dollar or euro. As every cryptocurrency, the Bitcoin is based on a blockchain public ledger serving as a platform for running of the Bitcoin protocol where all transactions are recorded for future public inspection. The protocol is essentially software which enables a system for transferring digital cash over the blockchain ledger from one person to another.[43] The third layer of Bitcoin is the currency itself, often shortened as BTC. While Bitcoin has its own blockchain and protocol, some other cryptocurrencies, or alt-coins (i.e. "alternative coins") run on another currency's blockchain and/or protocol. For example, the Counterparty cryptocurrency uses the Bitcoin blockchain ledger which means that all transactions in Counterparty are recorded in the Bitcoin blockchain[44]. This is similar to incorporation of side chains which are also denominated in the currency of the parent blockchain (see section 4.5.4 of this thesis).

Due to the fact that Bitcoin was the first successful cryptocurrency project, and so far, is the most widely accepted and used cryptocurrency, the following description of how the crypto transactions are made is based on the Bitcoin system.

New Bitcoins are generated via so-called mining process during which new transactions are verified and confirmed (see **Annex I. - Detailed Description of Blockchain Technology** and **Annex II. - Cryptocurrencies and Financial Services**). Bitcoin and other similar

[42] S. Nakamoto, '*Bitcoin: A Peer-to-Peer Electronic Cash System*', [2008], [online], available at: https://bitcoin.org/bitcoin.pdf, last accessed 19.8.2018.

[43] M. Swan, op. cit. no. 38, p. 1.

[44] Ibid, p. 2.

cryptocurrencies have been compared to *gold standard*[45], as similarly to gold[46] new Bitcoins have to be "mined" and the supply is not unlimited, as there is no centralized institution, such as a central bank, which would be charged with monetary policy and issuance of new currency. Subsequently, the supply is capped at approximately 21 million of Bitcoins. The Bitcoin protocol was written in such a way that the maximum amount is to be reached by 2140[47]. Nonetheless, the pace with which Bitcoins are mined is decreasing, thus, already almost 17 million Bitcoin units have been mined so far.

Particularly due to the fact that Bitcoin is in some ways similar to gold and its supply cannot be adjusted in case of economic difficulties, consequences such as deflation effects must be taken into account and might be at the root of the question of volatility[48] (see section 4.8 of this thesis). However, it should be emphasized that not all cryptocurrencies have a limited and fixed supply of tokens of value. For instance, Dogecoin does not have a limited amount, while Peercoins amount is flexible – there is a stipulated maximum of 2 billion tokens but if reached, new ones can be issued, as the main focus is maintaining annual inflation rate at 1 %.[49]

One Bitcoin unit consists of subunits called *mBTC* and *Satoshis*. The current value of one Bitcoin is roughly USD 6.5 thousand[50] and the whole Bitcoin market cap is estimated at around USD 110 billion[51]. The volatility of cryptocurrencies has been discussed many times and is subject of section 4.8 of this thesis. For details, especially in regard to merchant and user solutions for acceptance of cryptocurrency, see **Annex II. - Cryptocurrencies and Financial Services**. For information regarding the Ripple protocol, as a representative of semi-centralized cryptocurrency, see **Annex III. – Ripple**.

---

[45] M. Štika, '*Má naprosto svobodná virtuální měna bitcoin místo v právním státě?*' (2017), Bulletin advokacie 5/2018 [online] last accessed 19.8.2018, pp. 29-34; J. Baron, A. O'Mahony, D. Manheim, C. Dion-Schwarz, *National implications of Virtual Currency* (1st ed., RAND Corporation 2015), p. 8; T. I. Kiviat, '*Beyond Bitcoin Issues in Regulating Blockchain Transactions*' (2015), 65 Duke L. J. 569, [online] last accessed 18.2.2018, p. 583.

[46] ECB, '*Virtual Currency Schemes*' (2012), p. 13: Even though cryptocurrencies, same as modern fiat currencies, are not backed by actual gold, there were some exceptions in the past which attempted to link virtual currency to actual reserves of gold, e.g. *e-gold*.

[47] M. Swan, op. cit. no. 38, p. 6.

[48] T. I. Kiviat, op. cit. no. 45, p. 583.

[49] ECB, '*Virtual Currency Schemes – a Further Analysis*' (2015), p. 11.

[50] Data last accessed 20.8.2018.

[51] Data last accessed 20.8.2018. For current information on the price of various cryptocurrencies and state of their markets, please see '*Top 100 Cryptocurrencies By Market Capitalization*', available at: https://coinmarketcap.com/, last accessed 19.8.2018.

Most important aspects of cryptocurrencies are that they are not issued by centralized state authorities, their circulation is voluntary and most importantly, they are not just currencies but a whole transaction and settlement system which is based on decentralization, transparency and immutability. In order to understand cryptocurrencies from the legal point, we first need to consider why they are currently so popular and how they are used. Firstly, blockchain-based currencies and systems are used by general public as payment instruments for purchase of goods and services. Cryptocurrency options are increasingly offered namely in eCommerce markets (e.g. check-out process of eShops), however, solutions for non-remote retail markets are also becoming more widespread, as an example of which might serve popular Bitcoin cafés. Secondly, Bitcoins and other cryptocurrencies are largely exchanged and traded in marketplaces called exchanges, either for fiat currencies, or for other cryptocurrencies. In that regard, they might be subject of speculation due to the volatility of the market. And lastly, cryptocurrencies might also interfere with financial and capital markets with introduction of ICOs and derivates based on cryptocurrencies.

Many experts[52] have pondered about the reasons and causes of creation of cryptocurrencies. Currently, most of them come to the conclusion that one of the major reasons was the financial crisis in 2008 started by the bankruptcy of the Lehman Brothers Holdings inc. in the US and the following chain failure of global financial system and arising frustration of general public with monetary instruments and decisions of central banks around the world and other government authorities as a reaction to the crisis. While cryptocurrencies represent an exciting novelty for companies and investors in terms of new ways of investment, as will be discussed below, it must be stressed that average consumers called for change in monetary and payment affairs as well. The frustration of the general public with centralized authorities which required trust and were necessary for every transaction while imposing high fees and leaving little to no control to consumers themselves was likely at the root of ideas leading to the cryptocurrency concept based on peer-to-peer decentralization, traceability, immutability, lack of government control and most importantly, no trust. The

[52] A. Vondráčková, '*Regulation of Virtual Currency in the European Union*' (2016), Prague Law Working Papers Series, 2016/III/3, p. 2; A. Felländer, S. Siri and R. Teigland: '*The three phases of FinTech*' in R. Teigland, S. Siri, A. Larsson, A. M. Puertas, C. I. Bogusz (eds), *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond* (1st ed., Routledge, 2018), pp. 155-157; L. Němec, '*K právní regulaci kryptoměn, díl I*.' (2018), Právní rádce [online], available here: http://www.glatzova.com/k-pravni-regulaci-kryptomen-dil-i/, last accessed 19.8.2018.

only trust incorporated was the trust of users that the currency will prevail and will be tradable in future. Another key factor seems to be the increase of so-called strong and thriving virtual communities thanks to the strong presence of Internet, namely in connection with online games or social media.[53] Thus from the first glance, with Bitcoin manifesto a global private currency was created which was to escape the grasp of any and all world governments.

### 3.1.1. *Legal Definition and Regulation of Cryptocurrencies at the European Level*

Cryptocurrencies are likely to be considered digital cash but they might not be considered a currency/legal tender from the legal point of view. Namely, "*money is an economic category, as the currency is a legal category. So that money can be labeled a currency, it must be acknowledged as such by an authority (usually by the state), which specifies the form of the money and determines the precise conditions under which the currency is used*."[54] In case of cryptocurrencies, there is no such authority – could cryptocurrencies still be considered currency? It seems that at the EU level the conclusion is firmly negative, cryptocurrencies cannot be considered currencies. Yves Mersch, Member of the Executive Board of the ECB, supported this conclusion in May 2018 by stating that "*it is very clear that [virtual currencies] currently do not fulfill the three basic functions of money: they are inefficient media of exchange, poor stores of value and are not used as units of account*."[55]

The first EU institution to publish an opinion regarding cryptocurrencies was the **ECB** in 2012 in which it set forth a definition of virtual currencies as "*a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*".[56] Although the ECB later modified its definition, at that time, it viewed virtual currencies as a marginal system applied only "*within a narrow group of people*".[57] The ECB further specified that it recognized 3 types of virtual

[53] ECB (2012), op. cit. no. 46, p. 12: "*In some cases, these virtual communities have created and circulated their own digital currency for exchanging the goods and services they offer, thereby creating a new form of digital money*."

[54] A. Vondráčková, op. cit. no. 52, p. 1.

[55] See '*Virtual currencies ante portas*' by Yves Mersch, Member of the Executive Board of the ECB at the 39th meeting of the Governor's Club Bodrum, Turkey, 14 May 2018, available at: https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en.html, last accessed 19.8.2018.

[56] ECB (2012), op. cit. no. 46, p. 13.

[57] A. Vondráčková, op. cit. no. 52, p. 7.

currencies in total where the third type allowing "bidirectional flow" (i.e. exchange of fiat currency for virtual currency and *vice versa*) is what we generally know cryptocurrencies to be today.[58] While the ECB admitted that virtual currencies might under certain circumstances entail some considerable risks for central banks, namely in respect of (i) price stability[59], (ii) financial stability, (iii) payment system stability and (iv) reputation[60], it ruled out any serious implications based on the small significance of virtual financial markets. In the end, the ECB stressed that even though virtual currencies are used in exchange for goods and services, they could not be regarded as money and/or currency, nor do they fulfill the definition criteria of e-money (i.e. essentially state currency in electronic/digital form) and thus, could not be covered by the e-money Directive.[61] That is specifically due to article 11(2) which states: "*Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held*." As the ECB points out, this cannot be fulfilled in distributed transaction systems, such as Bitcoin. Firstly, Bitcoins are not issued in exchange for currency but created by mining. And secondly, their value depends on the state of the market and demand for Bitcoins.[62]

In its report from 2015 the ECB modified its definition of virtual currencies and removed certain inaccuracies: "*virtual currency [is] a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money*."[63] However, despite this rather liberal

---

[58] ECB (2012), op. cit. no. 46, p. 14.

[59] In this regard, the ECB acknowledged an interesting, while nowadays rather unlikely scenario which could theoretically arise, provided that namely the volatility of cryptocurrency is solved. "*In an extreme case, virtual currencies could have a substitution effect on central bank money if they become widely accepted. The increase in the use of virtual money might lead to a decrease in the use of 'real' money, thereby also reducing the cash needed to conduct the transactions generated by nominal income. In this regard, a widespread substitution of central bank money by privately-issued virtual currency could significantly reduce the size of central banks' balance sheets, and thus also their ability to influence the short-term interest rates. Central banks would need to look at their existing tools to deal with this risk (for instance, trying to impose minimum reserve requirements on virtual currency schemes).*" See ECB (2012), op. cit. no. 46, p. 35.

[60] The reputation risks are connected to the possibility that citizens might come to the conclusion that potential failures relating to cryptocurrencies are responsibilities of central banks due to their similarity with retail payments.

[61] 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, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110.

[62] S. Kasiyanto, '*Regulating Peer-to-Peer Network Currency: Lessons from Napster and Payment Systems*' (2015), Journal of Law, Technology and Public Policy, Vol. 1 No. 2, 40, p. 67.

[63] ECB (2015), op. cit. no. 49, p. 26.

definition, the ECB firmly repeated its conclusion that cryptocurrencies are not to be considered a currency or payment instrument and thus fall out of the scope of supervision and control of the ECB, thereby leaving their regulation to Member States.

In 2017, an additional report confirmed its stance that cryptocurrencies are currently not regulated at the EU level[64] and focused more on different approaches of Member States and other jurisdictions and additional technologies built on blockchain, e.g., smart contracts.

The **EBA** was the second European institution to focus on cryptocurrencies. Firstly, it issued a warning to consumers in 2013[65] where it emphasized risks related to trade of cryptocurrencies and secondly, in 2014 it issued a full report. In the report, the EBA provided a definition of virtual currencies which largely influenced the ECB's improved definition from 2015. Further, the EBA also concurred that although virtual currencies represent a "medium of exchange", they are not payment instruments, currencies[66] or legal tenders[67], at least within the EU.[68] Apart from determining the risks of trading with cryptocurrencies for users, regulators and other participants, the EBA strongly recommended regulation of cryptocurrencies and that "*national supervisory authorities discourage credit institutions, payment institutions, and e-money institutions from buying, holding or selling [virtual currencies], thereby 'shielding' regulated financial services from [virtual currencies]*."[69] What is particularly interesting, as the EBA pointed out, all main advantages that are so closely linked to cryptocurrencies, namely in regard to low transaction fees and shorter processing time, are less significant for EU citizens due to the well functioning framework of SEPA area[70] which will be elaborated on below. Therefore, such "*benefits are likely to materialize outside the EU, in regions where the payment infrastructure may be less developed or less trustworthy*."[71]

---

[64] ATHANASSIOU, Phoebus, '*Legal Working Paper Series: Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks*' (2017), European Central Bank, No 16/October 2017, p. 12.

[65] EBA, '*Warning to consumers on virtual currencies*' (2013), EBA/WRG/2013/01.

[66] EBA '*EBA Opinion on 'virtual currencies''* (2014), EBA/Op/2014/08, p. 12.

[67] Ibid, p. 13.

[68] This is to distinguish from cryptocurrencies backed or adopted by state for whichever reasons. An example might be the cryptocurrency issued by Venezuela in an attempt to decrease hyperinflation which is currently destroying their economy.

[69] Ibid, p. 44.

[70] Ibid, pp. 17-18.

[71] Ibid, p. 20.

Finally, the EBA also called for inclusion of crypto-exchanges and providers of eWallets into the scope of obliged persons under the anti-money laundering legal framework in the EU level (further elaborated on in the section on illicit behavior in relation to cryptocurrencies, please see 4.7 of this thesis). Consequently, these entities providing crypto-related services were indeed included in the scope of the obliged persons by the adoption of the fifth AML Directive[72] which entered into force on 9 July 2018. The fifth AML Directive is now the first European legal regulation which defines virtual currencies, as follows: "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*."

The firm conclusion that cryptocurrencies are not currencies or money at the EU level might be in contradiction with the opinion and interpretation of the **CJEU**. In its judgment *Hedqvist*[73] its main focus was the determination whether cryptocurrencies should be exempt from VAT (for the taxation issue, please see section 3.1.6 of this thesis). The CJEU eliminates the possibility that Bitcoin could be regarded as a form of e-money or security. Further, it comes to the conclusion that Bitcoin is a non-traditional currency but currency nonetheless whose sole purpose is to be a means of payment and accepts that parties may choose it as an alternative to legal tender.[74] However, it should be noted that it this judgment the CJEU considered provision of exchange services only in the bidirectional sense, i.e. cryptocurrency for fiat currency and vice versa. It remains to be seen whether the same approach would hold in case of purely crypto-transactions (cryptocurrency for cryptocurrency).

Among other EU authorities which expressed their opinion on cryptocurrencies was also the European Parliament which called for close monitoring of future development of this area, EP's Committee on Economic and Monetary Affairs, the European Parliamentary Research Service or European Commission.

---

[72] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843.

[73] Case C-264/14 *Hedqvist* [2015] ECLI:EU:C:2015:718.

[74] In particular, see paragraph 49 of the judgment. Authors of the ECB (2017) report, op. cit. no. 64, come to the same conclusion, i.e. that the CJEU takes a more liberal approach and regards cryptocurrency as currency, for further details please see page 19 of the report.

It should be pointed out that despite EBA's recommendation to discourage closer cooperation and interest of banks and financial institutions with virtual currencies, recent development shows that there are authorized and regulated banks in the EU willing to support or implement blockchain solutions. In 2013 a partnership between an international cryptocurrency exchange *Kraken* and German internet-based *Fidor Bank* specialized in innovative banking services was announced.[75] Another example might be a major Dutch bank called *Rabobank* which is reportedly considering acquiring an eWallet solution and offering their customers to access their fiat and cryptocurrencies within one bank account.[76] Moreover, certain banks based in Lichtenstein and Switzerland have already decided to offer trading and investment in cryptocurrencies. The Lichtenstein Bank *Frick* has opted for *cold wallets* which ensure offline storing of private keys, therefore, mitigating the potential hacker attack risk.[77]

There are currently three possible approaches of regulatory development[78]: (i) complete prohibition, (ii) government regulation, or (iii) provided that crucial aspects are regulated, such as AML, self-regulation, i.e. *laissez-faire*. Assuming that the first possibility is a solution *ultima ratio* in developed countries, it will not be further assessed. The camp supporting the second option calls for complete and specific regulation targeted at these systems which would set down particular requirements in terms of financial stability, security, etc. This group is especially supported by security experts and risk analytics.[79] While the EBA strongly supported this opinion in 2014, it should be emphasized that the above mentioned recommendations of the EBA were specifically referred to as immediate regulatory response until the issue is settled and a regime is agreed upon.[80] The advantage of this approach would

[75] Even though the aim of this partnership was limited to enabling safe trading of cryptocurrencies and payment services to customers, the *Fidor Bank* still represents the first cryptocurrency bank, namely in the European market and subject to German regulation. See A. Miyaguchi, '*Kraken.com to Offer Digital Currency Trading in Exclusive EU Partnership with Fidor Bank AG*' (2013), available at: http://www.prweb.com/releases/2013/10/prweb11211586.htm, last accessed 19.8.2018 and D. Cordell, '*Fidor Bank Partners with Kraken to Create Cryptocurrency Bank*' (2014), available at: https://www.ccn.com/fidor-bank-partners-kraken-create-cryptocurrency-bank/, last accessed 19.8.2018.

[76] G. Prisco, '*A Major Dutch Bank Is Considering a Cryptocurrency Wallet for Its Customers*' (2018), available at: https://bitcoinmagazine.com/articles/major-dutch-bank-considering-cryptocurrency-wallet-its-customers/, last accessed 19.8.2018.

[77] W. Zhao, '*Lichtenstein Bank Opens Up Cryptocurrency Investment for Clients'* (2018), available at: https://www.coindesk.com/liechtenstein-bank-opens-up-cryptocurrency-investment-for-clients/, last accessed 19.8.2018.

[78] S. Kasiyanto, op. cit. no. 62, p. 45.

[79] M. Szczepański, '*Bitcoin: Market, economics and regulation*' (2014), EPRS, p. 7.

[80] EBA (2014), op. cit. no. 66, p. 44.

be a unified front and harmonization which would exclude deformation of the internal market and "*shopping for the most convenient approach*"[81] within the EU.

The third group advocates for a rather liberal approach in the sense that submitting cryptocurrencies to the scope of anti-money laundering and payment frameworks stipulated by European legislation but carried out with slight differences at the national level, might be sufficient.[82] One of the main reasons for the conclusion which seems to be in line with the interpretation and recommendation of the ECB would be that distributed transaction systems are in many way very similar to traditional payment and financial systems. Therefore, should the regulation of these new systems be strikingly different, it might lead to distortion of competition.[83]

### 3.1.2. *Legal Definition and Regulation at National Levels*

In this section it will be briefly discussed how cryptocurrencies are viewed in certain individual jurisdictions within and outside the EU[84]. Many financial experts have stated that Bitcoin and other similar cryptocurrency schemes have the features of currency and commodity as well.[85] From the survey conducted in June 2018 it follows that there are four major approaches relating to qualification of cryptocurrencies that Member States take.

(i) Some Member States have expressed an opinion according to which they consider cryptocurrencies commodities. This group of states includes Austria and the Czech Republic.[86]

(ii) Other Member States, such as Latvia, Slovakia, Italy or Germany (Germany defines cryptocurrencies as "units of account") qualify them as financial instruments.[87]

---

[81] Ibid, p. 44.

[82] M. Szczepański, op. cit. no. 79, p. 7.

[83] EBA (2014), op. cit. no. 66, p. 37.

[84] The overview is mostly based on '*Regulation of Cryptocurrency Around the World*' (2018), The Law Library of Congress, Global Legal Research Center.

[85] M. Szczepański, op. cit. no. 79, p. 7.

[86] '*Regulation of Cryptocurrency Around the World*' (2018), The Law Library of Congress, Global Legal Research Center, pp 30-34.

[87] Ibid, pp 40-42, 44, 45, 54.

(iii) A couple of Member States apply a more lenient regime and either explicitly or implicitly treat cryptocurrencies as money and/or currency, for instance Luxembourg or Malta.[88]

(iv) The majority of Member States, however, take a rather passive approach in line with interpretations of the ECB and EBA. Some of them only warn consumers and state that cryptocurrencies are not regulated (Slovenia, Greece)[89]. Others explicitly stipulate that cryptocurrencies cannot be regarded as money/currency and legal tender without providing additional positive definitions (Belgium, Poland[90]).

In terms of jurisdictions outside the EU and their qualification of cryptocurrencies, the following states will be assessed: China, Japan, Canada and USA.

Chinese regulators have stated that cryptocurrencies were a "special virtual commodity". Due to their statement that cryptocurrencies were not currencies and were not to be used and circulated as such and subsequent prohibition of ICOs, China *de facto* banned cryptocurrencies altogether.[91]

Japan, a representative of a more liberal jurisdiction, has defined cryptocurrency as a "property value" and enacted a regulation package, including an amendment to Payment Services Act which imposes registration and other requirements on exchanges.[92]

Canada allows the use of cryptocurrencies on its territory, however, expressly states that they are not considered currency or legal tender, even though the Canadian law on anti-money laundering qualifies virtual currencies as "***money*** service businesses".[93]

In the USA, the regulation of cryptocurrencies is not exclusive to the federal level, thus individual states' authorities may contribute and enact their own definitions and regulations (e.g. Arizona, Delaware, New York), although federal regulation is in preparations. Many federal bodies have issued their opinions which, however, substantially differ and consensus

[88] Ibid, pp 46-50.

[89] Ibid, pp 42, 54.

[90] Ibid, pp 31-32, 52.

[91] Ibid, pp 106-107.

[92] Ibid, pp 111-113.

[93] Ibid. pp 10-12.

regarding legal nature and definition of cryptocurrencies has not yet been reached. Some of these authorities have considered cryptocurrencies as securities, some as commodities and some as money/currency[94] (to this regard, even the Supreme Court indicated that interpretation of money might need to be extended[95]).

In regard to the legal status of cryptocurrencies around the world, it is also necessary to note that there are jurisdictions which completely ban their usage and trade on their territory. Countries imposing absolute ban include United Arab Emirates, Egypt or Bolivia. In other states, the factual ban follows only implicitly from their respective regulatory framework – Colombia, Saudi Arabia but also for example China.[96]

### 3.1.3. *State-Backed Cryptocurrency*

While some countries have rigorously expressed their disapproval with potential state backed cryptocurrency development (e.g., Denmark), others are seriously considering it and there might be quite a few reasons for it. Firstly, it would enable central banks and other supervisory authorities to test different regulatory approaches and familiarize themselves with the inner workings of cryptocurrencies and their markets.

Secondly, in a hypothetical case where cryptocurrencies *de facto* become direct competition to legal tenders in terms of circulation, a cryptocurrency recognized as a legal tender would ensure stability. Simultaneously, central banks would feel more comfortable with accepting a crypto legal tender that they have designed or at least have some control over its development. State cryptocurrency might lead to deeper understanding, invention of solutions for blockchain issues which are currently unacceptable for most jurisdictions and all in all might also attract developers and investors.

Malta is among countries considering "*introducing its own cryptocurrency within a 'controlled framework'*" with the goal to test its newest crypto-regulatory package.[97]

---

[94] Please see S. Stankovic, '*US Cryptocurrency Regulation: Policies, Regimes & More*' (2018), available at: https://unblock.net/us-cryptocurrency-regulation/#h3, last accessed 19.8.2018.

[95] Please see P. Farquhar, '*The US Supreme Court just spoke about a Bitcoin future for the first time*' (2018), available at: https://www.businessinsider.com.au/the-us-supreme-court-just-spoke-about-a-bitcoin-future-for-the-first-time-2018-6, last accessed 19.8.2018.

[96] '*Regulation of Cryptocurrency Around the World*' (2018), op. cit. no. 84.

[97] '*Regulation of Cryptocurrency Around the World*' (2018), op. cit. no. 84, p. 49.

Similarly, Bahamas, namely, Grand Bahama Island, wishes to establish itself as a "*digital hub*" with its own cryptocurrency. More importantly, due to the fact that Bahamian dollar is pegged to the USD, potential Bahaman cryptocurrency might give them more monetary and economic freedom.[98]

Within Europe, Sweden and Switzerland are among countries considering to develop their cryptocurrencies serving as legal tenders, e-krona[99] and e-franc[100] respectively. Similar projects are in progress in Estonia (Estcoin)[101] or UK (RSCoin)[102]. However, should an EU Member State in fact proceed with establishment of cryptocurrency as a legal tender, it might face some challenges in terms of EU institutions and eurozone.[103]

Cryptocurrencies may also help developing countries or countries hit by a catastrophe resulting in instability, depreciation of hyperinflation of their currency. Nonetheless, it can also be used to deflect negative economic effects legally inflicted as sanctions, for example embargos. In the end of 2017 Venezuela became infamous as one of the first countries in the world to declare that it will establish its own cryptocurrency – *petro* – and to go even further Venezuelan government stated that it would be backed by their national oil reserves. Venezuelan economy is currently suffering extreme hyperinflation mainly due to sanctions imposed by the US government.[104] Despite following controversies caused by Venezuelan Parliament's declaration that the cryptocurrency is illegal and cannot be backed by oil reserves, *petro* is supposed to become a legal tender by the end of 2018 and Venezuelan

---

[98] J. McMahon, '*Bahamas is Launching a State Backed Cryptocurrency, is it Legitimate?*' (2018), available at: https://www.newsbtc.com/2018/06/25/bahamas-launching-state-backed-cryptocurrency-legitimate/, last accessed 19.8.2018.

[99] A. Fellënder and coll., op. cit. no. 52, pp 161-162.

[100] C. E. Kelso, '*Switzerland Formally Considers State Backed Cryptocurrency*' (2018), available at: https://news.bitcoin.com/switzerland-formally-considers-state-backed-cryptocurrency/, last accessed 19.8.2018.

[101] J. Liebkind, '*Estonia is Pushing for State-Backed Cryptocurrency*' (2018), available at: https://www.investopedia.com/news/estonia-pushing-statebacked-cryptocurrency/, last accessed 19.8.2018.

[102] A.M. Puertas, R. Teigland, '*Blockchain: The Internet of Value*' in R. Teigland and coll. (eds) op. cit. no. 52, pp 287-288.

[103] In September 2017, Mario Draghi, President of the ECB reportedly stated that "*No Member State can introduce its own currency; the currency of the eurozone is the euro.*" See K. Darrah, op. cit. no. 33, available at: https://www.worldfinance.com/markets/estonia-pushes-ahead-in-race-to-issue-first-state-backed-cryptocurrency.

[104] While the sanctions were reportedly firstly imposed as a consequence of inhumane treatment of Venezuelan protesters in 2014, US-Venezuelan relations have a long and hostile history and other factors might have influenced the current state of Venezuelan economy. For more details on Venezuelan crisis and how cryptocurrency may help, see K. B. II Haesly, '*How to Solve a Problem Like Venezuela: An argument for Virtual Currency*' (2016), 22 Law & Bus. Rev. Am. 261.

government is trying to provide incentives in order to ensure wide adoption among Venezuelan people.[105]

Another famous case of attempt at national cryptocurrency relates to Auroracoin, an altcoin established by private persons in Iceland with the goal to overcome strict monetary policy resulting from the 2008 financial crisis, namely in respect of stricter currency convertibility.[106] The founders gave away Auroracoins to every person registered in the Iceland's national ID database, however, probably due to the controversial status in terms of legality and negative statements from Icelandic political representatives, the Auroracoin project failed as the value plummeted.

Similarly, Scot-coin was created with intention to become a new Scottish legal tender which might become of crucial importance, should Scotland decide to leave the UK after Brexit.[107]

### 3.1.4. *Initial Coin Offering*

In recent years many centralized platforms for crowdfunding were introduced and quickly became popular, with the purpose of finding investors to back usually a controversial or risky idea. The underlying principle of platforms, such as Kickstarter or GoFundMe, is to accumulate smaller donations from individuals interested in the project while diluting the degree of risk depending on the number of participating individuals. In exchange for a donation, the "investor" is then given certain advantage relating to the project, the extent of which is directly dependant on the amount of the donation. The main difference between crowdfunding and stock investment is that crowd-funders are usually in a position of donators. Not often do they get equivalent value in return for their donation. However, there is a possibility to acquire something similar to shares of the startup company via crowdfunding, or more precisely crowdinvesting campaign, which makes the funding much more similar to actual stock investment but without the mandatory regulation. Furthermore, other differences include higher risk, as the percentage of success of crowdfunded companies is much lower

[105] '*Regulation of Cryptocurrency Around the World*' (2018), op. cit. no. 84, pp 17-18.

[106] J. Biggs, '*As Auroracoin "Airdrop" Approaches, What Does It Mean When A Nation Adopts A Cryptocurrency?*' (2014), available at: https://techcrunch.com/2014/03/01/as-auroracoin-airdrop-approaches-what-does-it-mean-when-a-nation-adopts-a-cryptocurrency/?guccounter=1, last accessed 19.8.2018.

[107] J. Baron and coll., op. cit. no. 45, p. 20.

than that of companies with regulated share exchange. Lastly, there is usually no option of dividends for investors participating in crowdfunding.

For this model to work, a certain degree of trust towards the fundraising organization, i.e. the platform, is necessary, similarly to regulated stock exchange investment. With application of blockchain, this need for trust can be eliminated and peer-to-peer investment can be further improved. "*Blockchain-based crowdfunding platforms make it possible for startups to raise funds by creating their own digital currencies and selling 'cryptographic shares' to early backers*." [108] The shares are thus represented by the amount of crypto-tokens.

The above mentioned blockchain-based crowdfunding campaigns are commonly referred to as **ICO**, initial coin offering in analogy of initial public offering (i.e. a first offer of company's shares to public, usually via a regulated stock exchange). The process is similar, the company's representatives present a project which they require funding for and interested investors buy the company's cryptocurrency in hopes that the value of the obtained shares increases in time and they can make profit by selling it. Due to the fact that investors of decentralized campaigns obtain certain value in exchange immediately, the fundraisers are referred to as crowdsales. The increasing significance that ICOs have attained can be shown by recent statistics, according to which ICO campaigns have raised 45 % of the amount raised by traditional IPOs in the second quarter of 2018.[109]

Nonetheless, it is evident that such mechanism may violate many national and European regulations which are put in place in order to protect consumers from illicit investment projects. Potential triggering of stock investment regulations depends on determination whether the cryptocurrency falls in the scope of financial instrument. As follows from the above mentioned, EU institutions largely leave that determination to Member States and do not provide a clear answer.[110] Subsequently, qualification differs across individual jurisdictions. Some Member States, such as Latvia, Slovakia, Italy or Germany have declared that they view cryptocurrencies as financial instruments.[111] In such a case, ICOs taking place

[108] M. Swan, op. cit. no. 38, p. 12.

[109] C. Long, '*ICOs Were 45% Of IPOs in Q2 2018, As Cryptos Disrupt Investment Banks*' (2018), available at: https://www.forbes.com/sites/caitlinlong/2018/07/22/icos-were-45-of-ipos-in-q2-2018-as-cryptos-disrupt-investment-banks/, last accessed 19.8.2018.

[110] P. Athanassiou (ECB 2017), op. cit. no. 64, p. 17.

[111] '*Regulation of Cryptocurrency Around the World*' (2018), op. cit. no. 84.

within their jurisdiction will trigger some statutory requirements. In line with the **ESMA**'s statement from 2017, entities participating in the ICO could potentially be involved in placing, dealing in or advising on financial instruments which are all regulated investment activities under the MiFID II package applicable from January 2018[112] and thus, are subject to authorization obligation. According to ESMA, "*the organization requirements, the conduct of business rules and the transparency requirements laid down in MiFID would then apply, depending in some cases on the services provided*." [113]

In the event that the cryptocurrency subject to an ICO meets the definition criteria of transferable securities[114] (particularly if shares in the issuing company are offered in exchange), additional statutory obligations may apply, namely the provision of required scope of information by way of prospectus in line with the Prospectus Directive[115]. This minimal scope of information shall include the identity of the "*issuer, the offeror, the party seeking admission to trading or the guarantor*".[116]

Finally, due to the fact that ICO organizers collect funds from the general public and apply their own rules, this activity might be categorized as "*[raising] capital from a number of investors, with a view to investing it in accordance with a defined investment policy*"[117] and as such, might qualify them as managers of alternative investment funds under the AIFM

[112] The MiFID II package comprises of a Directive and complementing Regulation, in particular, Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on market in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, full text available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014L0065 and Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0600.

[113] ESMA, '*ESMA alerts firms involved in Initial Coin Offering (ICOs) to the need to meet relevant regulatory requirements*' (2017), ESMA50-157-828.

[114] The MiFID defines transferable securities as „*those classes of securities which are negotiable on the capital market, with the exception of instruments of payment, such as: (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares; (b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities; (c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities currencies interest rates or yields, commodities or other indices or measures.*"

[115] Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003L0071.

[116] ESMA (2017) firms, op. cit. no. 112.

[117] Ibid.

Directive.[118] In such a case, they would need to comply with information, capital, operational and organizational obligations. Please note that application of AMLD is assessed separately in section 4.7 of this thesis.

Some other Member States have stated in relation to ICOs that they will assess legal nature and applicable obligations relating to ICOs on a case-by-case basis. Among these states are for instance the Netherlands, Lithuania, Ireland or Germany. Depending on the qualification of individual Member States, issuers of cryptocurrencies in terms of ICO might also be subject to authorization obligations. As was described above, Malta is introducing a regulatory package for cryptocurrencies. Interestingly, part of the proposed framework is a "financial instrument test" which shall help determining whether a cryptocurrency and an ICO fulfill the definition of a financial instrument and consequently, what regulatory requirements should apply.[119]

Nevertheless, the situation is a bit different for derivates based on cryptocurrencies. Based on ESMA's interpretation[120] these shall generally be considered as financial instruments, without the necessity for further assessment. The derivates may include namely cryptocurrency futures, cryptocurrency contracts for differences (CFDs) and cryptocurrency options.[121]

For the sake of completeness, it should be noted that apart from the warning to ICO issuers, ESMA has also issued a number of warnings to consumers in which it has emphasized particularly inadequate scope of provided information, instability of market and scarce exit options.[122]

Outside of the EU, some jurisdictions like China in 2017, have decided to ban ICOs completely, particularly due to doubts concerning protection of investors who are generally

[118] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0061.

[119] '*Regulation of Cryptocurrency Around the World*' (2018), op. cit. no. 84, p. 49.

[120] ESMA, '*ESMA alerts firms involved in Initial Coin Offering (ICOs) to the need to meet relevant regulatory requirements*' (2017), ESMA50-157-828.

[121] Financial Conduct Authority, '*FCA statement on the requirement for firms offering cryptocurrency to be authorised*' (2018), [online] available at: https://www.fca.org.uk/news/statements/cryptocurrency-derivatives, last accessed 19.8.2018.

[122] ESMA, '*ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs)*' (2017), ESMA50-157-829; ESMA, EBA and EIOPA, '*ESMA, EBA AND EIOPA warn consumers on the risks of Virtual Currencies*' [2018], available at: https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies, last accessed 10.8.2018.

not professionals. Some decentralized crowdsale platforms have tried to bypass the regulation and bans by way of approximating their activity more to crowdfunding platforms in the sense that they have tried to sell "*non-share items, such as early access to software. However, this is somewhat disingenuous because in many cases the market still looks a lot like selling shares. The result is that there can be de facto investors in cryptocurrency projects who are not getting much more than early access to open source software*."[123]

### 3.1.5. *Payment Services and Regulation*

Blockchain technology is among inventions and technologies which are highly interesting and developed in the FinTech sector. FinTech sector relates to companies which develop new solutions with the aim to innovate and improve financial and payment services, namely in the retail sector, and potentially, to dilute the high concentration of power which is currently given to financial institutions as authorized providers. This sector has been historically highly concentrated especially due to market barriers, whether due to regulatory/authorization requirements, or "*infrastructure, asymmetric information, the cost of holding capital, the ability to manage large capital flows, and low transparency.*"[124]

While decentralized transaction systems share many features with traditional retail payment systems, particularly e-money, they differ in some aspects. As was stated above, they lack supervision (no centralized authority), mostly also regulation and offer instant global coverage.[125] In respect of payment services, two major advantages that decentralized systems bring and that potentially may create competition for traditional payment systems are low transaction fees and shorter processing time.

As was elaborated by the EBA, "*although reliable and independent data on the exact costs of [virtual currencies] transactions is difficult to ascertain, some anecdotal suggestions have been made that average transaction fees on the Bitcoin network tend to be less than 0,0005 BTC, or 1 % of the transaction amount*." And continues: "*this compares with 2 % - 4 % for traditional online payment systems or an estimated 8 % - 9 % for remittance without involving bank accounts via money transmitters*."[126] The EBA is of the opinion that one of the

[123] M. Swan, op. cit. no 38, p. 13.

[124] A. Fällander and coll., op. cit. no. 52, p. 155.

[125] S. Kasiyanto, op. cit. no. 62, p. 20.

[126] EBA (2014), op. cit. no. 66, p. 14.

main factors responsible for this difference is that distributed transaction systems do not have to include costs incurred in security and compliance matters and further states that advantages relating to low transaction fees are much less significant for European citizens due to well-functioning SEPA project.[127] While it is true that thanks to SEPA, transaction fees for wire transfers in euro have considerably decreased, it should be emphasized that cryptocurrencies have the potential to go much further. Firstly, they are not limited to one currency, unlike SEPA and secondly, apart from transaction and eWallet fees, there are no other fees related to payment services. Therefore, many charges and levies currently imposed by financial institutions, such as account-holding fee, credit card related fees, wire transfer related fees and limitations, etc are non-existent in the crypto-world. Furthermore, as ECB[128] and EBA[129] concur, the economic potential grows if we take into account international payments[130] where banks attempt to transfer payments via the shortest route within the SWIFT system but impose high fees and require long processing time. Several days which are usually required for clearing and settlement of large transactions can be shortened to minutes or hours (depending whether we include verification time) on business days *and* weekends.

On the other hand, materialization of above mentioned advantages might be hindered due to consumer protection. Many of consumer risks follow from the fact that blockchain-based technologies are not yet mainstream and require a certain degree of IT knowledge.[131] Furthermore, even if a consumer is a victim of illicit behavior, due to the setting of system, it might be difficult to ascertain evidence.[132] To provide a concrete example, the immutability as a key aspect might also pose a problem under consumer legislation, in particular, once a transaction has been confirmed and added to the chain, it cannot be cancelled which is in contradiction with current consumer protection legislation that allows consumers to cancel a

[127] EBA (2014), op. cit. no. 66, pp 16-17.

[128] ECB (2015), op. cit. no. 49, p. 19.

[129] Ibid, p. 17.

[130] A. M. Puertas, R. Teigland, op. cit. no 101, p. 284: "*International money transfers are ineffective, slow, and complex, while domestic payments are rather efficient. For that reason, in the short term, the blockchain is expected to have a significant impact on international transfers by offering quick net gains though cost savings, whereas it will take longer to impact domestic payments.*"

[131] S. Kasiyanto, op. cit. no. 62, p. 43.

[132] Ibid, pp 69-70.

payment transaction. Should a reason for cancellation occur, a refund would depend on the merchant's good will.[133]

Consumer protection is why some think that decentralized transaction systems should be regulated to ensure that they fulfill the same requirements as other payment systems. Another reason is that until decentralized transaction systems are somewhat regulated, due to the lack of any centralized authority, state authorities, such as law enforcement bodies but also certified enforcement agents/bailiffs do not have any legal actions at their disposal to interfere with individual's crypto-resources without his or her permission. For instance, potential enforcement of court order to freeze assets including cryptocurrency may be very complicated or even impossible.[134] The principal reason against this opinion is that decentralized transaction systems are simply not yet big enough in terms of transacted mass.[135]

Potential application of currently available legal framework relating to payment services faces a number of obstacles. PSD2 Directive[136] which regulates provision of retail payment services within the EU market defines obliged entities as payment service providers the categories of which are enumerated in Article 1(1): (i) credit institutions, (ii) electronic money institutions, (iii) post office giro institutions, (iv) payment institutions, (v) the ECB and national central banks and (vi) Member States and their authorities. As follows from the ECB's opinion[137] decentralized blockchain-based systems are not likely to fall in the scope of the e-money directive as cryptocurrencies cannot be considered e-money. That leaves only one potential group of obliged entities – payment institutions. These are defined in Article 4(4) as "*a legal person that has been granted authorization in accordance with Article 11 to provide and execute payment services throughout the Union*." Among these services which are defined in Annex I of the PSD2, is also execution of transactions. A payment transaction is then defined in Article 4(5) as "*an act initiated by the payer or on his behalf or by the payee, of placing transferring or withdrawing funds, irrespective of any underlying*

[133] EBA (2014), op. cit. no. 66, p. 18.

[134] M. Štika, op. cit. no 45; S: Kasiyanto, op. cit. no 62, p. 43.

[135] See cited reports of ECB and EBA.

[136] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

[137] ECB (2012), op. cit. no. 46, p.43.

*obligations between the payer and the payee*." While it seems that decentralized transaction systems do meet all these criteria, the crucial word of the definition is *funds* which has a limited meaning under the PSD2 and encompasses only "*banknotes and coins, scriptural money or electronic money*". We thus arrive to the same issue and that is that if Bitcoin and others cannot be considered e-money, then all related regulation cannot be applied. Opposite interpretation would require extensive analogy.

More importantly, even if we disregard the above mentioned, the biggest issue is that the concept of PSD2 is based on centralized understanding of provision of payment services and does not fit with the cryptocurrency world. Namely, the PSD2 requires *legal entities* and providers of services which can hardly be pinpointed in a decentralized transaction system where a transaction is authorized and consequently verified multiple times by unrelated nodes in the network.[138] In line with the mentioned CJEU's decision in *Hedqvist* and most recent AMLD5, it could be argued that by analogy, PSD2 could be applicable at least to cryptocurrency exchanges.

Therefore, the prevailing conclusion is that the PSD2 is currently not applicable to decentralized transaction systems, such as Bitcoin.[139] Nevertheless, this conclusion might not pertain to all blockchain-based transaction systems.[140] As was described above, not all blockchain-based technologies are as decentralized as Satoshi Nakamoto described in his Bitcoin manifesto. Therefore, systems like Ripple which are centralized to some extent may qualify as payment providers and payment systems under the PSD2. Unlike Bitcoin, Ripple does have "*one single institution which is able to issue units at its choice*" which is the Ripple Foundation which also provides the cloud where the client cryptocurrency is stored[141]. The transaction is then processed via gateways (typically exchanges).[142] If we consider that such gateways and/or the Ripple Foundation itself can be, under certain circumstances, considered payment services providers, then the second obstacle standing in the way of PSD2

---

[138] S. Kasiyanto *Security Issues of New Innovative Payments and Their Regulatory Challenges* in GIMIGLIANO, Gabriella, *Bitcoin and Mobile Payments: Constructing a European Union Framework* (1st ed., Palgrave Studies in Financial Services Technology, 2016), p. 172.

[139] This conclusion is supported by European institutions (ECB, EBA) and authors (see Ibid).

[140] P. Valcke, N. Vandezande, N. Van De Velde, '*The Evolution of Third Party Payment Providers and Cryptocurrencies under the EU's Upcoming PSD2 and AMLD4*' (2015), SWIFT Institute Working Paper No. 2015-001, SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2665973, last accessed 19.8.2018, p. 53.

[141] ECB (2015), op. cit. no. 49, p. 11-12.

[142] Ibid, p. 13.

application, as shown above, can be circumvented. However, Ripple cryptocurrency is still not regarded as e-money, therefore, the interpretation issue remains.

Due to its more centralized nature which gives more control to financial institutions, Ripple system can be used as a complement to services provided by already authorized providers of payment services. That is the case of the German *Fidor Bank*, as described above, which decided to implement the Ripple system for some of its payment services.[143]

In addition, blockchain technology can also serve financial institutions and other obliged persons under the PSD2 to ensure compliance, e.g. authentication and sharing of information. This is especially interesting for so-called RegTech projects which are subject of section 4.9 of this thesis.

### 3.1.6. *Taxation*

Taxation is generally viewed as an issue when it comes to cryptocurrencies. The reason is their complicated legal status and qualification, as per previous paragraphs. However, irrespective of their legal definition and potential volatility, cryptocurrencies do hold value and trade with them can generate substantial revenue, similarly to securities and other financial instruments intended for investment.

At the European level, the VAT represents the only harmonized tax and as such is subject to the VAT Directive[144]. As already mentioned in 3.1.1 of this thesis, in 2015 the CJEU adjudicated a preliminary question submitted by a Swedish court in case *Hedqvist*. David Hesqvist, a Swedish citizen, wanted to establish a company which would provide bidirectional exchange services (cryptocurrency for fiat currency and *vice versa*) for a consideration (fee) included in the respective exchange rate. Before starting his business, Mr Hedqvist referred to the Swedish Revenue Law Commission with a request for preliminary assessment whether such activities would be subject to VAT. The Revenue Law Commission expressed the opinion that exemption under Article 135(1)(e) of the VAT Directive relating to exchange services of legal tenders should be interpreted as encompassing Mr Hedqvist's

[143] Ibid, p. 14.

[144] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0112.

activity, as the cryptocurrency has the same purpose as legal tenders – to serve as means of payment.[145]

Nonetheless, Skatteverket – the Swedish Tax Authority disagreed and subsequently initiated administrative proceedings which gave rise to the preliminary question at hand.

The Court held that such services are to be considered as provision of services for consideration and thus subject of the VAT Directive. Moreover, the Court stated that "*transactions exempt from VAT under those provisions are, by their nature, financial transactions even though they do not necessarily have to be carried out by banks or financial institutions*."[146] Further, it interpreted the exemption under Article 135(1)(e) of the VAT Directive concerning "*transactions, including negotiation, concerning* ***currency, bank notes and coins used as legal tender****, with the exception of collectors' items, that is to say, gold, silver or other metal coins or bank notes which are not normally used as legal tender or coins of numismatic interest*" as encompassing other, non-traditional currencies, including cryptocurrencies, that the parties to the transaction chose as an alternative to legal tender.[147] Based on the CJEU's opinion that Bitoin's (the cryptocurrency in question) sole purpose was to serve as a means of payment[148], it held that the exchange services in the case at hand shall be exempt from VAT. This conclusion is in line with principle of fiscal neutrality and the Opinion of the AG Kokott[149] who emphasized that the objective of the exemption at hand was to prevent hindering of the convertibility of legal tenders and as Bitcoins do not have other purpose than to serve as means of payment, the distinction whether they are "good" or "bad" currency does not justify their different treatment VAT-wise.[150]

As follows, due to the VAT Directive and the CJEU's approach in Hedqvist, the regulatory stance across Europe[151] is rather unified in this matter. Most EU Member States concur and exempt exchange services from VAT. However, the situation is different for other practices relating to cryptocurrencies, for instance the mining activities. Finland considers the

[145] See paragraph 17 of the judgment.

[146] See paragraph 37 of the judgment.

[147] See paragraph 49 of the judgment.

[148] See paragraph 52 of the judgment.

[149] AG opinion in Case C-264/14 *Hedqvist* [2015] ECLI:EU:C:2015:498.

[150] See paragraph 38 – 45 of the Opinion.

[151] Overview based on '*Regulation of Cryptocurrency Around the World*' (2018), op. cit. no. 84.

mining activity as production of goods and therefore, subjects it to the VAT[152]. Similarly, Russia (even though not a Member State) imposes VAT obligation after a certain energy consumption threshold is reached[153], while Austria[154] and Sweden[155] exempt mining from the VAT due to the fact that there are no identifiable recipients.

Apart from VAT, other taxes, in particular income related, may apply, depending on legal definition and regulatory approach of individual Member States. The situation will differ, as income taxes are not harmonized. Essentially, individuals' revenues tend to be subject to capital gains taxes, especially if cryptocurrencies are regarded as similar to commodities, for instance Finland, Ireland or UK[156]. Business revenues, namely in relation to financial services and exchanges are usually taxed as corporate income tax, e.g., Bulgaria, Italy, Poland, Romania, Spain, the UK[157]. Another relating issue then arises in respect of tax deductions. Some jurisdictions allow submission of losses incurred in crypto-markets (whether due to usual volatility or due to an attack), as tax deductions for the purposes of income taxes. These jurisdictions include Denmark and Italy[158]. Other Member States do not see them as tax deductible, e.g. Finland[159]. For the sake of completeness, it should be noted that Spanish government even considers introduction of "tax breaks" to attract blockchain developers.[160]

## 3.2. Smart Contracts and Ethereum

### 3.2.1. *Ethereum*

The Ethereum project was proposed in 2013 by a Bitcoin enthusiast Vitalik Butarin who based some fundamentals on the Bitcoin's protocol but went a step further to enable self-

[152] Ibid, pp 36-38.
[153] Ibid, pp 75-76.
[154] Ibid, pp 30-31.
[155] Ibid, pp 55-58.
[156] Ibid, pp 36-38, 42-44, 58-59.
[157] Ibid, pp 44-45, 52-53, 55, 58-59.
[158] Ibid, pp 34-36, 44-45.
[159] Ibid, pp 34-36.
[160] Ibid, p. 55.

executing smart contracts and a Turing-complete protocol which would allow building of additional programming layers.

Turing-completeness refers to an "*ability to run any coin, protocol, or blockchain*"[161] and is ensured by Ehtereum's programming language called Solidity which has been often compared to JavaScript, the basis of many applications, such as Gmail or Facebook.[162] The language is stack-based, not binary like Bitcoin which is what enables creation and execution of smart contracts, as it enables unlimited number of contract stages. "*With Bitcoin, the transactions are binary – the Bitcoin are either spent or not spent. With Ethereum, the contract does not have to be fulfilled or not fulfilled, but can be in stage one pre-negotiation, stage two offer, etc.*"[163] Another thing which makes Solidity well-suited for smart contracts is that it is contract-oriented (as opposed to object-oriented) which enables it to understand "*concepts such as identity, ownership, and protection forms*."[164]

Apart from smart contracts, Ethereum has developed additional supporting protocols "*to achieve a complete decentralized ecosystem*".[165] The first is called *Whisper* and is intended for secret, encrypted messaging within the Ethereum network. "*Whisper is also designed to provide communication layer that cannot be traced and provides 'dark communication' between parties*"[166] which could entail more complications for law enforcement authorities (see section 4.7 of this thesis). The second supporting protocol is called *Swarm* and was developed to enable decentralized data storage.[167]

Ethereum is currently the second most widespread cryptocurrency and values USD 290[168] per unit while the whole market cap is estimated at approximately USD 29 billion[169].

---

[161] M. Swan, op. cit. no. 38, p. 21.

[162] L. Lee, '*New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market*' (2016), 12 Hastings Bus. L.J. 81, p. 114; see also A. M. Puertas, R. Teigland, op. cit. no. 101, p. 292.

[163] L. Lee, op. cit. no. 154, p. 115.

[164] A. M. Puerstas, R. Teigland, op. cit. no. 101, p. 292.

[165] I. Bashir, *Mastering Blockchain: Distributed ledger, decentralization and smart contracts explained* (1st ed., Packt Publishing, 2017), p. 267.

[166] Ibid, p. 268.

[167] Ibid.

[168] Data last accessed 20.8.2018.

[169] Data last accessed 20.8.2018.

### 3.2.2. *Smart Contracts*

Smart contracts are not a new notion brought forward with the creation of blockchains. It is a concept authored in 1994 by computer scientist Nick Szabo who defined a smart contract as "*a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs*."[170]

Essentially a smart contract is like any other contract between two or more parties which expresses their agreement relating to a specific subject-matter, except that it is digitalized and transformed in code and then embedded in blockchain. What makes it smart is the possibility to be self-executing without any human input, only depending on occurrence of a specified condition. That condition could be anything; it could be based on the passage of time or occurrence of an event. The first option should be relatively easy to verify, as the contract can mathematically follow the passage of time and when a specific date and time occurs, it can automatically act in accordance with instructions enshrined in its code.[171]

In order to ensure the second option where the smart contract should act on an event occurring outside of the blockchain world which it does not have access to, a specific type of program, called Oracle, was developed. Oracles are used to provide to smart contracts essentially any kind of external data ranging from stock prices and exchange rates to weather forecast and flight schedules. They can also provide IoT data and data embedded in other blockchains. To ensure authenticity of the data, decentralized verification services such as TLSNotary can be deployed.[172]

Additionally, to ensure physical execution of smart contract in terms of data recorded within the blockchain, Ethereum implements Ethereum virtual machine (EVM) programs

---

[170] Ibid, p. 198.

[171] M. L. Perugini, P. Del Checco, '*Smart Contracts: a preliminary evaluation*' (2015), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2729548, last accessed 19.8.2018, p.21.

[172] I. Bashir, op. cit. no. 157, p. 207.

which are also run by every node in the network. To prevent tempering, EVMs are completely isolated and only accept instructions from the smart contract.[173]

From the business point of view, smart contracts could bring easier, faster and more precise negotiation and conclusion of business transactions.[174] For instance, even though the majority of an acquisition today is done online, some documents still need to be signed personally and manually by authorized persons. Smart contracts would eradicate the travelling necessary to ensure signatures on relevant documentation which is nowadays usually required, especially in more complex transactions. From the legal point of view, smart contract are especially revolutionary because they prevent a breach of contract resulting from non-action of the counterparty after particular contractual conditions are met. To provide an example, if we picture a contract on sale of goods for which the counterparty is obliged to provide payment in regular monthly installments, the final decision whether the installments are going to be indeed regular or whether they would be sent at all is always inherently up to the buyer. Indeed, the seller does have legal options to defend and enforce his or her claim and even enforce payment of penalties; however, all of these solutions come *ex post*, after the breach of contract already occurred. The definitive outcome depends on many factors – the buyer's will to cooperate, potential arbitration or court decision, evidence, etc. Apart from that, the seller would need to spend substantial effort, time and financial resources to defend his or her rights. "*In short, traditional contract enforcement is messy and resource-intensive – and it is this perceived inefficiency that motivates much of the excitement about smart contracts*."[175]

As follows, smart contracts may turn the tables, so that a seller who has already shipped the goods can ensure the payment if conditions are met. Certainly, smart contracts do not exclude judicial control, i.e. in the event that the buyer does not agree with the execution of the smart contract, he or she should be able to recover the provided means before the court. Another example where default payment by smart contracts might be convenient are unconditional bank guarantees where the bank should not have the power to decide whether the claim for the bank guarantee is justified or not. Apart from just automatic payment, smart

[173] Ibid, pp 222-223.

[174] R. O'Shields, '*Smart Contracts: Legal Agreements for Blockchain*' (2017), 21 N.C. Banking Inst. 177, p. 183.

[175] K. E.C. Levy, '*Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law*' (2017), Engaging Science, Technology and Society Vol. 3 (2017), p. 3.

contracts can perform many more actions e.g., suspend provision of services or delete a file.[176]

Nonetheless, there are some obstacles which have to be overcome before smart contracts can become a norm; they are of technical and legal nature.

With respect to technical issues, it should be noted that while smart contracts can generally be used to transfer any kind of asset or right, they have certain limits. They are essentially only enforceable towards property which can be digitalized, such as license rights to digital music.[177] Goods and especially services which require physical presence and action in the real world will always require active will of the counterparty, regardless of the code of the smart contract. This is why personal services will not be suitable for smart contracts at all. However, adjustments can be made so that objects which are part of the real world can become digitalized and thus, subject to smart contract transactions. The solution was brought forth by Colored Coins, an alt-coin originally based on Bitcoin but in the Ethereum platform running on Ether, which turns assets into "smart property" marking the crypto-tokens in the blockchain with specific color to represent a particular asset[178], e.g. a car or a house, but also "*commodities, certificates, shares, bonds, and voting [rights]*".[179] The relevant asset can be equiped with a system[180] which can be connected to the blockchain, therefore, smart contract can complete self-execution with consequences in the real world. An often provided example is that of a car which due to the installed program cannot be ignited if payment is not provided and contract executed.[181] Potential digitalization of all tangible and intanglible assets can have distrorting effects on how we understand property law. „*For instance, access to property can be programmatically limited to specific users or device, or even be limited to a person who is identified in a record on a blockchain. When brought to the extreme, every piece of property could be tied to a potential kill switch, whereby property could be disabled or divested remotely though the simple click of a button or a computer algorithm. In such a world,*

[176] R. O'Shields, op. cit. no. 164, p. 179.

[177] M .L. Perugini, P.Dal Checco, op. cit. no. 161, p. 10.

[178] L. Lee, op. cit. no. 154, p.115.

[179] I. Bashir, op. cit. no. 157, p. 172.

[180] For instance, „*software code, QR codes, NFC tags, iBeacons, WiFi access, etc.*" See M. Swan, op. cit. no. 38, p. 14.

[181] M. Raskin, '*The Law and Legality of Smart Contracts*' (2017), 1 Geo. L. Tech. Rev. 305, pp 305-341, p. 310; L. Lee, op. cit. no. 154, p. 114.

*property ownership could vanish, replaced by a web of temporary leasehold interests governed by contracts*."[182]

In terms of legal issues, there have been some reflections relating to theoretical concepts of contract law and whether smart contracts would indeed be able to keep up with them, for example, good faith, rescission, legal capacity, manifestation of consent, error, unenforceability on public security and other public policy grounds.[183] These topics will require substantive legal research in order to determine whether smart contracts would indeed be legally viable. In order to demonstrate potential difficulties of applying legal regime on self-executing technology, a number of particularly interesting practical problems will be assessed.

One of the proclaimed principles of smart contracts is *the code is law*, meaning that whatever is set down in the code should be final and enforceable. However, this principle may have some unanticipated consequences. In particular, in the event that the execution of smart contract is subsequently contested before a court, one of the problems is that the court will likely not be able to read code in which case judicial review of contractual terms would not be possible which is not acceptable in a state bound by rule of law principle. "*This problem could be handled prospectively by developing and maintaining an isolated version of the code translated into natural language when the smart contract goes into effect, which could be updated as changes to it are made. This should not be burdensome to developers of this technology in that they will need to provide a natural language version of the contract to the parties to obtain mutual consent*."[184]

Relating issue concerns the immutability of transactions which is the underlying principle of all blockchains. As was already established, when a transaction is embedded in the blockchain ledger, it is essentially "set in stone" which does not work well for contracts that may be re-negotiated and amended. Similarly, even if a court held that some provisions are not legally valid and wanted to modify them in compliance with applicable legal regulations (especially if, for instance, consumer protection is triggered), it would not be possible under current settings. "*It seems unlikely that large financial institutions, regulators,*

[182] A. Wright, P. de Filippi, op. cit. no 39, p. 35.

[183] See for example R. O'Shields, op. cit. no. 164; K. E. C. Levy, op. cit. no. 165; M. Raskin, op. cit. no. 171.

[184] R. O'Shields, op. cit. no. 164, p. 190.

*and government officials will embrace a technology that cannot be changed later, if necessary*" [185] However, opposite might be true as quite a few international banks have already in 2016 conducted tests on application of smart contract within financial sector, including JP Morgan, BNP Paribas or Barclays.[186]

A number of doubts are raised with respect to procedural side. Blockchain technology entails complications when determining jurisdiction. While the parties are free to provide for competent courts or arbitration tribunal and governing law, it is not clear how the situation would be handled if parties do not do so, especially if contracting parties are also decentralized entities and cannot be pinpointed to one particular jurisdiction. Moreover, parties might face difficulties evidence-wise, e.g. how the court would accept blockchain settings and apply legal requirements on authenticity and integrity of data.

Lastly, one of the most discussed issues is the correlation between legal language and code. Simply put, code requires clear, precise and deterministic language which would enumerate any and all potential situations which might arise. While the (legal) language is constantly evolving, it is naturally abstract and sometimes ambiguous because it is usually not possible to encompass all potential aspects in connection with the contract. On the one hand, many have welcomed it as the lack of flexibility in interpretation would also exclude or minimize the parties' ability to escape their contractual obligations.[187] Simultaneously, smart contracts' templates would also minimize the scope of situations when a lawyer is needed to draft a contract. This could be also beneficial to lawyers who "*will no longer focus on the drafting of boilerplate legal provisions; they could leave the details to a machine, and concentrate on higher order legal work to identify the core provisions of a contractual agreement that should be implemented into code*." [188] Nevertheless, the parties must articulate the terms very precisely because an unintended inaccuracy may trigger the contract execution at the expense of one party. To be sure, this poses enormous requirements on lawyers. It may significantly affect lawyers' liability and also, would require lawyers to closely cooperate

[185] R. O'Shields, op. cit. no. 164, p. 187.

[186] M. Del Castillo, '*JP Morgan, Credit Suisse Among 8 in Latest Bank Blockchain Test*' (2016), available at: https://www.coindesk.com/jp-morgan-credit-suisse-among-8-in-latest-bank-blockchain-test/, last accessed 19.8.2018; J. P. Buntinx, '*BNP Paribas Sees Smart-Contracts in the Future of Legal Code*' (2016), available at: https://news.bitcoin.com/bnp-paribas-smart-contracts-legal-code/, last accessed 19.8.2018.

[187] A. Wright, P. de Filippi, op. cit. no 39, p. 25.

[188] Ibid, p. 24.

with IT specialists and understand programming concepts behind smart contracts.[189] That is why this potentially new generation of IT educated lawyers is referred to as "smart lawyers".

### 3.2.3. *Dapps, DAOs*

Notwithstanding the above mentioned, smart contracts do not have to exist in an isolated environment and for a short period of time. Instead, they can become more complex, eventually even self-programmed, and interact with other smart contracts and even AI.

First step of construction on the fundamentals of blockchain and smart contracts are the decentralized applications (Dapps). Although there are many definitions, Dapp is essentially a smart contract that coordinates and executes other smart contracts in a pre-defined fashion[190]. Similarly to applications built on JavaScript, there are virtually no limits as to what kinds of Dapps can be construed. Most popular Dapps are targeted on market prediction and trading, but also games or social networking.[191] One of the first Dapps created on the Ethereum platform was *Augur* which was referred to as the most complex Ethereum Dapp and is an application for betting on market development.[192] Another example of Dapps might be *Storj* for decentralized storage services. It works on similar principles like cloud but instead of acquiring data centers, the storage space is leased by users in the network who are rewarded for it. In addition, *OpenBazaar* is a decentralized market place, similar to eBay.[193]

A decentralized autonomous organization (DAO) is created by establishing some kind of internal organization which "*[outlines] its governance publicly on the blockchain, and a mechanism for financing its operations such as issuing equity in a crowdfunding*." In DAO smart contracts are elevated to agents who act in accordance with instructions, e.g. for a specific task, and can raise and spend financial resources.[194] If we compare DAOs with traditional organizations, DAO „i*s an organization where the rules of management are predetermined and run on computers*."[195] What's more, unlike usual software, DAO's smart

---

[189] R. O'Shields, op. cit. no. 164, pp 192-193

[190] M.Swan, op. cit. no. 38, p. 23.

[191] '*DAPP Rankings*', available at: https://www.stateofthedapps.com/rankings, last accessed 19.8.2018.

[192] J. Young, '*Most Complex dApp on Ethereum Already Has Millions of Dollars at Stake*' (2018), available at: https://www.ccn.com/most-complex-dapp-on-ethereum-already-has-millions-of-dollars-at-stake/, last accessed 19.8.2018.

[193] A. Wright, P. de Filippi, op. cit. no 39, p. 11.

[194] M.Swan, op. cit. no. 38, p. 24.

[195] M. Raskin, op. cit. no. 171, p. 336.

contracts can be programmed to evolve and adapt over time, e.g. „*through the use of evolutionary algorithms that would change the organization's behavior as it collected information during the course of its operation*." This particular aspect brings blockchain technology closer to machine learning and AI.

In 2016 Ethereum created and crowdfunded a DAO (called "the DAO") targeted at investment without management but controlled by „*shareholders voting based on their stakes on a blockchain*".[196] However, that same year an insider, reportedly, found and exploited a weakness in the programming which led to a hack attack draining more than USD 50 million from the DAO's funding[197]. While the money was subsequently recovered in a counter-attack[198], the incident left crypto-community disturbed and wondering whether smart contracts are actually viable. To stop the attack, the developers introduced a hard fork which caused controversy, as a part of Ethereum users believed that it goes against decentralization principles and immutability. Subsequently, Ethereum split. Those who accepted the hard fork upgrade stayed on the Ethereum platform with the currency Ether (ETH), while the "orthodox" users renamed the original Ethereum platform as the Ethereum Classic with the currency Ether (ETC).[199]

Due to their strictly decentralized and pseudonymous nature, the deployment of DAOs in practice might entail some legal difficulties, e.g. in respect of jurisdiction and their predisposition for criminal activities.

### 3.2.4. *Management of Intellectual Property Rights*

Intellectual property rights refers to protection of human ideas and all values that are hence created, regardless whether the result has tangible or intangible form. At the European level, protection of intellectual property rights is ensured by a number of primary and secondary legal instruments, including the package of directives and regulations targeted at different kinds and aspects of intellectual property to ensure approximation of Member States'

---

[196] Ibid, p. 336.

[197] R. Brandom, '*How an experimental cryptocurrency lost (and found) $53 million*' (2016), available at: https://www.theverge.com/2016/6/17/11965192/ethereum-theft-dao-cryptocurrency-million-stolen-bitcoin, last accessed 19.8.2018.

[198] D. A. Zetsche, R. P. Buckley, D. W. Arner, '*The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*' (2017), EBI Working Paper Series, 2017-007, p. 8.

[199] I. Bashir, op. cit. no. 157, p. 208.

laws.[200] The purpose of the legislation is to ensure protection of authorship, fair and adequate licensing requirements and distribution of royalties.

At this time there are quite a few issues which make determination and enforcement of IP rights complicated and ineffective. For instance, current procedures for registration of patents, trademarks, industrial designs or copyrights, if applicable[201], are lengthy, complicated and non-transparent and in many cases lead to disputes regarding determination of who is the author/owner, when was the protected mark or design used for the first time, etc. Further, the management of copyright is nowadays usually left to intermediaries for collective management who, thanks to their unique and convenient position, are allowed to retain large portions of royalties which results in unfair treatment of authors of copyright works and allocation of revenues.[202]

Blockchain can improve some aspects of the situation. Firstly, any kind of work can be registered in blockchain immediately after it is created, or even as a draft[203]. Additionally, the recorded data can be encrypted to prevent parasite behavior.[204] Due to its transparency, traceability and immutability a large blockchain database can help track the history of any kind of idea which may simplify the registration process and prevent disputes. Even though databases can be created on a centralized basis as well, "*the difference with blockchain is that the sequence of events and associated timeline is much more reliable and consequently much better evidence for court or registry proceedings.* "[205]

It is important to keep in mind that blockchain cannot replace registration offices such as patent offices due to the fact that even though blockchain can prove authenticity and integrity of information (as a proof of existence), it cannot guarantee that recorded content should be granted IP protection, e.g. that an invention should be granted a patent due to its benefits *and* novelty. These services can, so far, be only provided by patent offices comprised

---

[200] List of legislation: '*European Union (EU) (182 texts)*', available at: http://www.wipo.int/wipolex/en/profile.jsp?code=EU, last accessed 19.8.2018.

[201] Some Member States have enacted legislation which allows individuals to register their works protected by copyright.

[202] S. Sharmin, '*Music Copyright Management on Blockchain: Is it legally viable?*' (2018), Uppsala Universitet, p. 27.

[203] Ibid, p. 12.

[204] R. Burbidge, '*The Blockchain Is in Fashion*' (2017), 107 Trademark Rep. 1262, p. 1267.

[205] Ibid: "If blockchain containing data on trademarks is linked to advertising platforms, every case of trade mark usage can be marked and saved for future. This can help to prove how widely and when was the trade mark or yet unprotected mark used in order to prevent future disputes."

of human beings. On the other hand blockchain database with proofs of existence can minimize risks of speculation, as it becomes exponentially more difficult for a "patent troll" to prove that he or she should be granted patent or trademark protection instead of the rightful author/owner.

Secondly, the territorial principle which IP rights are based on requires separate registration in individual Member States, in some cases simplified and harmonized at the European level. However, in the event that all works, marks and designs are registered in a global database not depending of territorial borders, which blockchain can provide, one registration can ensure protection across the EU, in line with the one-stop-shop principle.

Thirdly, together with deployment of smart contracts, blockchain can enable automatic and fair licensing which might, to some extent, eliminate need for intermediaries. Moreover, licensed rights can be effectively bundled so that each user gets and pays for what he or she exactly needs. Smart contracts can also ensure that licensed rights can be subject to inheritance so that collections of digital content can be passed down similarly to tangible books, DVDs or gramophone desks.

In this regard, the recent spike in popularity of streaming services, such as Spotify, Pandora or Netflix might suggest that the consumer culture of copyright works will switch from licensed ownership to online streaming which would mean that blockchain databases would seemingly not be necessary in this field. The switch of approach was enabled by lower prices of mobile internet access and widespread coverage of WiFi networks and by the new business model which these services are based on and which provides unlimited content for relatively low price. In light of the case *PRCA v NLA and Others*[206], streaming was deemed compliant with the InfoSoc Directive[207], as only transient copies[208] are created and these fall in the scope of exception (temporary reproductions) under Article 5(1) of the InfoSoc Directive[209]. However, not even streaming services can fully ensure that authors of works are

[206] See decision of the CJEU, Case C-360/13 *PRCA v NLA and Others* [2014] ECLI:EU:C:2014:1195.

[207] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, full text available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001L0029.

[208] See T. Headon, '*Ghosts in the Machine: Copyright and Temporary Copies*' *(2011), Computers & Law Magazine of SCL, Vol. 22 Issue 4.*

[209] Article 5(1): "*Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an*

adequately paid their share of royalties. For instance, "*Spotify specified that they didn't pay out the royalties as they simply didn't have the essential data to find out whose claims were legitimate, or even how to find the lawful right holders. Additionally, the company said that music industry lacked a reliable database that covered all existing music rights*."[210] This might have prompted the company to consider blockchain technology, as it subsequently bought a blockchain startup Mediachain Labs to develop a database able to keep track of intellectual property rights.[211]

Another interesting aspect of blockchain implementation is that it might enable pseudonymous and even anonymous authors to protect their works without sacrificing their privacy, as all transactions could be traced back to one public address and then provided as proof, e.g. for royalty purposes.[212]

Nevertheless, potential implementation of blockchain technology within the IP sector might be hindered with enactment of new EU legislation referred to as Copyright Directive[213] proposed by the European Commission and at the time of writing subject to trilogue negotiations and awaiting second vote in the European Parliament.[214] While the proposal has raised many controversies, especially relevant to blockchain is Article 13[215], according to which every online platform operator would be required to scan user content to prevent infringement with IP rights before its posting which would essentially imply applying YouTube filtering policies to the Internet as a whole. For these reasons, Article 13 has been

---

*intermediary, or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.*"

[210] S. Sharmin, op. cit. no. 192, p. 14.

[211] Ibid, p. 14.

[212] T. W. Bell, '*Copyrights, Privacy, and the Blockchain*' (2016), 42 Ohio N.U. L. Rev. 439, p. 464.

[213] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM/2016/0593 final – 2016/0280 (COD), full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593.

[214] J. Vincent, '*EU sends controversial internet copyright reforms back to the drawing board*' (2018), available at: https://www.theverge.com/2018/7/5/17535874/eu-copyright-law-article-11-13-rejected-first-vote, last accessed 19.8.2018; J. Reda, '*EU copyright reform/expansion*' (2018), available at: https://juliareda.eu/eu-copyright-reform/, last accessed 19.8.2018 .

[215] Especially paragraph 1 is of crucial importance: „*Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate. The service providers shall provide rightholders with adequate information on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the works and other subject-matter*."

referred to as "censorship machine". In terms of blockchain, this particular article may have grave consequences. As was stated above, blockchain technology gives users the freedom to record any data they want which means that even illegal data or data which are infringing third parties' IP rights may end up immutably recorded in the blockchain ledger.[216] While permissioned blockchains used by private entities can be regulated *ex ante*, requirements as per Article 13 of the proposal would largely affect Dapps providing data storage, such as above mentioned *Storj* or *Swarm*. If not completely abolish, it is ambiguous how else would these requirements be enforced in the environment of permissionless blockchain where no single centralized party effectively exercises control over the ledger.

[216] W. Peaster, '*EU's Controversial Article 13: Considerations for the Blockchain Space*' (2018), available at: https://bitsonline.com/eu-gdpr-article-13-copyright-blockchain/, last accessed 19.8.2018.

# 4. Particular Aspects and Potential Issues

## 4.1. Interoperability, Interconnectivity

As a distributed public ledger, blockchain has the capacity to become the largest database of information. This feature grants the opportunity to reach further, beyond the boundaries of payment systems and FinTech sector. Whenever, there is a need to store large amounts of information in a transparent and traceable way, blockchain can become the foundation into which particular parts of the system are intertwined. Namely, blockchain could contribute to further development of wearable computing, Internet-of-Things (IoT), smart cars or smart homes, etc.[217] The decentralized system which does not require validation or supervision of a trusted third party could therefore take a step further and become completely machine-to-machine effective without the need of human intervention for routine processes.

What could this result into in practice? M. Swan brings forth some interesting ideas: "*Some examples of interdevice micropayments could be connected automobiles automatically negotiating higher-speed highway passage if they are in a hurry, microcompensating road peers on a more relaxed schedule. Coordinating personal air delivery drones is another potential use case for devide-to-device micropayment networks where individual priorities can be balanced. Agricultural sensors are an example of another type of system that can use economic principles to filter out routine irrelevant data but escalate priority data when environmental threshold conditions (e.g., for humidity) have been met by a large enough group of sensors in a deployed swarm*."[218] Some of these ideas may already be materializing, for instance, Toyota is initiating cooperation with developers which should establish an IoT usage-based insurance platform with the aim to reduce insurance costs and prevent fraud.[219]

From another point of view, immutability and transparence together with smart contracts makes blockchain suitable for any kind of public database, such as ownership records, cadastres, commercial registers, libraries etc. Blockchain would enable maintaining

[217] M. Swan, op. cit. no. 38, p. XI.

[218] Ibid, p. XII.

[219] A. G. Simpson, '*Toyota, MIT Lab Eye Using Blockchain in Insurance Rating of Driverless and Shared Vehicles*' (2017), available at: https://www.insurancejournal.com/news/national/2017/05/23/451913.htm, last accessed 19.8.2018.

transparent history of transactions which could lead back to the original owner. The blockchain database could include numerous kinds of metadata, including ownership deeds, company's articles of association and other documents relating to property or registered objects and entities. This would largely minimize risks of fraud and simplify procedures requiring proof of ownership and authentication

## 4.2. Personal Data Protection

### 4.2.1. *EU Regulatory Development*

One of the most often discussed features of blockchain is its perhaps revolutionary approach towards personal data. Over the recent years, the topic of data protection has become more and more pressing, the primary reason being the obvious disregard of privacy and personal data protection principles which some large corporations have expressed when dealing and trading with personal data of their clients.[220] With the wave of social networks and social media the issue only grew, namely due to popular interpretations that personal data contained within social networks represent property of the social network company, and in any case, are part of public data which should be allowed to be a subject of trading. The CJEU actively sought to set boundaries to such treatment of personal data and promote privacy principles and protection of natural persons' rights. In one of its most famous cases from this area, the *Google Spain case*[221], the CJEU articulated the right to be forgotten for the first time which was supposed to ensure that modern technologies like social networks or search engines do not retain personal data forever, without sufficient purpose and legal grounds and in direct contradiction of a natural person's wishes. Within the EU, the efforts to reinforce data protection legal framework culminated in the enactment of the GDPR[222] which

[220] L. D. Ibáñez, K. O'Hara, E. Simperl, '*On Blockchains and the General Data Protection Regulation*', EU Blockchain Forum, [online] available at: https://www.eublockchainforum.eu/knowledge, last accessed 19.8.2018, p. 4: "Take *for example the recent Facebook-Cambridge Analytica scandal, where personal data was transferred to a third party without data subjects knowing when and for what*."

[221] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.

[222] The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), full text available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

essentially follows the principles set by the Data Protection Directive[223] but also brings forth a couple of new terms and obligations for data controllers and processors (such as data protection officer or right to portability, etc.), and more importantly, unlike the Data Protection Directive, the GDPR is a regulation and thus, aims to harmonize the data protection legislation within the whole territory of the EEA.

### 4.2.2. *Blockchain and Personal Data under GDPR*

What is so radical about blockchain in respect to personal data is that blockchain technology in principle does not require any processing of personal data in order to successfully function. As was already established, a user is not required to disclose his or her name, date of birth, account number or any other piece of personal information to be able to transact with any other user over the blockchain network. Public address and public key, even though available to all persons viewing the ledger, will generally not be considered as personal data under the article 4 paragraph 1 of the GDPR and in line with the CJEU's reasoning in *Patrick Breyer*[224], as on their own they do not relate to an identified or identifiable natural person. They can only be used to identify a natural person if they are connected to the specific and unique private key which, in normal circumstances[225], only the relevant natural person disposes with. The private key, however, does fall in the scope of personal data and due to its connection to user's financial resources and ability to single-handedly identify a natural person represents a very sensitive piece of information which should by closely guarded.

Notwithstanding the above mentioned, blockchain can contain other personal data apart from private keys, depending on the contents of the transaction. A simple, basic transaction for transfer or exchange of an amount of cryptocurrency will usually not include any personal

---

[223] The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, full text available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[224] Case C-582/14 *Patrick Breyer* [2016] ECLI:EU:C:2016:779 which concerned legal qualification of IP address ad personal data. The CJEU ruled that dynamic IP address shall be considered a personal detail by all controllers who dispose with other data which, in combination with the dynamic IP address, can be reasonably used to identify a natural person.

[225] The term normal circumstances here refers to basic concept where each user generates and keeps his or her own private key. However, with development of eWallet services, private keys can be transferred for safe keeping with third parties providing these services. From the point of view of such providers, even the public address and public key qualifies as personal data due to the fact that they possess private key and can link them to other personal data, including public address and key.

details, unless the interested parties wish to include them in metadata of the transaction file. However, with the assistance of smart contracts (see section 3.2.2 of this thesis), blockchain can also serve as a solution for secure file-sharing, e.g., for the purposes of transfer of smart property or license. There are two principal options, either (i) the electronic file itself is recorded and shared over blockchain, or (ii) a hash of the file is shared with or without enabling certain parties to reach the file itself which is stored "off-chain". Due to the fact that in respect of the former option the file is accessible to everyone on the network and the ledger and its blocks are doomed to become much larger which will inevitably be projected to transaction fees and thus, may become considerably expensive, the latter option might be more preferable. But if, for any reason, the file itself is uploaded in the ledger, GDPR principles will have to be observed and the protection of contained personal data ensured. If possible, it is recommendable to anonymize any document which could be accessed without limitation from any node within the network.

#### 4.2.3. *Digital Identity*

Due to the specific nature of the private key, there have been many projects building on private keys in one way or another to develop software for verification of digital entity of a person. We are used to verify our identity online for most of our online actions where a form of registration is required, regardless whether new access data are generated (username and password) while the identity is verified via email address, or whether the verification process is wired through an already established digital identity, such as Facebook, LinkedIn, Gmail or other social media profiles. While these practices became usual, they are not the most secure way to verify a person's identity, especially when there is a lot at stake, e.g., shopping online. This is where blockchain could help. Projects like *OneName* or *BitID* aim at facilitating a universal digital identity interface which could be implemented in any website requiring registration, in particular for eCommerce purposes but also in other areas not related to crypto-balance and payments.[226] In order to put more layers between the user's private key and the digital identifier, the software uses eWallet address of users to ensure verification. Instead of remembering the complicated and long eWallet address, the user can set a specific username – "Bithandle" which he or she uses whenever verifying identity. Due to the fact that

[226] M. Swan, op. cit. no. 38, pp 34-35.

the Bithandle is recorded in the blockchain and linked with the user's address, it can be easily traced if needed.[227]

While on the one hand, these applications enable the users to have more control over their digital identity and ensure higher level of security than the usually centralized social media ever can, on the other hand, there are still some security and privacy concerns. Firstly, if the digital authorization software is built on eWallet software, which is likely to be centralized, the issue of centralization and related security risks, as described below, is mitigated but not completely eliminated. Secondly, even though the level of security is improved, having one digital identity identificator or authenticator may still entail some danger, in particular, under certain circumstances it may make identity theft easier. Taking over someone's Facebook or Gmail identity today is still relatively easy and consequences range from a nuisance to some serious harm, depending on the number of connected services and websites. However, if we consider a scenario where the blockchain-based authenticator becomes the universal norm regarded as sufficiently secure way to prove digital identity and is used to connect to more than just eShop websites, for instance to internet banking, social security profiles, or health records in established eGovernment, the consequences can amount to a complete identity loss the actual extent of which we have grasped, so far, only within science-fiction movies. Therefore, even though it can be argued that private keys "are harder to steal" or recover against a user's will, a potential involuntary leak or theft can lead to catastrophic results.

#### 4.2.4. *GDPR Compliance*

Even if we take into account the above mentioned considerations, the data protection area is not completely resolved in terms of blockchain technology. Although it could be argued that a higher level of protection of rights and freedoms of natural persons can be ensured when their personal data is stored and transferred over the blockchain-based software, as opposed to other IT solutions, a couple of questions, in particular relating to enforcement of rights, have to be raised in respect of GDPR compliance.

Firstly, it is ambiguous who should be in the position of controller of personal data contained in the ledger. For instance, if we consider a distributed payment system where all

[227] M. Swan, op. cit. no. 38, p. 35.

nodes are equal, who should a user – a natural person – turn to if he or she wishes to exercise his or her rights as a data subject? Should the independent nodes be even regarded as processors? Under the GDPR, if personal data is included in transactions, each node should be considered as processing personal data, as none of the stipulated exceptions is likely to be applicable. If the relevant data protection authority adopted such stance, it is likely that every node would then be considered a controller of personal data, or possibly all nodes would act as joint controllers. However, according to some authors, it is questionable whether joint controllership could even be applied due to the lack of clear allocation of obligations.[228] It might be a little less ambiguous in case of permissioned (closed) blockchain system, for instance deployed by bank consortia, "*In the latter case of [permissioned blockchain] one can easily imagine regulators to focus on either a technical system operator (if any, e.g., a joint venture set-up) or consider the group of participating entities as joint controllers*".[229] Similarly, blockchains with only a relatively small number of full nodes (for instance within the *Lightning Network* system applying side blockchain networks, see section 4.5.4 of this thesis) could be by analogy regarded as a closed group of joint controllers.

Perhaps even more burning issue is the incompliance with the privacy-by-default principle and the physical impossibility to ensure exercise of the right to erasure of personal data, i.e. the right to be forgotten and similarly, the right to rectification of personal data. Blockchain is based on transparency and traceability – once a block is added to the chain, it cannot be erased or altered without consensus among nodes. "*If old transactions were to be removed retroactively, under current [blockchain] models, the majority of all P2P connected nodes would have to verify again the legitimacy of every effected transaction backwards, unbuild the entire [blockchain] block by block and then rebuild it afterwards, with every such transaction step to be distributed block-wise to all existing nodes*."[230] Such practice would be not just very impractical but also extremely time and energy consuming which leads some authors to believe that adequate interpretation of legitimate interest under article 6 letter f) of the GDPR would be necessary to include the "*core functioning*" of the technology.[231] Other

[228] M. Berberich, M. Steiner: '*Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers*' (2016), 2 Eur. Data Prot. L. Rev. 422, p. 424; L. D. Ibanez and coll., op. cit. no. 210, p. 6,10.

[229] M. Berberich, M. Steiner, op cit. no. 218, p. 424.

[230] Ibid, p. 326.

[231] Ibid.

potential solution might lie in anonymization[232], as opposed to currently deployed pseudonymization[233], which is regarded by some experts as equivalent to erasure.[234]

It should be noted that there are many other issues which might prevent compliance with GDPR, such as uncontrollable transfers to third countries due to blockchains decentralization; however, some authors have pointed out that blockchain technology might have certain features which make it suitable as a tool for reaching compliance. For instance, blockchain could enable more granular and easier management of consent and data subjects' rights, e.g., a controller could keep blockchain records of the data subjects consent in respect of different kinds of personal data.[235]

### 4.3. Fight against Censorship

Due to it decentralized nature, blockchain has been suggested as the most effective solution in fight against censorship, suppression of human rights and over-the-top regulation. In, particular, blockchain has been brought up in relation with management of "transnational public goods and organizations", such as Internet or Wikipedia.[236] Firstly, regulation and potentially even abolishment of any jurisdiction is likely to be futile in respect of blockchain technology, should it decide not to adhere, as there are not many options for governments to shut down a whole decentralized, even global network technically-wise. This could be

[232] P. Voigt, A. van dem Bussche, *The EU General Data Protection Regulation (GDPR)* (1st ed., Springer International Publishing, 2017), p. 13: "*Anonymisation is a way of modification of personal data with the result that there is/remains no connection of data with an individual. Anonymised data is either information that does not relate to an identified or identifiable individual or personal data that was rendered anonymous in such a manner that the person is not or no longer identifiable*."

[233] Ibid, p. 15: "*Pseudonymisation is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, Art. 4 No. 5 GDPR. This could be achieved by replacing the name or other characteristics with certain indicators. The additional information potentially allowing identification must be kept separately. Also, pseudonymisation must be further ensured by additional technical and organisational measures. This could be achieved by encoding the information and sharing the key with only a few people*." In line with recital (26) of the GDPR, pseudonymized data are still personal data and should be protected under the GDPR: "*Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*." Blockchain technology is based on pseudonymization because the private key can be linked with the remainder of data and thus, a natural person can be identified. This is in line with the opinion 05/2014 of Working Party 29 that considered hashing as a pseudonymisation method.

[234] See recital (26) of the GDPR; L. D. Ibanez and coll., op. cit. no 210, p. 7-9; P. Voigt and A. van dem Bussche, op. cit. no. 222, p. 161: "*It should no longer be possible to restore the data without excessive effort. Moving data to the computer's recycle bin will not be sufficient, as said data could be restored with marginal effort. On the other hand, a purely theoretical possibility of restoring the data, with e.g. specialised software, does not entail the unsuccessfulness of the erasure*."

[235] L. D. Ibanez and coll., op. cit. no. 210, pp 10-11.

[236] M. Swan, op. cit. no. 38, pp 30-31.

demonstrated on the Wikileaks example. Although there are opposing opinions in terms of legitimacy of such an instrument, it remains evident that the general public had and still has interest in accessing leaked information. As follows from considerations of some authors, if Wikileaks was on blockchain in 2010 when Edward Snowden leaked confidential information and the organization itself needed donations to continue with its activity, following bans on transactions imposed by centralized governments and financial institutions would be scatheless.[237]

Secondly, by recording information in a permissionless blockchain, it enables anybody and everybody to verify its content. This aspect might be especially important in regard to Internet censorship and currently much discussed notion of "fake news", i.e. incorrect or inaccurate news orchestrated out of propaganda and other political purposes. For instance ICANN, an organization managing Internet domains on the international level, could be effectively replaced by a decentralized equivalent which would make shutting down of websites in totalitarian regimes much more difficult.[238] Namecoin was a cryptocurrency developed for these purposes.[239] Therefore, blockchain can effectively fulfill what samizdat literature did for books of politically persecuted authors. Another example might be Alexandria blockchain which contains unaltered accounts of Twitter feeds.[240]

Nevertheless, it should be kept in mind that with lack of government control, no one can guarantee or even remove illegal, immoral or inhumane data from blockchain either, which poses considerable risks namely in terms of child pornography and terrorism.[241] The similar issue arises in relation to encrypted communication which might also be enabled by using blockchain technology (e.g. *Whisper*). This might be especially interesting with regard to the proposal of ePrivacy regulation[242] and ongoing discussion whether government should be entitled to access private communication on legitimate grounds, such as fight against

[237] M. Swan, op. cit. no. 38, p. 31; L. Lee, op. cit. no.154 , p. 92.

[238] I. Bashir, op. cit. 157, p. 42 ; A. Wright, P. de Filippi, op. cit. no. 39, pp 8, 13-14.

[239] M. Swan, op. cit. no. 38, pp 31-32; L. Lee, op. cit. no. 154, p. 116; M. Atzori, '*Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*' (2016), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713, last accessed 19.8.2018, p. 3.

[240] M. Swan, op. cit. no 38, p. 32.

[241] I. Bashir, op. cit. no. 157, p. 474.

[242] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN.

terrorism via so-called "back doors", technically implemented by electronic communication providers.[243]

### 4.4. Security

Personal data, especially in relation to financial resources and services, have always attracted attackers with the aim to overpower the systems set up for the protection of data and extract every piece of personal, sensitive or otherwise useful information which can then be either sold to interested parties or held for ransom. There are three main goals in respect of the security of systems processing and storing personal data which must be ensured: *integrity* (meaning that the data are not altered without permission), *confidentiality* (meaning that the data are not disclosed to unauthorized persons) and *availability* of data (meaning that regular backups are undertaken so that a copy of data is available in case of an incidental loss).[244]

Over the years, data losses consisting either in incidental security breaches or hacking thefts have become increasingly occurring, especially with the steep rise of Internet. Big security scandals pertained to social networks, financial institutions or telecommunication operators and other service providers.[245] Interestingly, financial and health sectors are especially sensitive in terms of ransomware. The fact that the health providers and other actors cannot afford to lose health data of thousands of patients makes them an easy target of attackers.[246] Consequently, security requirements imposed by regulation and the service providers themselves constantly increase, e.g. deployment of cloud solutions and proficient risk management; however, so far, most of these services are based on *pull technology*

---

[243] For further information see S. Gibbs, '*EU seeks to outlaw 'backdoors' in new data privacy proposals*' (2017), available at: https://www.theguardian.com/technology/2017/jun/19/eu-outlaw-backdoors-new-data-privacy-proposals-uk-government-encrypted-communications-whatsapp, last accessed 19.8.2018; '*In support of the ePrivacy Regulation*' [2017], available at: https://medium.com/@wireapp/in-support-of-the-eprivacy-regulation-36fe8197b2cb, last accessed 19.8.2018; A.M. Devriendt, '*e-Privacy: What happened and what happens next*' (2017), available at: https://edri.org/e-privacy-what-happened-and-what-happens-next/, last accessed 19.8.2018.

[244] S. Kasiyanto, op. cit. no. 137, p. 147.

[245] T. Armerding, '*The 17 biggest data breaches in 21st century*' (2018), available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, last accessed 19.8.2018; '*The most infamous data breaches*' (2018), available at: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/, last accessed 19.8.2018; '*2 Canadian banks hacked, 90.000 customers' data stolen*', available at: https://www.csoonline.com/article/3276275/data-breach/2-canadian-banks-hacked-90000-customers-data-stolen.html, last accessed 19.8.2018.

[246] M.U. R. Askari, '*Significance of Ever-evolving Cybersecurity Landscape: Challenges and Possible Pathways*' (2017), National Journal of Cyber Security Law, Vol. 1 Issue 1, p. 25.

meaning that "*the user's personal information is on file to be pulled any time it is authorized*". The pull technology requires collection and storage of large amounts of data in data centers which essentially become centralized honeypots[247], irrespective whether the company stores the data on its own servers or whether it procures cloud services. Honeypots are attracting hackers because, even though they are strongly protected, they are placed in a specific location and thus, the hackers can focus all their efforts and computational power on one place, for example for a brute force attack.

Blockchain technology has been often proclaimed as a possible solution to these security breaches and risks, namely in respect of financial data and services. As opposed to traditional payment systems, blockchain is a *push technology* which lets the user initiate and submit information relevant for the particular transaction to the network[248]. Thus, the design of the system primarily does not require operation of large data centers; however, as the ledger is growing and many users are relying on the minority of full nodes to verify all transactions, these nodes become mining pools requiring more storage and therefore, become very much alike to data centers of centralized systems.

Nonetheless, despite its reputation as a revolutionary transaction system transforming the way we view currency, payment and security of transactions, it should be noted that even though there are many perks in blockchain technology security-wise, many of these are not automatic and require adequate adjusting and further development. To begin with, there are palpable limits in regard to three above mentioned goals which should be attained to ensure security of data and storage systems.

Firstly, while blockchain ledgers do ensure integrity of recorded data, as after a block is added to the chain it cannot be altered without enormous computational power which would require complicated unbuilding and rebuilding of the chain, it should be emphasized that blockchain "*does not make inaccurate data accurate*".[249] If inaccurate data passes the authorization process (i.e. transaction is considered true), it will be recorded in the ledger forever as the technology does not allow inspection of contents of recorded data.

---

[247] M. Swan, op. cit. no. 38, p. 4.

[248] Ibid.

[249] D. A Zetsche and coll., op. cit. no. 188, p. 13.

Secondly, blockchain ledgers are generally open (if permissionless) and transparent which in its nature goes against confidentiality – whatever is recorded in the ledger (e.g. the addressee or value of the transaction) is accessible to everyone who is connected to the network. However, recent development shows that there might be a way around this issue. For example, by implementing so-called zero-knowledge proofs in Ethereum blockchains. This technology introduces public pieces of information, authenticators, which serve as a verification of a given fact without the necessity to actually send a document or other proof of such fact.[250]

Finally, availability might be in some ways difficult to ensure. While the contents of a blockchain ledger are shared among all participating nodes which ensures that the ledger continues to exist even if one node is compromised or destroyed, if it is the chain itself that is compromised, e.g. in case of an attack, its consequent restoring again requires unbuilding and rebuilding which is not easy.[251]

As follows, even though distributed ledgers do improve security of data systems, they are not "bullet proof".[252] Within last five years, there have been quite a few scandals involving in a security breach which resulted in loss, or better yet theft of millions of crypto-tokens. For instance, the infamous *Mt. Gox* security incident occurred from 2011 until 2014 in Japan-based Bitcoin exchange. Although the cause of the loss of 750,000[253] customers' Bitcoins is still not completely resolved[254], the incident eventually led to the then largest

---

[250] An example of zero-knowledge protocols operating on Ethereum is zk-SNARKs. See C. Lundkvist, '*Introduction to zk-SNARKs with examples*' (2017), available at: https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b, last accessed 19.8.2018.

[251] D. A Zetsche and coll., op. cit. no. 188, p. 11.

[252] Ibid, p. 13.

[253] The incident resulted in total loss of 750,000 customer Bitcoins and 100,000 Bitcoins owned by the exchange owners. In 2014 that corresponded to more than USD 400 million.

[254] The Mt. Gox itself originally declared in the past that the reason of loss was a *transaction malleability* hack which basically consists in a double-spend attack relying on altered transactions, as described further below in the text. Some authors and experts seem to be convinced by this explanation, namely due to the exchange's history of issuing wrong or blank transactions from time to time (for this line of argumentation, please see: E. Felten, '*Understanding Bitcoin's transaction malleability problem*' (2014), available at: https://freedom-to-tinker.com/2014/02/12/understanding-bitcoins-transaction-malleability-problem/, last accessed 19.8.2018 or D. A. Zetzche and coll., op. cit. no. 188. However, as E. G. Sirer explains, the likelihood of transaction malleability issue is rather low, namely due to the fact that the theft of large amounts of cryptocurrency that were stolen would require considerable communication with the exchange in order to convince them that the original transactions were false and the altered ones should be accepted in their stead. For a nice explanation of E. G Sirer where he debunks other implausible theories as well, such as lost keys or government seizure, please see: E. G. Sirer, '*What Did* Not *Happen At Mt. Gox*' (2014), available at http://hackingdistributed.com/2014/03/01/what-did-not-happen-at-mtgox/, last accessed 19.8.2018.

Bitcoin exchange's declaration of bankruptcy.[255] Other incidents resulting in damage of lower amounts include for example European *Bitstamp* exchange hack (2015), Hong-Kong base *Bitfinex* exchange hack (2016) or attack on Ethereum's DAO (2016), the latter one, however, ended up being saved by a hacking counter-attack.[256] This year's attack at a Japanese exchange *Coincheck* and consequent loss of more than USD 500 million worth of cryptocurrencies[257] serves as a proof that incidents continue to happen which might mean that blockchain technology is not as secure as we were led to believe. Potentially weak spots in the blockchain infrastructure which might be at the root of some of the continuous incidents are sometimes divided into two groups: (1) issues relating to the blockchain technology itself and (2) issues relating to so-called supporting systems of the blockchain-based technology.[258]

### 4.4.1. *Malleability Bugs and Double-Spending*

The first group of issues is caused by the language and design of the blockchain system and its coding. As no code is perfect or invincible, blockchain code can be broken or overridden as well.[259] These weaknesses enable attackers to perform double-spend attacks which are based on attackers' efforts to alter an already broadcasted but not yet confirmed transaction and add the altered transaction to the chain before the original one (see **Annex I. - Detailed Description of Blockchain Technology**).[260] The reason behind is the default setting of the system which is always focused on determination whether the transaction is true[261], i.e. whether the necessary parameters are fulfilled. This lets the attackers to modify some aspects of the transaction while still keeping it true.[262] There are, however, quite a few technical obstacles which make double-spend attacks less logical, namely, the attacker must be

[255] D. A Zetsche and coll., op. cit. no. 188, p. 7.

[256] Ibid, pp 7-8.

[257] E. Cheng, '*Japanese cryptocurrency exchange loses more than $500 million to hackers*' (2018), available at: https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html, last accessed 19.8.2018.

[258] S. Kasiyanto, op. cit. no 147, p. 153.

[259] According to the crypto-programming community, there are currently 9 sources of malleability which may motivate the attackers to explore them. See https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki.

[260] E. G. Sirer, op. cit. no. 244, explains the attacker's steps on the Mt. Gox example: "*an attacker can ask Mt. Gox to transfer some Bitcoins, capture the transaction order Mt. Gox issues, and modify it in a way that causes the money transfer to take place yet confuses Mt Gox about whether or not it actually did. This confusion then enables the attacker to contact Mt Gox, claim that the transaction did not go through, and get issued a second payment, thereby stealing money. It's outright fraud and/or theft*.

[261] S. Kasiyanto, op. cit. no 137, p. 165.

[262] Ibid.

connected to many nodes in the network and must dispose with sufficient computing power; and even if such criteria are met, blockchain is designed in such a way that it makes authorization process (i.e. mining) of true transactions primarily more profitable than creation of false ones.[263]

### 4.4.2. *51 % Attacks*

Another issue is the possibility of majority attack or also called 51 % hash power attack. Unlike double-spend attacks, this practice does not presume control only over one transaction. The attacker must control the majority of the computing power of the whole network, thus 51 %.[264] If the control is ensured, the attacker does not have to alter a broadcasted transaction or race with other nodes to add the altered transaction to the chain; he or she can force the approval of submitted transaction by brute force without "innocent" nodes noticing. For these reasons, the control of the network is closely monitored within the cryptocurrency community and if one entity gets even close to 51 %, panic occurs.[265] It should be noted that attackers are more likely to achieve the 51 % threshold by overpowering less secure nodes in the network due to the fact that each miner is free to decide and choose the used equipment and consequently the level of the node's security.[266] The possibility of 51 % attacks is also higher in any blockchain which is somewhat centralized and where "*only a few large mining pools control the majority of the transaction recording*."[267] The centralization tendency is a relevant factor namely in large ledgers with large amounts of recorded data where only few powerful nodes operate, in permissioned (closed) blockchains which however, include only known and verified players and should therefore, be able to mitigate the risk, and finally, certain extent of centralization is a result of supporting services, such as eWallets which are mostly offered by a centralized entities.

---

[263] Ibid, p. 154.

[264] S. Nakamoto, op. cit. no. 42: "*The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes*".

[265] In 2014 entity called GHash.IO was the one almost reaching 51 % and the community started publishing warning, even though the entity itself stated that it would not engage in a 51 % attack as it is less profitable than honest transaction verification. Please see: S. Kasiyanto, op. cit. no. 137, p. 154 and M. Swan, op. cit. no. 38, p. 83.

[266] D. A Zetsche and coll., op. cit. no. 188, p. 17.

[267] M. Swan, op. cit. no. 38, p. 83.

It should be noted, that due to the enormous amount of power that is necessary to take control of 51 % of a network, it is logical that attackers are keener to attempt such attack on a smaller and newer networks which do not yet encompass that many nodes and thus, less computational power is necessary to overpower them. Furthermore, thanks to market places offering mining hardware and software for rent, attackers might be able to amass large amounts of computational power without actually having to purchase them.[268] This might significantly simplify and increase possibility of 51 % attacks and simultaneously make them more profitable for attackers. One website even tries to calculate how much would a 51 % attack cost, depending on the particular network[269]; however, according to some sources, the website does not take into account the actual costs of purchasing necessary computational power (hardware and software) and might; therefore, paint somewhat distorted image.[270] The crucial detail in the blockchain setting which might be explored in order to prevent or at least deter potential attackers from any future attacks might be the number of required verifications by other nodes in the network necessary for a transaction to be added to the chain. For instance, Bitcoin Gold which was a victim of many such attacks recently increased the number from 5 to 50 which, so far, seems to be working.[271]

In addition, some bugs in blockchain code might lead to other forms of attacks, such as Zerocoins case where an attacker was enabled to create and obtain large amounts of completely new and yet unspent coin.[272]

### 4.4.3. *Cryptography*

Lastly, attention should also be given to the cryptography method as well. Blockchain technology is generally based on the *Elliptic Curve Cryptography* which, according to some past predictions, might have been "crackable" by 2015[273] which has obviously not been the

---

[268] A. Hertig, '*Blockchain's Once-Feared 51% Attack Is Now Becoming Regular*' (2018), available at: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/, last accessed 19.8.2018.

[269] The costs might be as low as e.g. USD for an hour long attack: '*PoW 51% Attack Cost*', available at: https://www.crypto51.app/, last accessed 19.8.2018.

[270] A. Hertig, op. cit. no. 258.

[271] Ibid.

[272] The authors also provide good explanation of steps which network's key personnel take after an attack is discovered in order to temporarily block all transactions and quickly enforce a hard fork of the protocol remove the bug: P. Insom, '*Zcoin's Zerocoin bug explained in detail*' (2017), available at: https://zcoin.io/zcoins-zerocoin-bug-explained-in-detail/, last accessed 19.8.2018.

[273] M. Swan, op. cit. no. 38, p. 83.

case yet, as Bitcoin continues to use the *Elliptic Curve Digital Signature Algorithm (ECDSA).*[274] In this regard, doubts are raised particularly in connection with quantum computing which can possibly generate much more computational power and may be a tool for breaking asymmetric cryptography which blockchain is based on.[275]

#### 4.4.4. *eWallets*

The second group of issues concerns supporting technology and equipment which every person participating in a blockchain network needs, regardless whether it is a general user, miner or developer.[276] One of the downfalls of a decentralized system which has no supervising authority is that the management and safe-keeping of private keys is left to users themselves. Due to the fact that private keys are essentially an illogical long set of characters which most people would have trouble remembering, eWallet software has been developed to ensure safe-keeping and user-friendly access at the same time. The eWallet services have many advantages, namely, if a person forgets or loses the password/handle to his or her eWallet, it does not automatically mean that all cryptocurrency kept in the eWallet is lost as well (which is the case if a person does not keep the cryptocurrency in an eWallet). This is due to the fact that the company providing eWallet services usually also provides customer service and can help recover the password and reinstate access. The drawback is that the company is usually based on centralized systems requiring storage of data, including private keys of clients, in data centers which consequently become honeypots for potential attackers. To mitigate this risk, many eWallet providers store clients' private keys in "cold storage", i.e. without access to Internet which ensures that they are not accessible online and should an attacker wish to obtain them, he or she would have to be physically present in the data center.[277]

---

[274] '*Elliptic Curve Digital Signature Algorithm*', available at: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm, last accessed 19.8.2018; '*Secp256k1*', available at: https://en.bitcoin.it/wiki/Secp256k1, last accessed 19.8.2018.

[275] ENISA, '*Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector*' (2016), p. 15.

[276] S. Kasiyanto, op. cit. no. 137, p. 155.

[277] E. G. Sirer, op. cit. no. 244.

### 4.4.5. *Exchanges*

The situation is similar in case of exchanges where users can trade and exchange cryptocurrencies for other cryptocurrencies or for fiat currencies. Although technically similar, as follows from provided examples, security breaches which took place at an exchange represent a vast majority of all cryptocurrency losses. While there might be more reasons, the prevailing one seems to be that while eWallet providers are usually "honest" companies, many exchange operators seek to obtain quick gain by speculation and manipulation of the crypto-market. Another reason lies in the fact that as new start-ups, these companies are less likely to focus its investment efforts and resources on security risks.[278] As consequence, majority of exchanges are based on outdated and underdeveloped software which enables numerous attacks.[279] This is not a general rule, as there are likely exchanges ensuring that they use and develop the best IT solutions possible, but rather a tendency which can be observed from reported breaches.

It goes without saying that there are necessary requirements in respect of customer due diligence which should be attained. They include regular backups and updates of software, including the whole eWallet, secure storage (for private keys outside eWallets preferably cold storage), strong passwords, etc.[280]

### 4.4.6. *Consumer Protection*

Cryptocurrency and blockchain-based transaction systems are currently not suitable for an average consumer. Even if we disregard the financial side of trading and exchange of currencies and additional payment and financial services, a certain amount of IT knowledge is necessary to participate in the system without quickly losing all savings exchanged for cryptocurrency (e.g., by loss of private keys, choice of wrong exchanges, etc.)[281]. While many cryptocurrencies try to provide necessary information and even security warnings and advice to its clients and other interested parties, for example in relation to eWallet safe-keeping[282],

[278] S. Kasiyanto, op. cit. no. 137, p. 165.

[279] E. G. Sirer, op. cit. no. 244.

[280] S. Kasiyanto, op. cit. no. 137, p. 156; see also A. Nova, '*After $500 million Japan cryptocurrency theft, here's how to keep yours secure*' (2018), available at: https://www.cnbc.com/2018/01/29/after-500-million-japan-cryptocurrency-theft-heres-how-to-keep-yours-secure.html, last accessed 19.8.2018.

[281] S. Kasiyanto, op. cit. no. 62, p. 43.

[282] '*Securing your wallet*', available at: https://bitcoin.org/en/secure-your-wallet, last accessed 19.8.2018.

there are yet no standards nor codes of conduct in this area. Consumer protection is one of the main drives and strongest arguments of those who call for regulation of blockchain and/or cryptocurrencies[283], meaning that states should step in and define requirements and conditions under which provision of crypto-related services could be provided to consumers. One of the first states is Malta whose MPs have recently passed a set of three bills regulating cryptocurrencies and blockchain which also introduce a new supervisory and regulatory body.[284] According to the Maltese government, their goal is to establish Malta as one of the leading jurisdictions in the area of blockchain technology.[285]

#### 4.4.7. *Key Personnel*

On a separate note, the system's basic setup in terms of "key personnel" might also be regarded as a potential risk. The term key personnel refers to the core developers having access to the altcoin's software who decide about major updates and can propose hard forks which, however, require support of the majority of users.[286] Firstly, "*in all business organizations key people pose risk to the organization – they could become sick, tired, mentally unwell, subject to extortion or corruption. Regardless of the reason if the trust put in key people is ill-placed the ledger's security and reliability are at risk.*" Secondly, the position of influence of such persons inevitably creates tempting opportunities for personal gain at the expanse of the rest of the network, regardless whether it is manipulation of the market in regard of exchanges, investment fraud or practices similar to insider trading due to the fact the core developers will always dispose with more information than the rest of the network. This particular factor might even stand behind some of the infamous cryptocurrency losses that were mentioned above. For instance, Jon Montroll, founder of BitFunder exchange and other crypto investment platforms has recently pleaded guilty to "*securities fraud and obstruction of justice*" in front of US courts for theft of thousands of Bitcoins blamed on a

[283] S. Kasiyanto, op. cit. no. 137, p. 163.

[284] G. Fenech, '*Malta Regulator Opens Consultation after Publishing Cryptocurrency, Blockchain Bills*' (2018), available at: https://www.ccn.com/malta-regulator-opens-consultation-after-publishing-cryptocurrency-blockchain-bills/, last accessed 19.8.2018.

[285] S. Das, '*Exclusive: Malta PM Confirms Parliament Will Pass Three Cryptocurrency Bills*' (2018), available at: https://www.ccn.com/breaking-exclusive-malta-pm-confirms-parliament-will-pass-three-cryptocurrency-bills/, last accessed 17. 8. 2018.

[286] D. A Zetsche and coll., op. cit. no. 188, p. 19.

hack.[287] Similarly, Mark Karpeles, former CEO of Mt. GOX was charged and is currently tried by Japanese courts for embezzlement and manipulation of data.[288] Lastly, the idea of blockchain and related services primarily came out of frustration and concern with behavior and instruments of government's centralized supervisory organizations, such as central banks. The power and influence that is in hands of core developers goes against that idea. Even though blockchain is sometimes referred to as a form of direct democracy due to the necessary support of majority, the key personnel is not held accountable to anyone. Unlike in the case of centralized authorities, so far, there are no terms, no codes of conduct, no supervision. In some cases, we do not even know the identities of these persons.

### 4.4.8. *EU Market - NIS Directive*

At the European level, the cyber security issue was addressed by the enactment of the NIS Directive[289] which imposes obligations on defined regulated persons and services. The obligations particularly relate to management of security risks and reporting of security incidents. The first issue which needs to be resolved is whether the NIS Directive can even be applicable to blockchain.

In article 4 paragraph (1) the NIS Directive provides a relatively wide definition of "network and information system". Apart from obvious inclusion of electronic communications networks in letter (a), for the purposes of NIS Directive network/information system shall also be "*(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.*"

---

[287] S. Das, '*Bitcoin Stock Exchange Operator Pleads Guilty to Securities Fraud*' (2018), available at: https://www.ccn.com/bitcoin-stock-exchange-operator-pleads-guilty-to-securities-fraud/, last accessed 17. 8. 2018.

[288] J. Cook, '*The CEO of bitcoin exchange Mt Gox described what it was like to discover he had been hacked: 'It felt like I was about to die'*' (2018), available at: https://www.businessinsider.com/mt-gox-ceo-mark-karpeles-hacked-i-was-about-to-die-2018-3, last accessed 19.8.2018; J. Young, '*Mark Karpeles Will End Up Taking $859 Million From Mt. Gox Bankruptcy*' (2017), available at: https://www.ccn.com/mark-karpeles-will-end-taking-859-million-mt-gox-bankruptcy/, last accessed 19.8.2018.

[289] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

Blockchain distributed ledgers may be considered a digital data stored and processed by a "*sophisticated algorithm*"[290] and thus, can be deemed as falling in the scope of networks and information systems. However, if the NIS Directive is applicable, who should be required to fulfill the imposed obligations? The problem lies in the decentralization aspect of blockchain ledgers. As was already mentioned, all nodes connected and participating in a decentralized ledger are equal and none of them, not even the miners or developers' nodes, exercise control of others. Thus, as there is no centralized point of control or contact, any security requirement following from the NIS Directive would be generally hard to enforce. To apply the NIS Directive, we therefore need to assess whether there are any entities or nodes in a blockchain which could fall in the scope of defined regulated entities, i.e. operators of essential services or digital service providers.

Essential services are services which are crucial for the functioning and well-being of society, provided that they fall into the scope of sectors pre-defined by Annex II of the NIS Directive. They include for example energy, health, financial or drinking water supply and distribution sector. The NIS Directive then imposes obligation on providers of such services and on operators of networks which are fundamental for smooth running and provision of essential services, i.e. for instance communication system of a hospital.

Firstly, no blockchain network in the sense of the transaction system, such as Bitcoin or Ethereum network is likely to be considered an essential service on its own. Since blockchain transaction systems are in many cases not even considered as payment instruments from the legal side of view, it can be concluded that they are not critical or essential for smooth running of state economy or well-being of society in respect of banking or financial sector[291]. Furthermore, even if it was possible to treat blockchain transaction system, such as Bitcoin, as a payment instrument, "*it is impossible to identify who is the 'service provider' in the Bitcoin system*".[292]

Secondly, the situation might be slightly different if we look at blockchain from the perspective of information and/or communication system supporting an essential service. Namely, actors in financial and banking sectors may deploy blockchain solutions to store and

[290] S. Kasiyanto, op. cit. no. 137, p. 172.

[291] Which might change should a strictly blockchain-based platform, DAO or DAP be considered a trading venue under Annex II of the NIS Directive and in accordance with the MiFID.

[292] S. Kasiyanto, op. cit. no. 137, p. 172.

share information. Such blockchain would, however, probably be a closed/permissioned blockchain with a limited number of participants. In such a case all participants, probably banks or commercial financial institutions, would be required to ensure that security measures as per article 14 of the NIS Directive are met with respect to the system – namely reporting of incidents. This would require cooperation, internal set of rules and division of obligations among the members of the permissioned blockchain.

And thirdly, blockchain should also be assessed from the angle of digital services and digital service providers. The NIS Directive does not provide direct definition of digital services; instead it refers to article 1 paragraph 1 letter (b) of the Directive on Information Society services[293] which defines services as "*any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*." Nonetheless, the NIS Directive further narrows this scope by referral to Annex III, thus, digital services subject to the NIS Directive, are limited to (1) online marketplaces, (2) online search engines and (3) cloud computing services.

In this regard, first conclusion is that some blockchain-based services might be considered as online marketplaces. This is especially the case of cryptocurrency exchanges which "*basically provide service to users by providing platforms enabling users to exchange real money [cryptocurrencies]and vice versa*".[294] In such a case, they would be required to apply technical and organizational measures, procedures for notification of incidents and fulfill other obligations under the NIS Directive.

The second conclusion is that blockchain solutions might also be considered as a form of cloud computing. The NIS Directive defines cloud computing as "*a digital service that enables access to a scalable and elastic pool of shareable computing resources*."

While cloud services are currently provided almost exclusively by centralized providers disposing with large data centers, the same services can be provided by a (un)limited group connected in a network. "*While the European law-maker did presumably not anticipate it, the*

[293] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, full text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_241_R_0001.

[294] S. Kasiyanto, op. cit. no. 137, p. 174.

*blockchain infrastructure layer is actually similar to the single service provider model from a functional perspective. It could thus be considered as a specific kind of cloud computing service where the computing resources are (i.) constituted by the network-powered platform (Platform as a Service or "PaaS") and (ii.) provided and allocated according to the governance rules of the blockchain platform*."[295] It is not clear, whether such interpretation would indeed be possible or whether amendment would be necessary, as the CJEU has to this day not yet interpreted cloud computing in its judgments. Nevertheless, if we accept such interpretation, the issue of pin-pointing a service provider and thus, obligated person under the NIS Directive remains[296]. If we consider that cloud computing services were to be provided on the basis of a permissioned blockchain, the issue can be overcome, even if with certain difficulties; however, should the cloud provision be based on a permissionless blockchain with open access (e.g. *Storj*, *Swarm*), provisions of the NIS Directive would likely not be enforceable under current circumstances and wording and thus, an amendment might be necessary to ensure the same level of security a protection.

### 4.5. Capacity and Potential Scaling

One of the often discussed issues of transaction systems based on blockchain is their limited capacity which is affected and caused by many factors. Firstly, regard must be given to the processing time of the network. If we take Bitcoin as a representative of cryptocurrencies, namely due to its ubiquity and popularity, the processing time of a transaction within the Bitcoin network is at average 7 minutes while the network is updated every 10 minutes[297]. As opposed to traditional payment systems which usually take hours or even days to process a payment order and complete a transaction, the time necessary for the completion of transaction, i.e. addition of new block to the chain, is measured in seconds, however, the preceding step consisting in verification of the transaction by a pre-defined

---

[295] C. Ducuing, '*Fifty shapes of cloud on the internet: the blockchain infrastructure layer as a cloud computing service*' (2018), available at: https://www.law.kuleuven.be/citip/blog/fifty-shapes-of-cloud-on-the-internet-the-blockchain-infrastructure-layer-as-a-cloud-computing-service/, last accessed 19.8.2018.

[296] Ibid; J. Czarnecki, '*Why Blockchain Firms Shouldn't Ignore New EU Cybersecurity Laws*' (2017), available at: https://www.coindesk.com/why-blockchain-firms-shouldnt-ignore-europes-new-cybersecurity-laws/, last accessed 19.8.2018.

[297] H. Holmberg, *How to scale Bitcoin: A payment network that no one controls* in R. Teigland and coll., op. cit. no. 52, p.. 310: „*This waiting time is the sum of: (1) the time it takes for the transaction to reach a mining node; (2) the time it takes for the mining node to create a block; and (3) the time it takes for this block to reach the user with information about the validity of the transaction.* "

number of nodes[298] connected to the network called mining (further described in **Annex I. - Detailed Description of Blockchain Technology**) requires more time, mostly depending on the size of the block. In other words, the bigger the file, the longer it takes to verify the transaction as true. For these reasons, Bitcoin network limits the maximum size of a block to 1 MB of data[299].

If we disregard limitations applied by banks and payment providers in respect to the transacted amount, i.e. value of transaction, no other limits are present in the traditional payment systems. This difference is mirrored in the manner how the transactions fees are calculated. Namely, Bitcoin systems follow the rule – the bigger the file, the higher the transaction fee, while traditional payment providers derive the amount of their fees from the value of the respective transaction.[300] The existing abyss in terms of capacity between Bitcoin and traditional payment providers, such as Visa, can be further demonstrated if we take into account the number of transactions processed per second. With 200 million transactions per day, Visa system can process 2,300 transactions per second on average (while up to 56,000 transactions per second can be processed at maximum). Bitcoin, on the other hand, currently processes 280,000 transactions on daily basis which means that only 7 transactions are processed per second. [301] The difference seems enormous.

If we continue to regard Visa as a representative of traditional payment providers, we can see that in its case, any issue relating to capacity, can be resolved relatively easily. Due to its being a centralized system controlled by a very narrow circle of persons/entities, it is not difficult to ensure more computing power by reinforcing the nodes in the network with more powerful computers. Bitcoin, on the other hand, is a distributed ledger, decentralized network of computers with different computing power and no authority to order use of specific hardware and software which might ensure more computing power. Every node in the network is free to decide which hardware and software it chooses, provided that it enables running of the whole system, which is obvious if we take into account hard forks and different versions of essentially one blockchain system (for example Ethereum and Ethereum Classic).

---

[298] Ibid: in order to be able to broadcast and complete a transaction, the concerned computer must be connected to at least 8 other nodes in the network.

[299] Ibid, p. 316.

[300] Ibid.

[301] Ibid, p. 309.

### 4.5.1. *Shortening of Processing Time*

Nonetheless, the majority of experts insists that Bitcoin's capacity can be increased and thus, that the decentralized payment system can accept and process more transactions. The more obvious solution might be the shortening of the processing time by making the problem which the nodes have to solve easier and less computing power consuming. However, that would lead to higher risks of hacker attacks and double-spend attacks and would effectively weaken the system[302]. If the decentralized payment system loses security as one of its strongest features, it also loses most of the advantages that it has over traditional centralized systems and essentially becomes useless.

### 4.5.2. *Increase of Block Size*

The other approach to increasing Bitcoin's capacity is to increase the size of blocks. This, however, also has certain downfalls. Firstly, when connecting to network, the user downloads the complete history of the ledger up to the Genesis block. Currently, that means more than 110+ GB of data.[303] "*An alternative to becoming a full node is to download simplified payment verification (SPV) software. SPV software does not verify the entire transaction history; instead it relies on other full nodes for its verification. SPV software can be installed on smartphones, and is the most common way to use Bitcoin.*"[304] For the purpose of better user experience, the SPV software informs the user only of relevant information, such as completion of verification of transaction – addition of new block or balance on the user's address.[305]

By enlarging the blocks in the chain, the complete ledger of transactions would become exponentially larger, and therefore, a user wishing to become full node capable of mining would need to fulfill more demanding requirements in respect of employed hardware and software.[306] Eventually, most users would opt for SPV solution and the mining would be left to a few nodes powerful enough to "do all the work". Apart from increased likelihood of attacks, this would likely lead to centralization of the distributed payment systems to some

[302] Ibid, p. 315.

[303] Ibid, p. 310.

[304] Ibid, pp 310-311.

[305] M. Swan, op. cit. no. 37, p.82.

[306] H. Holmberg, op. cit. no. 287, p. 315.

extent which may be viewed as honeypots of decentralized systems; and again the whole concept might be jeopardized. For these reasons, it has been discussed whether the full nodes in the network should be additionally rewarded[307], so as to provide incentive. Should the majority of full nodes decide that the particular blockchain network means more problems than advantages, the whole system would crumble. This strong dependence on full nodes raises concerns not just in respect of centralization, but also stability of currencies and relating payment systems.

### 4.5.3. *Bitcoin Unlimited*

It may seem that there is no feasible way to increase Bitcoin's capacity without weakening some of its strong suits. Bitcoin Unlimited takes the plunge and tries to remake one of the downfalls into an advantage, or at least less of a problem. It removes the limit on block size and lets the interested parties decide which of the objectives is more important and how much they wish to gamble, based on the "*miner's fear of losing the block reward due to an orphaned block*". The rate of orphaned blocks is likely to be higher if the blocks are bigger because by the time one big block is duly verified and added to the chain, a couple of smaller blocks may already be added. In accordance with the longest chain principle this would mean that the bigger the block, the more likely it is to be orphaned in which case the miner that verified it does not receive any reward, be it the transaction fee or a sliver of newly created Bitcoin. Bitcoin Unlimited therefore allows the mining nodes themselves to decide what risk in respect of the size of blocks is acceptable to them.[308] They might feel more comfortable to take the risk of bigger blocks if they dispose with more capable equipment (such as stronger internet connection) which would enable them to solve the problem more quickly. This is in turn connected to inevitable centralization of the system where only big nodes with immense computing power would be capable of processing big blocks and would thus earn all rewards.[309] If that was the case, it is questionable whether Bitcoin would even be still considered as a peer-to-peer payment system, or whether these powerful nodes would become something alike centralized authorities which require trust.

---

[307] M. Swan, op. cit. no. 38, p. 82.

[308] H. Holmberg, op. cit. no. 287, p. 316. To be exact, miners dispose with memory pool which serves as a reservoir of all received transactions. Subsequently miners themselves decide which transactions are to be included in the pool, provided that they solve the problem. They can, therefore, accumulate more or fewer transactions, depending on their will to take the risk.

[309] Ibid, pp 316-317.

### 4.5.4. *Lightning Network*

Another idea was brought forward by a Bitcoin upgrade called *Segregated Witness* which is more modest in terms of the block size increase and sets the limit to 1.6 – 2 MB. Essentially, this upgrade aims to enable users to transact privately on a separate network – side chain (called the *Lightning Network*) without relying on the whole Bitcoin network while using a method similar to security deposit or letter of credit in traditional payment systems. The transaction is mostly kept private between the two nodes; however, the Bitcoin network and all its nodes remain a possibility in case of an issue with the transaction. In other words, the Bitcoin network becomes something similar to a settlement or arbitration instrument. If the respective opposing party causes a problem or tries to prevent the user from collecting its due amount, the user is always allowed to broadcast the transaction within the whole Bitcoin network and subsequently can collect the opposing party's deposit. Particular advantage represents the level of privacy which the users may enjoy. If all interested parties are satisfied, the transaction never has to be broadcasted in the public ledger. "*The possibility to connect bidirectional payment channels with each other will enable an off-chain payment network, and estimates show that if users broadcast three transactions per year onto the main Bitcoin network, then the Bitcoin ecosystem would be able to serve 35 million users with a 1 MB block size.*"[310]

In general, creation of side chains which would be connected to the main chain and would be able to broadcast a transaction in case of a problem especially makes sense in regard to blockchains used for machine-to-machine communication (e.g. DAPs, DAOs) or IoT which require storing of large amounts of data and deployment of micropayments.[311] M. Swan suggests that different kinds of specialized blockchains would need to be developed for different kinds of services and communication: "*Maybe there could be daily purchase blockchains for the grocery store and coffee shop purchases, and others for large-ticket items like real estate and automobiles. More stridently different functionality is needed for noneconomic-market blockchains, for government services, intellectual property registration, notary services, science activities, and health-record keeping. The key question is distinguishing the economic principles needed for the different range of functions with which*

[310] Ibid, 317.

[311] M. Swan, op. cit. no 38, p. 65.

*blockchain technology could be helpful. However, not every operation is one of value registration and exchange.*" Another advantage of side chains is that they can be quarantined, i.e. a potential attack or breach of a side chain does not have to automatically affect all blocks and data recorded in the whole blockchain.

### 4.6. Energy Consumption

What makes blockchain technology demanding energy-wise is the process of mining, especially the proof-of-work method which requires the mining nodes to spend enormous computational power to find a solution for difficult mathematical problems. This aspect has been labeled as wasting of energy, namely in terms of protection of environment and sustainable development.[312] Some studies from 2016 have compared the then spent energy to 20 % of an average nuclear power plant[313], while some predict that by 2020 the energy consumption will be equal to that of the whole country of Denmark.[314] The enormous amounts of energy that are required for mining have resulted in creation of specialized mining pools comprising of warehouses filled with specialized hardware and placed in convenient geographic places with low costs of electricity, e.g. China, which in turn increases security risks related to such centralization.[315]

There have been two major proposals of solution of this issue. Firstly, some have suggested that another more energy preserving method of verification should be implemented. For instance, proof-of-stake is based on the node's amount of already mined cryptocurrency and relating interest in well-functioning of the network which then allows implementation of voting process instead of energy-consuming solving of problems. Ethereum will reportedly switch from proof-of-work to proof-of-stake with its *Casper* update.[316]

The second proposal tries to use the spent energy for other purposes, i.e. to give the mathematical problems of proof-of-work method another, more useful purpose. For example, CureCoin implements problems based on folding proteins which can help find a cure for

[312] M. Swan, op. cit. no. 38, p. 54; I. Bashir, op. cit. no. 157, p. 165.

[313] L. Lee, op. cit. no. 154, p. 105.

[314] I. Bashir, op. cit. no. 156, p. 165.

[315] E. D. Baker, 'Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange' (2015), 45 Sw. L. Rev. 351, p. 366.

[316] I. Bashir, op. cit. no. 157, p. 469.

cancer, Alzheimer's or Parkinson's disease.[317] Primecoin also uses spent computational power for scientific purposes, in particular for discovering special number chains[318] which are important in many scientific fields, e.g., in physics.[319]

### 4.7. Illegal Activities and Anti-Money Laundering Regulation

Cryptocurrencies, and especially Bitcoin, have often been brought up in relation with illicit activities which might have been one of the factors preventing widespread adoption, as a large portion of general public has gained an impression that cryptocurrencies are commonly issued and used by criminals. Nonetheless, while there have been instances of criminal exploitation of crypto-technology, so far, there is no evidence that cryptocurrencies have been purposefully issued by organized crime for financing of criminal activities.[320] To provide context necessary for determining the extent of criminal activity within crypto-market, blockchain's potential uses for different kinds of crime will be briefly assessed.

Blockchain does have some properties which might be convenient for commission of criminal acts. Firstly, it is strictly pseudonymous and if an individual does not disclose the private key, it is generally very difficult to trace transactions to one particular natural person. Even more so, if the individual uses additional techniques like masking of IP address (VPN), mixing service[321] or creation of number of public addresses, it makes identification and traceability even less feasible. Secondly, deployment of smart contracts decreases the necessity of direct contact between criminals (e.g., principal and agent) while at the same time eliminating trust and ensuring that both parties hold up their end of the bargain. Consequently, deployment of smart contracts for criminal acts like leakage of government secrets, assassination or theft of private information might increase the likelihood that the crime will

[317] L. Lee, op. cit. no. 154, p. 116.

[318] Called Cunningham chains and bit-twin chains.

[319] I. Bashir, op. cit. no 157, p. 165; L. Lee, op. cit. no. 154, p. 116; M. Swan, op. cit. no 38, p. 54.

[320] J. Baron and coll., op. cit. no. 45, p. 19.

[321] S. Gruber, '*Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*' (2013), 32 Quinnipiac L. Rev. 135, p 177: Mixing service "*prevents third parties from tracking Bitcoin transactions originating from a particular address and if properly done, you can eliminate any chance of finding your payments and make it impossible to prove any connection between a deposit and a withdrawal inside [the] service.*"

be successful.[322] Additionally, the interaction between criminal parties is even more simplified with deployment of decentralized encrypted communication which cannot be traced back to them, such as above mentioned *Whisper*.

In particular, one of the crimes that Bitcoin was used for was operation of illegal marketplaces, especially the most famous one – the Silk Road. Silk Road was a marketplace of dark web[323] which could only be accessed in a specified manner and which served as an intermediary for sale of drugs, illegal weapons, forged official documents (e.g., passports), etc.[324] The only currency which could be used for payment for purchases was Bitcoin. Even though relatively anonymous itself, the operators designed a system of further covering up of transaction traces, so-called "tumbling" which involves in creation of fake transactions to divide large amounts of currency into a series of smaller ones. Furthermore, any communication was wired through a number of separate servers to cover the location of origin.[325] As a result, the transactions were untraceable and the illegal trade thrived. The Silk Road[326] operated roughly from 2011 to 2012 until US FBI managed to gain control of one server and consequently dismantle internal organization.[327] Its founder, Ross Ulrich was arrested and consequently sentenced for life imprisonment, however, not many other criminal actors engaging in the Silk Road's trade activities were successfully arrested, namely due to enhanced anonymity that the marketplace provided.[328]

Similar techniques of anonymity and non-traceability, such as tumbling and encrypted communication are used for other types of crypto-related crimes. In particular, in the past Bitcoin has been used for ransomware which implies theft of personal or sensitive data and consequent demand for ransom in cryptocurrency to ensure that the transaction cannot be

---

[322] A. Juels, A. Kosba, E. Shi, *'The Ring of Gyges: Using Smart Contracts for Crime' [2016], The 2016 ACM SIGSAC Conference, [online], available at: https://www.researchgate.net/publication/310821111_The_Ring_of_Gyges_Investigating_the_Future_of_Criminal_Smart_Contracts, last accessed 19. 8. 2018.*

[323] Dark web is commonly referred part of Internet network which does not use world wide web protocol and can only be accessed via a specialized software. Historically, it has been used for criminal activities.

[324] E. G. Sanchez, '*Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens*' (2017), 28 U. Fla. J.L. & Pub. Pol'y 167, pp 183-184.

[325] Ibid, pp 183-184.

[326] For more details on Silk Road, see N. Christin, '*Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*' (2012), Cornell University Library, available at: https://arxiv.org/abs/1207.7139, [online] last accessed 19.8.2018.

[327] E. G. Sanchez, op. cit. no. 314, pp 183-184.

[328] Ibid, pp 183-184.

traced back to the criminal.[329] An example from 2015[330] involved in malware spread via spam and after encryption of data on a device was conducted, the data was not released until a crypto-ransom was paid. In a similar manner, in 2012 US presidential candidate Mitt Romney was a victim of ransomware in relation to his past tax reports which the hacker threatened to publish.[331]

Allegedly, cryptocurrencies have also been targeted by terrorist organizations. The most commonly known case included Islamic State (ISIL) supporters requesting donations of other supporters in Bitcoins. However, adoption of cryptocurrencies by terrorist organizations is not as widespread and common, as we might be led to believe. "*This situation may well change in the future, however, if non-state actors feel they have more to gain—politically, economically, or operationally—by moving toward increased [virtual currency] usage*."[332]

Finally, cryptocurrencies can be used for money laundering and tax evasion. Money laundering implies any kind of hiding and covering of true, illegal source of money. Tax evasion includes hiding traces of money in order to not have to report respective revenues to the tax office. Due to fact that both of crimes deploy similar practices, they will be assessed together. The main issue of investigation authorities is that if there are no traces, no documentation, no proof which would establish a link between a natural person and a particular sum of money, there is no crime.[333]As was already stated, there are numerous techniques which, if properly executed, can ensure that transactions will not be traced back to their origin or to the receiving party. An example includes cryptocurrency exchange Liberty Reserve which was established for money laundering purposes but which was a centralized entity.[334] On the other hand, some experts believe that crypto-markets are currently simply not big enough to make money laundering practices attractive.[335] In respect of tax evasion, it might be slightly different. Large-scale tax evasion usually requires so-called tax havens with

[329] J. Baron and coll., op. cit. no. 45, p. 19.

[330] N. Hajdarbegovic, '*Bitcoin Ransomware Now Spreading via Spam Campaigns*' (2015), available at: https://www.coindesk.com/bitcoin-ransomware-now-spreading-via-spam-campaigns/, last accessed 19.8.2018.

[331] S. Gruber, op. cit. no. 311, pp 135-139.

[332] J. Baron, op. cit. no. 45, p. 19.

[333] E.G. Sanchez, op. cit. no. 314, pp 188-189.

[334] S. Robbins, '*Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash*' (2013), available at: https://www.insightcrime.org/news/analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash/, last accessed 19.8.2018.

[335] M. Szczepański, op. cit. no. 79, pp 6-7; C. Kim, '*DEA Agent: Speculators Are Using Bitcoin More Than Criminals*' (2018), available at: https://www.coindesk.com/most-bitcoin-transactions-now-used-for-speculation-not-drugs-report/, last accessed 19.8.2018.

banks which usually impose very strict criteria on bank secrecy.[336] The elimination of need for banks, centralized institutions which, even if mitigated, entail some risks, might make blockchain very suitable for tax evasion.[337]

Taking into account the above mentioned, it is logical that European institutions took steps to prevent and minimize the potentials of criminal activities associated with cryptocurrencies. While one approach is abolition, such decision would be detrimental to future development of modern technologies, namely in respect of financial services, and more importantly, it is not clear whether it would even be possible to truly abolish such decentralized technology.

In 2014 the EBA called for inclusion of cryptocurrency exchanges and eWallet providers in the scope of obliged persons under the anti-money laundering framework due to the fact that these entities are in a position of „gateways" and have access to information relating to transactions while at the same time being centralized and capable of being a single point of contact. In 2016, after terrorist attacks in France, the European Commission initiated[338] negotiations for drafting of the AMLD4[339]. However, the recommendation of the EBA was in the end not implemented in the AMLD4, and while some Member States, e.g. the Czech Republic, voluntarily followed the recommendation and included crypto-providers within the implementation process, in line with Article (4) of the AMLD4[340]; at the EU level, exchanges and eWallet providers have not yet been included.

Eventually, the European Commission realized the error and submitted a proposal of AMLD5 which, among other things, adds crypto exchanges and eWallet providers in the list of obliged persons under the directive, with two important specifications. Firstly, cryptocurrency exchanges which trade only in cryptocurrency, i.e. do not provide services of exchange for fiat currency, do not supposedly fall in the scope of the definition in line with

---

[336] O. Marian, '*Are Cryptocurrencies Super Tax Havens?*' (2013), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863, last accessed 19.8.2018, p. 11.

[337] Ibid, p. 5: "*In cyberspace, financial institutions – the emerging agents of tax collection – are taken out of the picture. Thus, cryptocurrencies have the potential to become* super *tax havens.*"

[338] A. Vondráčková, op. cit. no. 52, p. 7.

[339] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141 (5 June 2015), full text available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32015L0849.

[340] A. Vondráčková, op. cit. no. 52, p. 8.

recital (9) of the AMLD5 which acknowledges that the regulation does have limits.[341] Secondly, the AMLD5 pertains only to "custodian wallet providers", meaning only those eWallet services which exclusively keep their clients' private keys which, however, is not the only possible way of provision of eWallet services.[342] The AMLD5 was adopted on 19 April 2018 and came into effect on 7 July 2018. Member States have until January 2020 to implement its requirements.[343]

Under the AMLD5, the above defined crypto-providers will be obliged to register in line with Article 47(1) of the AMLD5. As follows from the wording of the provision, the registration will not require licensing procedure; therefore, Member States will only be required to maintain lists of crypto-providers operating on their territory, provided that these entities are established on a centralized basis.

In compliance with Article 11 of the AMLD, the crypto-providers will have to fulfill customer due diligence obligations, not only at the time of establishment but also during the course of commercial relationship. Due diligence, also referred to as know-you-customer principle (KYC) under Article 13 AMLD5 implies *inter alia*, identification of the customer[344] and its beneficial owner(s) and political status, if applicable, purpose and nature of the relationship (e.g. risk profile) and ongoing monitoring of suspicious transactions (e.g. without economic purpose, unusually large and/or complex, etc.). In this regard, in line with Article 33 AMLD5 crypto-providers will also have to retain necessary information, report suspicious transactions and cooperate with financial investigation units of Member States and provide information, if and as requested.

---

[341] The AMLD5 defines cryptocurrency exchanges as "*providers engaged in exchange services between virtual currencies and fiat currencies*". Recital (9) states *inter alia*: "*The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers*." See also N. Novak, '*EU Introduces Crypto Anti-Money Laundering Regulation*' [2018], available at: https://medium.com/@nejcnovaklaw/eu-introduces-crypto-anti-money-laundering-regulation-d6ab0ddedd3, last accessed 19.8.2018.

[342] The AMLD5 defines custodian wallet provider as: "*an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies*." See also N. Novak, op. cit. no. 330.

[343] See: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018L0843.

[344] In respect of cryptocurrency providers, Article 13(1)(a) states that identification can be based, among other possibilities, on "*any other secure, remote or electronic identification process regulated, recognized, approved or accepted by the relevant national authorities*" which enable identification on the basis of private keys with respect to eWallet providers.

Finally, under Article 8 of the AMLD they will be obliged to establish internal control and risk assessment and management policies and procedures pertaining to a wide ragnge of risks, such as customers, countries of origin or destination of transaction, nature of services, etc.

According to a recent study[345], 68 % of cryptocurrency exchanges and eWallet providers currently fail to implement satisfying background checks and KYC measures to meet the requirements of the AMLD5.

It should also be noted, that in case that ICO entities are qualified as falling in the scope of issuers of financial instruments and thus, triggering application of the MiFID, they will have to ensure compliance with the AMLD5 as well. This conclusion follows from the ESMA's warning to firms, according to which ICO entities might be qualified as financial institutions under the AMLD5.[346]

### 4.8. Volatility

While legal qualification of cryptocurrencies is mostly not clear, they do represent value, even if prone to volatility. The issue might not be that obvious if we regard cryptocurrencies as a means of exchange in day-to-day transactions, as persons and entities may tend to immediately convert them into fiat currencies[347], but it becomes apparent if they are viewed as an investment instrument which should be able to store value relatively stably.[348]

Sometimes extreme volatility[349] of cryptocurrency prices is the reason why crypto-technologies have many opponents on one hand, who see it as a flaw which will inevitably

---

[345] T. Delahunty, '*Two Thirds of US, EU Crypto Exchanges Fail to Verify Customer Identities*' (2018), available at: https://www.newsbtc.com/2018/06/06/68-of-u-s-eu-cryptocurrency-exchanges-and-wallets-fail-to-verify-customer-identities-research/, last accessed 19.8.2018; A. Hankin, '*Most major cryptocurrency exchanges lack sufficient background checks, research report says*' (2018), available at: https://www.marketwatch.com/story/most-major-cryptocurrency-exchanges-lack-sufficient-background-checks-research-report-says-2018-06-06, last accessed 19.8.2018.

[346] ESMA (2017) firms, op. cit. no. 119; see also N. Novak, op. cit. no. 330.

[347] M. Tsukerman, 'The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future' (2015), 30 Berkeley Tech. L.J. 1127, p. 1133; G. Bonaiuti, *Economic Issues on M-Payments and Bitcoin* in G. Gimigliano, op. cit. 137, p. 41.

[348] J.Brito, A. Castillo, '*Bitcoin: A Primer for Policymakers*' (2013), Mercatus Center, George Mason University, p. 21.

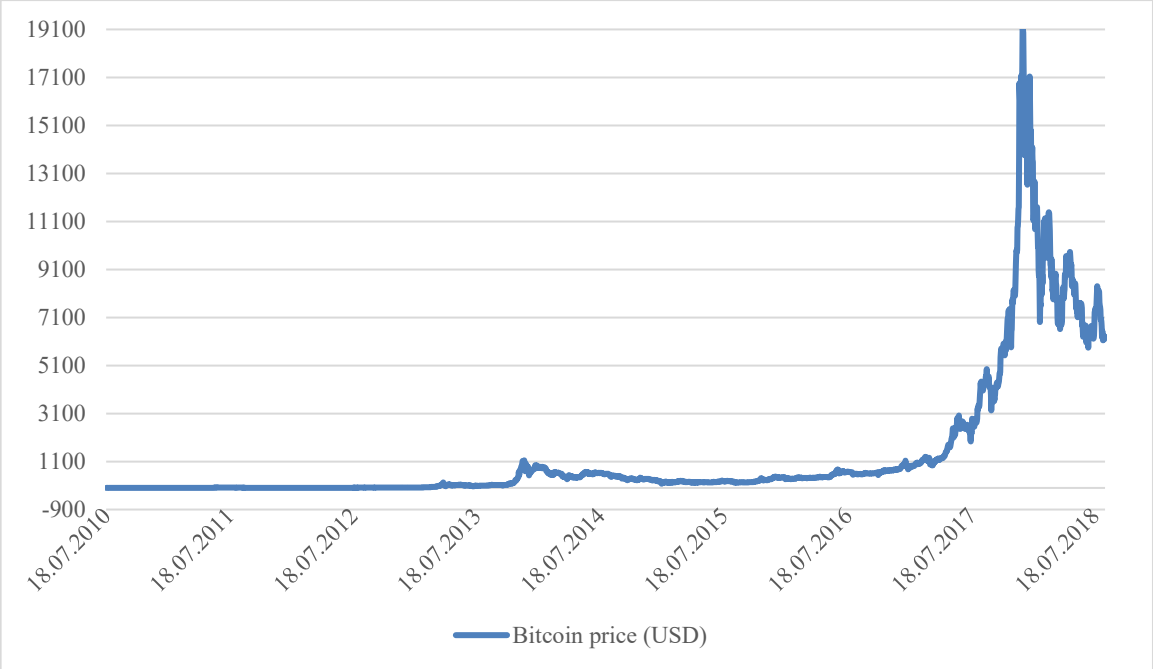
[349] F. M. Ametrano, '*Hayek Money: The Cryptocurrency Price Stability Solution*' (2016), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270, last accessed 19.8.2018, p. 18.

cause failure of Bitcoin[350]. And on the other hand, many supporters who view the instability of market as an opportunity to gain profit. The most obvious reason of volatility is the decentralized nature of cryptocurrencies which principally excludes possibility of external influence and manipulation of market. However, neither is this the sole reason, nor is it an absolute without exceptions. Bitcoin will be used as an example for the following assessment.

As follows from *Figure 2* below, Bitcoin's exchange rate has been relatively stable in the past, as opposed to more recent development. The prices revolved around $300, with the exception of the spike in 2013, which was caused by the Cyprus banking crisis.[351] Nonetheless, with wider adoption and rather positive approaches of many jurisdictions, the price quickly recovered.

*Figure 3* displays how the price of Bitcoin changed over the last year, whereas *Figure 4* depicts the change in the price of Bitcoin in the last three months.

**Figure 2 - Bitcoin (USD) Price (July 2010 - Aug 2018)**

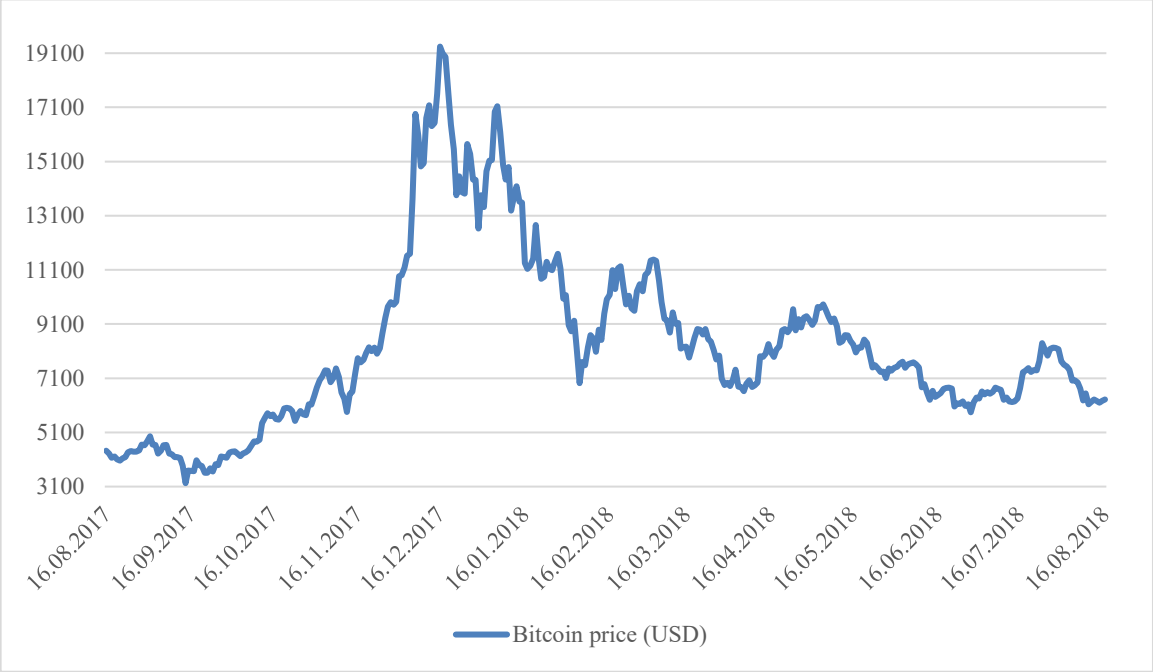



*Source: (Coindesk), own figure processing*

[350] See M. Farrel, '*Strategist predicts end of Bitcoin*' (2013), available at: https://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html, last accessed 19.8.2018.

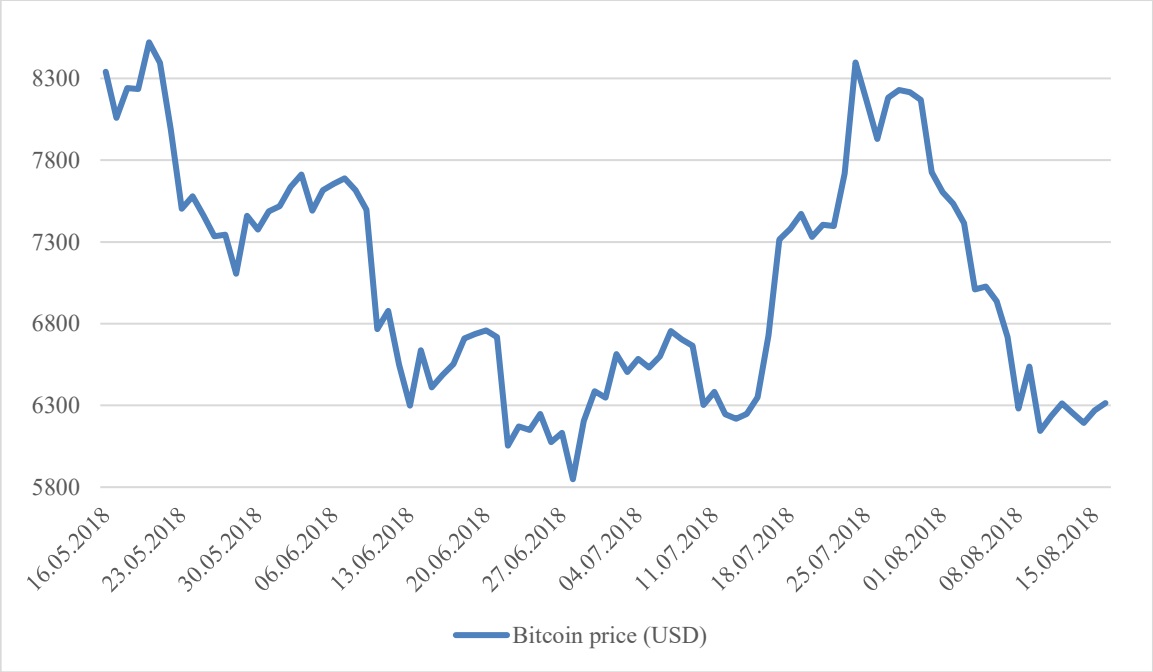
[351] M. Swan, op. cit. no. 38, p. 5.

**Figure 3 - Bitcoin (USD) Price (Aug 2017 - Aug 2018)**




*Source: (Coindesk), own figure processing*

**Figure 4 - Bitcoin (USD) Price (May 2018 - Aug 2018)**




*Source: (Coindesk), own figure processing*

In 2012 the ECB[352] considered 5 major factors which affect the price volatility. Firstly, it is the supply of money and other issuer's actions. As was stated above, Bitcoin is an example of cryptocurrency with fixed money supply. This means that when the total amount of Bitcoins is mined, approximately in 2140, there will not be a possibility to issue more in case it is needed.[353] Fixed supply has a deflationary effect. It might cause the price to continue to grow, provided that public's demand will grow as well, and it may due to the growth of price, which in turn causes the decrease of all other prices in general. In the end it might even lead to deep economic crisis.[354] While according to some authors, deflationary effect is to some extent natural and could be balanced by opposing economic effects present on crypto-markets[355], national central banks usually artificially prevent growth of value of currency in fear of crisis. Any kind of interventionist monetary policy in time of crisis is simply impossible with Bitcoin.[356] Nonetheless, certain actions of core developers and key personnel may have similar effects, namely due to the fact that in the end they decide how the system will be upgraded and what kind of fork will be implemented. These decisions strongly influence users' demand for the cryptocurrency and consequently, its price.[357]

Secondly, according to the ECB, the market volatility is also caused by the size of the network[358], i.e. smaller currencies with fewer users exhibit stronger volatility and *vice versa*. Such conclusion is also supported by economists – as long as users do not conduct economic calculations in Bitcoins, i.e. do not grow accustomed to it similarly to traditional currencies, Bitcoin cannot fully stabilize.[359]

---

[352] ECB (2012), op. cit. no. 46, p. 38.

[353] F. M. Ametrano, op. cit. no. 338, p. 18.

[354] D. Stroukal, J. Skalický, *Bitcoin: peníze budoucnosti* (1st ed., Ludwig von Mises Institut, 2015), pp 123-124: This effect is called deflationary spiral.; T. I. Kiviat, op. cit. no. 45, p. 583.

[355] D. Stroukal, J. Skalický, op. cit. no. 343, pp 123-125: Opposite effect - If users continue to buy and stash Bitcoins because their value continues to grow, at some point there would just not be enough of them and the demand would switch to another cryptocurrency, which in turn would decrease the Bitcoin's value. See also F. M. Ametrano, op. cit. no. 338.

[356] C. M. Christopher, '*The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*' (2016), 17 Nev. L.J. 139, p. 152.

[357] M. Atzori, op. cit. no 229, p.16.

[358] ECB (2012), op. cit. no 46, p. 38.

[359] D. Stroukal, J. Skalický, op. cit. no. 343, p. 121.

Third factor is the level of trust of the general public which the cryptocurrency can generate and based on the opinion of the ECB. It mainly depends on cryptocurrency's "institutional conditions", i.e. internal settings, transparent polities, etc.[360]

Fourth aspect is the issuer's reputation. Lastly, fifth factor involves in speculative practices and attack scandals generally connected to cryptocurrencies.[361]

While the above mentioned are certainly valid factors which do affect frequent spikes of Bitcoin's value, there seem to be other circumstances not included by the ECB. In particular, ambiguous regulatory environment across various jurisdictions does not help stabilizing the market. Although there are different approaches in terms of legal qualification and the extent of necessary regulation, it seems that similarly, as different jurisdictions take time to follow and observe the evolution of crypto-market before enacting any specific rules and procedures, the market itself will need time to adapt to these different stances and crystallize into a norm. In this regard, as a relatively new and small market, the crypto-market also exhibits high sensitivity to media outlets and slightest changes of public and especially government opinions. Consequently, the size of the market, the number of users and this sensitivity are an easy target for those who intend and are in the position to manipulate the market for personal gain, e.g. via insider information following ICOs, etc.

Simple solution to the volatility issue, which is often proposed, is to change the supply policy.[362] While it should be possible to force a hard fork of the system to this effect, it might end in catastrophic results in terms of user support. It is clear that fixed supply was something that was intended by Satoshi Nakamoto from the very beginning, likely with the intention to approximate Bitcoin to gold and differentiate it from traditional currencies strictly controlled by governments. The purpose of Bitcoin was to be free, independent of external influences. While this proves to be unattainable, Bitcoin and other cryptocurrencies are increasingly adopted by wider population in spite of their volatility and numerous warnings by government authorities. Apart from speculation and lowered transaction costs, one of the reasons might be

[360] ECB (2012), op. cit. no. 46, p. 38.

[361] ECB (2012), op. cit. no. 46, p. 38.

[362] F. M. Ametrano, op. cit. no. 338.

that even if unstable, in some cases, cryptocurrencies prove to be capable of storing value more that some traditional currencies, such as Venezuelan bolívar.[363]

Another suggested solution is pegging the Bitcoin (or other cryptocurrencies) to one traditional currency. It should be noted that in such case, the cryptocurrency would be dependent on all factors influencing the value of the traditional currency, such as government decision-making or international relations, as traditional currencies are not fully independent either. [364] While this solution cannot work in connection with fixed supply, some view it as a compromise and potential future development which might be useful for all cryptocurrencies in times of crisis.[365] Recently established EURS might serve as an example of crypto-EUR relation. Its issuers hope to fulfill all requirements of Maltese new regulation package.[366]

### 4.9. RegTech and Corporate Solutions

Unlike FinTech sector, RechTech companies do not want to compete with financial institutions; instead their business model is aimed at development of solutions for financial and other regulated entities in order to ensure compliance with regulatory requirements.[367] The primary reason is the cost-saving. According to Santander, "*blockchain technology could reduce banks' infrastructure costs by USD 20 billion annually*."[368]

Blockchain technology, especially in its permissioned form which is more suitable for sensitive financial data, could be beneficial in respect of all requirements based on client identification, screening and transaction monitoring.[369] Clients could be generated digital identities, including their ownership shares and interests which would then help identify

---

[363] See K. B. II Haesly, op. cit no 103, p. 268.

[364] J. Baron and coll., op. cit. no. 45, p. 7.

[365] C. Masters, '*Stasis Launches Euro-Pegged Stablecoin EURS on DSX Exchange*' (2018), available at: https://cryptovest.com/news/stasis-launches-euro-pegged-stablecoin-eurs-on-dsx-exchange/, last accessed 19.8.2018.

[366] G. Fenech, '*Crypto Exchange HitBTC Adds Support for Euro-Pegged Stablecoin 'EURS"* (2018), available at: https://www.ccn.com/crypto-exchange-hitbtc-adds-support-for-euro-pegged-stablecoin-eurs/, last accessed 19.8.2018; G. Fenech, '*Stasis Onboards First Institutional Client for EURS Stablecoin*', available at: https://www.ccn.com/stasis-onboards-first-institutional-client-for-eurs-stablecoin/, last accessed 19.8.2018, Other examples include EURT or USDT – see C. Masters, op. cit. no. 354.

[367] Y. Lootsma, '*Blockchain as the Newest Rechtech Application – the Opportunity to Reduce the Burden of KYC for Financial Institutions*' (2017), Banking & Financial Services Policy Report, Vol. 36, Number 8, 16, p. 17

[368] R. L. Stanley, R. P. Buckley, 'Protecting *the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses*' (2016), 17 Melb. J. Int'l L. 83, p. 105.

[369] Y. Lootsma, op. cit. no. 356, p. 17.

ultimate beneficial owners and report suspicious transactions. These requirements are usually referred to as know-your-customer (KYC) principle and are the basis of many regulations, such as AMLD5 or PSD2.[370] A peculiar fact should be emphasized – while it is not clear how permissionless blockchain as a FinTech solution may fulfill regulatory requirements, interestingly, permissioned RechTech version is suitable to be used as a tool for complying with the same requirements.

Furthermore, as the regulated institutions are in some instances required to share data[371], projects based on closed blockchains with authenticated participants that can create their own private blockchains may serve as a solution. In order to ensure sufficient protection of privacy and sensitive information[372], the common blockchain can contain only reference data and subsequently serve as a dispute settlement instrument.[373] An example might be the *Hyperledger* project with IBM as the leader of development which ensures "*confidentiality, transparency, flexibility and scalability*."[374] International interbanking system SWIFT has announced that it will initiate a trial using *Hyperledger* within the platform.[375]

Blockchain has also a range of options in the corporate governance, namely as was stated above, blockchain can simplify shareholder decision-making (remote general meeting), and also can monitor company stock distribution and transactions for the accounting and auditing purposes.[376] If implemented, it could mitigate risks of insider trading and hostile takeovers.[377]

### 4.10. Social and Psychological Obstacles

Perhaps the least heavy but still significant obstacle standing in the way of mass adoption of blockchain-based currencies, applications and other technologies is the general

[370] Ibid, p. 18.

[371] A. Felländer and coll., op. cit. no. 52, p. 160.

[372] Y. Lootsma, op. cit. no. 356, p. 19; For privacy considerations in terms of KYC principle, see also A. Biryukov, D. Khovratovich, S. Tikhomirov, '*Privacy-preserving KYC on Ethereum*' [2018], Reports of the European Society for Socially Embedded Technologies, ISSN: 2510-1591.

[373] A. M. Puertas, R. Teigland, op. cit. no. 101, p. 295.

[374] A. M. Puertas, R. Teigland, op. cit. no. 101, p. 295; see also N. Acheson, '*PSD2 and the blockchain*' (2017), available at: http://www.fintechblue.com/2017/05/psd2-and-the-blockchain/, last accessed 19.8.2018.

[375] A. M. Puertas, R. Teigland, op. cit. no. 101, p. 295.

[376] Ibid, p. 296.

[377] Ibid, p. 296.

feeling that blockchain represents something far too complicated and alien for an average person. Indeed, the peer-to-peer transaction system based on encryption, private keys and fairly volatile tokens of value has mostly not yet become very user-friendly, even though a basic human error while handling the system may lead to grave consequences. Public and especially private keys represent crucial pieces of information which, if lost, lead to loss of access to the crypto-balance. A person averagely acquainted with computer technology does not anticipate that he or she will be required to memorize a particularly long illogical set of letters and numbers serving as something like a password, in order to access his or her financial resources. Yes, as a society we have grown more accustomed to more demanding criteria in terms of log-ins, passwords and other access data, namely in connection with internet banking; however we can rest assured that if we by any chance forget a part of our access data, there will always be someone who will help us recover them or change them.

This role has traditionally been assigned to banks and other financial institutions watching over our savings. No such role is present in blockchain-based systems. While the solution, to a certain degree, might lie in eWallet software, two additional issues are connected. Firstly, some access data has to be established in order to secure the eWallet itself, thus users will inevitably have to memorize some data, albeit chosen by them (if we set aside the possibility of access by a fingerprint[378]). Secondly, eWallet in principle represents centralization and as such might raise security issues.

Nonetheless, there are already companies, such as Circle Internet Financial or Xapo coming up with ideas "*with the goal of being the 'Gmail of Bitcoin' in terms of frontend usability - and market share*".[379]

[378] M. Swan, op. cit. no. 38, p. XV: "*The current ewallet security standard is now widely thought to be* multisig *(using multiple key signatures to approve a transaction), but most users (still early adopters, not mainstream) have not yet upgraded to this level of security."*

[379] M. Swan, op. cit. no. 38, p. XIII.

## Conclusion

The decentralized nature of blockchain is the main reason why it is difficult to categorize blockchain even though networks are generally nothing new for any given legal system. This applies especially to permissionless blockchains which, under normal circumstances, cannot be controlled by any centralized entity. This aspect will pose problems, regardless whether the blockchain-based solution is used as e.g. payment service or IP rights management solution.

I have shown in this master's thesis that the first major obstacle standing in way of future mass adoption of blockchain technology is its legal definition. Although cryptocurrencies are only a part of the whole blockchain concept, their volatility and use for investment purposes makes them particularly sensitive in terms of consumer protection which consequently triggers the attention of regulators. I have presented the opinions of Member States and EU institutions which are not always conclusive. Namely, the CJEU's reasoning in the *Hedqvist* case will likely have further consequences for legal qualification of cryptocurrency in individual Member States. Moreover, with the newest enactment of the AMLD5 and conclusion of some crypto-providers in the scope of obliged persons, we can anticipate more CJEU judgments and further development in terms of legal qualification and subsequent related regulatory framework. However, as I have demonstrated, even if permissionless blockchains are considered as payment instruments, application of PSD2 will be difficult, as due to the decentralized nature, there are essentially no specific payment providers. It is thus more likely that unless relevant authorities decide to ban permissionless blockchain altogether, cryptocurrencies and related services and instruments will remain unregulated to a large extent.

In terms of smart contracts, I have established that it would not be simple to implement them as true contracts within the traditional principles of contract law. In particular, parties to a smart contract will face difficulties should they request judicial review. Apart from obvious concerns which lie in the court's inability to read code or evidentiary complications, I expect that many legal researchers will focus on the jurisdiction problem in the near future.

From the presented overview of ten particular aspects of blockchain, in my opinion, most regard will have to be given to the security issue and protection of personal data which are the two areas that need considerable development to be considered safe and compliant with applicable legislation. Another potentially very complicated situation might occur if a

(eurozone) Member State adopts a cryptocurrency as its legal tender. In such areas, it might be more efficient and convenient if a common action is taken at the European level.

On the other hand, I have shown that many concerns which are nowadays most discussed, such as the volatility, capacity or energy consumption and which are certainly important, seem to be gradually getting resolved on their own, as the market grows, or by developers and enthusiasts alike due to the open source nature of the code. Therefore, some issues like the latter group will not require the regulators to step in.

Whatever the future development and approach of European and Member States' legislators might be, I believe that blockchain should only be regulated on the basis of the particular utilization and purpose and not as a technology in general. While I agree with opinions of EU institutions that cryptocurrencies and other blockchain services and instruments may pose grave risks and even graver consequences, over-the-top regulation in fear of such consequences would lead to hindering and detriment of new and exciting technology that can considerably improve and simplify the way we manage not just businesses but even our daily lives. Thus, the current stance taken by the majority of stakeholders in the EU which can be described as wait-and-see-and-step-in-if-necessary might be the right way.

# Annexes

## Annex I. - Detailed Description of Blockchain Technology

Blockchain technology manages to overcome the General's Problem by way of complex mathematical problems which the computers participating in the blockchain – the nodes, seek solution for. The solution to these problems requires substantial computing power. The potential traitor or an attacker wishing to corrupt the recorded information would have to possess the majority of the computational power of the entire network of nodes to be successful with its attack. It is easier for the engaged nodes to trust each other, therefore, not requiring assistance of a third trusted party anymore, thus the designation *trustless*.[380]

That also brings us to the difference between a centralized and decentralized ledger. The decentralized or distributed ledger means that all nodes "*are connected with each other and store all data simultaneously, and together constitute the common ledger. [It] requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device, as with a centralized ledger*."[381] Truly decentralized systems do not differentiate between vertical and horizontal connection, there is no entitled party charged with supervision and control. All participating nodes have equal positions and value in reaching the consensus. There is, however, an exception to this rule. As opposed to the described truly decentralized systems (also called permissionless because not one of the engaged nodes is entitled to give permission), there may also be blockchain systems which are centralized to a certain degree – "permissioned" blockchains. Such blockchain ledgers allow for concentration of power where "*a limited group of actors retain the power to access, check and add transactions to the ledger*".[382] Permissioned blockchains do not need to provide incentives in order to "stay relevant" and functioning; instead, they enable access only to trusted nodes which have other than purely economic interest in the blockchain's functioning.[383] In practice, this approach will be especially interesting to banks or governmental entities wishing to retain some control over the recording process, in particular,

[380] A. Wright, P. de Filippi, op. cit. no. 39, p. 6.

[381] D. A Zetsche and coll., op. cit. no. 188, p. 11.

[382] P. Boucher and coll., op. cit. no. 41, p. 5.

[383] A. M. Puertes, R. Teigland, op. cit. no. 101, p. 300.

in case of very sensitive data. An example of such blockchain protocol of "trusted parties" is Ripple. These trusted parties are then known as "validation nodes"[384].

## 1. Verification Process

In order to be able to comprehend how the consensus between participating nodes is reached and therefore, how the blockchain technology really works, the process of recording of transactions need to be briefly described from the technical point of view. Due to the fact that Bitcoin was the first successful cryptocurrency project, and so far, is the most widely accepted and used cryptocurrency, the following description of how the crypto transactions are made is based on the Bitcoin system.

Firstly, every computer which wants to engage in a blockchain transaction must download the software containing a full and updated copy of the blockchain ledger. Therefore, every participating computer has access to all data recorded in the blockchain ledger up to the first recorded transaction. The ledger is viewable via the Internet[385], is constantly updated, at regular intervals of 10 minutes[386], and every change of the record is automatically known to all computers participating in this *de facto* network. Consequently, any file which is to be recorded in the ledger is compressed to a 64-character code called the *hash*.[387] The hash is like the file's fingerprint, it is unique for the particular file, i.e. package of information, and no two hashes (made from different files) are the same. Moreover, even though one file can be transformed in multiple copies of hashes, the file's hash cannot be transformed back to the file; it is not reversible. As the next step, the compressed hash of the file is given a time stamp and then inserted to be recorded. Provided that the operation consists in a simple payment transaction without deployment of smart contracts, the file itself is never submitted to the ledger, it stays in the original computer.

To be registered in the ledger, the transaction needs to be firstly accepted as true and validated by a pre-defined number of nodes. The transaction is true or legitimate, if e.g. "*the*

---

[384] D. A Zetsche and coll., op. cit. no. 188, p. 12.

[385] M. Swan, op. cit. no. 38, p. 2: blockchains can be viewed via the „*block explorers*", specialized internet sites, such as www.blockchain.info for the Bitcoin blockchain.

[386] H. M. Botos, '*A Blockchain Intelligence Analysis*' (2017), 13 Res. & Sci. Today 42.

[387] M. Swan, op. cit. no. 38, p. VIII.

*request comes from the authorized person, the house seller has not already sold the house, and the buyer has not already spent the money*[388]". For this determination, two separate mathematical methods have been developed. The more usual one is the so-called *proof-of-work* and it basically consists in a mathematical operation, a problem which the computers on the blockchain compete to solve. Each transaction proposes a new problem and the first computer to solve it, is subsequently rewarded, apart from the transaction fee, usually by a sliver of the newly made blockchain's cryptocurrency. The remaining nodes of the system then verify that the solution is correct[389]. Once an adequate number of computers[390] confirm the solution to the problem, the transaction is accepted as true and then recorded in the block of transactions which is linked to previous blocks of transactions. As such, they form a long chain of blocks of transactions going all the way back to the first recorded transaction – the *genesis block*[391]. While the designated amount is transferred immediately, it takes approximately 7 minutes for simple and low-amount transactions to be verified through the described process of problem solving. The process is called *mining* and is used in most blockchain protocols, such as Bitcoin, for example. The miners offer their computing power for the solution of problems and therefore, validation of transactions. In exchange, they obtain a portion of transaction fees and some of them, the one solving the problem first, a portion of the newly created token of cryptocurrency as well. These rewards serve as an incentive to ensure that sufficient number of computers keep performing the necessary mathematical operations. "*Without a community of nodes running the protocol and verifying transactions the system stops working. If all the members have moved to a new system all data stored on the blockchain cease to exist*."[392] Therefore, the lack of interest would inevitably entail the destruction of the whole decentralized system.

The second method of validation, the *proof-of-stake*, is based on the "relevance" of participating computers. The determination of which computer will be charged with

[388] P. Boucher and coll., op. cit. no. 41, p. 5.

[389] M. Atzori, op. cit. no. 229: While the *proof-of-work* itself is difficult to produce, as it requires extensive sources of power and time, it is subsequently not demanding to verify its results by other computers.

[390] D. A Zetsche and coll., op. cit. no. 188, p. 12 „*The number of nodes required for the consensus is set in the code underlying the system and is thus a fundamental aspect of the design of any system. This also provides one of the major known vulnerabilities in many blockchain systems, including Bitcoin*. "

[391] M. Swan, op. cit. no. 38, p. X.

[392] D. A Zetsche and coll., op. cit. no. 188, p. 12.

confirming and recording the transaction will depend on the computer's previous transactions and its account balance in the blockchain's cryptocurrency. Essentially, computers which have the most traffic (have analyzed and confirmed most transactions) in the past and thus, have been rewarded most of the distributed cryptocurrency, will be likely chosen to perform the recording successfully again, as they have more interest in well functioning of the system.[393] Due to the fact that such method might lead to significant centralization where only few "mighty" computers will effectively perform all actions, more sophisticated protocols were developed which build on the relevance of the computers (their stake) but combine it with various mathematical methods of selection, including randomization. The biggest advantage of this method is that a lot less energy is necessary for the completion of the recording process. As the computers are not required to "waste" enormous computing power for problem solving and subsequent validation, this approach is considered as more energy efficient and economical (for the energy consumptions issues and consequences, please see section 4.6 of this thesis). For example, Peercoin protocol is based on the proof-of-stake method and Ethereum is supposed to introduce this method in the near future as well.

**Table 1 - Simple overview of main consensus protocols**

| CONSENSUS PROTOCOL | OVERVIEW |
|---|---|
| **Proof of Work** | Uses computational power to validate new blocks of data.<br>To participate in this scheme, participants are required to collate transactions within single block and then apply a hash function with the use of some additional metadata. |
| **Proof of Stake** | Validators (special nodes) voting on valid blocks whilst posting collateral in order to be able to participate in the validation process.<br>Unlike Proof of Work, Proof of Stake relies on proving the user is invested in the underlying token of value of the network being mined rather than being the owner of a large amount of computing power. |
| **Ripple Protocol** | In order to validate new transactions servers amalgamate outstanding |

[393] L. Lee, op. cit. no. 154, p. 29.

| | |
|---|---|
| | transactions into a “candidate list”.<br><br>All participants then vote on valid transactions then be included in the ledger.<br><br>Transactions that meet the 80 % threshold of “yes” votes are included within the following last closed ledger state. |
| **Proof of Elapsed Time** | As part of its Intelledger proposal, Intel has devised a means of establishing a validation lottery that takes advantage of the capability of its CPUs to produce a timestamp cryptographically signed by the hardware.<br><br>Whoever in the chain has the next soonest timestamp will be the one to decide which transactions will be a part of the next block in the chain.<br><br>This consensus method is extremely energy efficient compared to Proof of Work and therefore more adapted to IoT devices. |

*Source: ENISA (2016), op. cit. no. 265, p. 10, own table processing*

After the hash is recorded in the ledger, it is permanent. Unless some unpredictable and unusual circumstances arise, such as a hacker attack, the data can never be amended or erased from the blockchain ledger. All other nodes in the network use the updated version of the blockchain for verification of new transactions which makes the ledger *transparent*. Later, when a stakeholder wishes to prove that the file has not been changed and therefore, is subject to the particular transaction recorded in the blockchain, it is sufficient to make a new 64-character hash of the file and compare it with the one recorded in the ledger. If the code is exactly the same, the file has not been tempered with.

## 2. Forks and Rule of the Longest Chain

In terms of addition of new blocks to the chain of transactions, each node within the network follows the principle of the longest chain, meaning that the node verifying the transaction will always accept a new block which it considers as the continuation of the longest chain. Nonetheless, it is theoretically possible that two different transactions are completed at exactly same time which effectively leads to a split of the chain, also called a fork. This issue is resolved when another node within the network accepts and adds a new block to the end which it deems the longest (for example due to the fact that it adds the block

before it receives information that the chain was split). Therefore, upon this moment one split end becomes longer and all other nodes verifying the following transactions are bound by the longest chain rule and only add blocks to the one longer end of the chain. Blocks of transactions which are set aside and abandoned due to the split resolution are usually referred to as "*orphan blocks*". Nodes whose blocks became orphan blocks eventually lose the right to a reward. The rate of forks and orphan blocks is regarded as one of factors for determination of the level of security of the whole network, as they often occur at the times of "*double-spend attacks*"[394] when the relevant node attempts to spend the same tokens of cryptocurrency twice, i.e. for two separate transactions. "*A node can decide to broadcast a transaction in one block, and if the transaction value is high enough, it can try to broadcast another transaction spending the same Bitcoins in another block. To invalidate the first transaction, it needs to create a chain of blocks that is longer than the chain that already contains the first transaction. This in turn creates an increase in orphaned blocks independent of the success of the attack. Furthermore, a system that naturally has a high rate of orphan blocks is more vulnerable to double-spend attacks. This is due to the fact that a forked chain reduces the number of blocks that the attacker needs to create in order to invalidate one of its own transactions.*" Such attacks are, however, immensely energy consuming.[395]

On the other hand, some forks of the chain may be intentional and legitimate. The particular design of the ledger system and all its properties, including the requirements for consensus, are set up by a group of core code developers who *de facto* represent administrators of the system. They are constantly developing and improving the software, similar to internet applications. Each major update of the blockchain system (namely but not limited to cryptocurrencies such as Bitcoin) is referred to as "*hard fork*" and all users are requested to download the latest version of the software[396]. Due to the fact that the majority of blockchain-based software is open source, the entire community of blockchain enthusiasts is allowed to participate in further improvement of the software. What's more, each node may independently decide on the version of software (the particular fork) it supports and follows

[394] For detailed description of double-spending please see M. Rosenfeld, '*Analysis of hashrate-based double-spending*' (2012), Cornell University Library, available at: https://arxiv.org/abs/1402.2009, last accessed 19.8.2018.

[395] H. Holmberg op. cit. no. 287, p. 313.

[396] D. A Zetsche and coll., op. cit. no. 188, p. 21.

which it signals to other nodes when connected to the network.[397] Due to the fact that each upgrade of the network by way of a hard fork needs support of the majority, otherwise it is "doomed to fail", this has been referred to as a *de facto* type of direct democracy.[398] However, even though the core developers usually do take into account suggestions and complaints of individuals and entities, the decision-making regarding the development rests with them. This aspect of so-called "*key personnel*" can potentially have negative effects, in particular with respect to the security of the system[399] (please see section 4.4.7 of this thesis).

### 3. Cryptography

Nonetheless, another piece of the puzzle is crucial for mainstream acceptance of blockchain and that is the encryption. The encryption ensures pseudonymization, i.e. separation of identifiers which are the data that identify or may identify a natural person. For these reasons, every person that opens an account with cryptocurrency and wants to perform a blockchain transaction is automatically assigned two pieces of information: (i) public key, or more precisely public address, and (ii) private key. Only the public key is registered in the ledger and unless the private key is leaked or openly connected to the public key by the particular person, no one can identify the concerned person (for more details regarding the encryption, please see **Annex II. - Cryptocurrencies and Financial Services**).

[397] H. Holmberg op. cit. no. 287, p. 319.

[398] Ibid, pp 319, 321.

[399] D. A Zetsche and coll., op. cit. no. 188, p. 19.

## Annex II. - Cryptocurrencies and Financial Services

For the sake of completeness, cryptocurrencies based on Bitcoin and Satoshi's manual are usually called alt-coins (derived from the word *alternative*). Further, some authors differentiate between different alt-coins based on their inherent purpose.[400] Firstly, alt-coins which have been designed for the same purposes as Bitcoin, that is to serve as a means of payment in a decentralized transaction system are referred to as pure alt-coins, or simply alt-coins. Secondly, cryptocurrencies with focus on privacy can be referred to as anonymous coins and thirdly, cryptocurrencies which only use blockchain transaction systems as an underlying layer which they build on for additional purposes can be referred as Appcoins.

Although the Bitcoin is not the first digital currency project in history, the Satoshi's paper presents a first solution to the above mentioned *Byzantine General's Problem* by creating a decentralized network which does not require trust towards an intermediary. Furthermore, it solves the previously unsolvable *Double-Spend Problem.* "*Until blockchain cryptography, digital cash was, like any other digital asset, infinitely copiable (like our ability to save an email attachment any number of times), and there was no way to confirm that a certain batch of digital cash had not already been spent without a central intermediary*."[401] It follows that an intermediary was not only necessary to establish trust between the involved parties but also to prevent fraudulent activities consisting in transferring the digital cash intended for the payment several times to several individuals.

For ensuring that one token of digital currency is not used twice at the same time Satoshi combines the BitTorent protocol for peer-to-peer file sharing and encryption technology based on unique private key solely known and available to the users themselves.[402] What should be emphasized is that no special account needs to be opened in order to be able to participate in a decentralized transaction system, such as the Bitcoin. Every user is given a public address which serves as an identificator of the particular person when another person sends them digital money. In the traditional transaction system the public address corresponds to the bank account number. For example in the Bitcoin system, the

[400] J. Baron and coll., op. cit. no. 45, pp15-16.

[401] M. Swan, op. cit. no. 38, p. 2.

[402] Ibid, p. 2.

public address is composed of 26 to 34 alphanumeric characters, such as 1JDQ5KSqUTBo5M3GUPx8vm9134eJRosLoH which can also have the form of a QR code.[403] It is practically impossible that two individuals are generated the same public address.[404]

On the other hand, the private key paired to the public address represents a secret code, which is never given away by the user and its sole purpose is identification of the user, i.e. to assign the particular digital cash balance to the particular person. The private key is usually a 256-bit number and is even longer than the public address shown above as an example.[405] Without the private key the user cannot access its digital finances and cannot proceed with transacting a sum to another person's public address.[406]

In addition to this information, a person must have a computer and internet access to either become a full node within the network or to use SPV software relying on other nodes; nothing else is necessary for a blockchain transaction. Nevertheless, the private key represents an extremely sensitive piece of information – there is "*no customer service number to call for password recovery or private key backup*"[407]. If it is lost, there is no way it can be recovered, and thus, all digital cash is lost as well. As a consequence, other software has been developed to ensure safe-keeping of private keys. This software is usually referred to as *eWallet*[408] and apart from the public address and private key, it may also include a part of the blockchain database relating to the user's past transactions, similar to a statement of account. One eWallet may keep access information to more than one transaction system and more than one cryptocurrency. Examples of eWallets include ChromaWallet, Counterwallet or OneWallet. The eWallets also help to make the blockchain system more user-friendly, as instead of

[403] Ibid, p. 97.

[404] Ibid, pp 98-99: Upon registration, the pair of public and private key is generated first, on the basis of the current standard which is the Elliptic Curve Digital Signature Algorithm. Additional steps are taken for the public address to be generated. Essentially the public key is transformed into a shorter format with assistance of encryption protocols like SHA-256 and RIPEMD-160. While it is technically possible that the same public address is generated for two separate individuals, the odds of such possibility are less than 0,0001 %. Furthermore, potential derivation of the private key based on the public key or public address would be either impossible (one-way hashing operation) or would require extreme computing power and thus, would be extremely expensive.

[405] Ibid, p. 99.

[406] Ibid, p. 3.

[407] Ibid.

[408] Ibid.

remembering the complicated public address and private keys numbers, a person can set up a personalized, sufficiently safe password. However, as shown in section 4.4.4 of this thesis, they can also represent concentration and centralization to a certain degree which may consequently result in formation of new "honeypots" – hackers' targets.

In regard to mainstream acceptance of Bitcoin and other virtual currencies, a vendor wishing to accept cryptocurrencies must dispose with a particular payment processing solution (as it is not reasonable to expect usual consumers to pay for a cup of coffee via Internet). In the traditional sense of payment this solution corresponds to a credit card terminal, as an interface capable of reading the customer's public address and interacting with his eWallet.[409]. Some of the most common merchant solutions include BitPay and Coinbase in the United States. Coinbase has also recently started to provide an eShop, i.e. eCommerce, solution for integration of Coinbase payment option in the checkout process[410]. In Europe, e.g. BitcoinPay enables operation with many traditional currencies, including CZK. Another solution, CoinGate also offers mobile processing of payments.[411]

While it is definitely useful that the above mentioned payment processing solutions provide for immediate exchange of Bitcoins into traditional currency, such as euros, for most small businesses it will probably rather pose an obstacle than a convenience to install additional forms of payments, even more so if we take into account the current instability of the majority of virtual currencies (for more details on the issue if instability of altcoins, please see section 4.8 of this thesis). For these reasons, one of the foremost areas of focus for future development might be providing a solution capable of combining traditional and decentralized payment processing solutions.[412] Among first steps in this direction is BitPay VISA Prepaid

[409] As follows from the Bitcoin's official website, "*some Bitcoin merchant solutions also provide invoices and easy to use Point-Of-Sale (POS) applications that run on a smart phone or tablet. Many merchant processors instantly convert the Bitcoin payment to your local currency at the current exchange rate. There are also a number of stand-alone tools available online for merchants to identify the current conversion rate quickly if needed*". Please see '*Merchant Solutions*', available at: https://www.bitcoin.com/merchant-solutions/, last accessed 19.8.2018, for further description and list of merchant solutions.

[410] Please see L. Shen, '*Meet 'Paypal for Crypto,' a New Way to Pay With Bitcoin and Litecoin*' (2018), available at: http://fortune.com/2018/02/15/bitcoin-paypal-coinbase-commerce/, last accessed 19.8.2018 and '*Coinbase Commerce –the Easiest Way for Merchants to Accept Digital Currency*' [2018], available at: https://medium.com/@coinbasecommerce/coinbase-commerce-the-easiest-way-for-merchants-to-accept-digital-currency-54ba64966f8d, last accessed 19.8.2018.

[411] In respect of mobile processing by way of an application for iOS or Android, some of the most common, apart from CoinGate, are European XBTerminal and Coinify.

[412] M. Swan, op. cit. no. 38, p. 4.

Card project which enables the consumer to pay in Bitcoins at every vendor place accepting VISA credit and debit cards.[413] This solution definitely represents one of the first steps of "rapprochement" of traditional and decentralized payment systems.

With respect to purchase of Bitcoins, the Bitcoin's official website provides a list of "*places to buy Bitcoin in exchange for other currencies*". Some of the prominent international exchanges include Kraken or Bitstamp while others, such as BitPanda or BL3P are focused on the European market.[414]

While not technically an exchange, Bitcoin trading places, such as Coinbase, provide exchange services as well. Their customers can buy and sell Bitcoins and other virtual currencies. For these purposes Coinbase has enabled transferring of funds via credit and debit cards and even PayPal[415], however only within the US market. PayPal, with more than 227 million active users[416], was prohibiting usage of their payment processing services for the purposes of *de facto* exchange operation in the past, however they have since then changed their stance and are now cooperating with Coinbase so that the users of Coinbase can now sell Bitcoin and receive payments via their PayPal accounts.[417] PayPal has even acquired a subsidiary Braintree for the purpose of enabling their users to pay for Uber rides or Airbnb rentals with Bitcoin.[418] As of March 2018, there have been reports that the company even filed for a patent with the US patent office with the objective of speeding up the decentralized transaction processing time.[419] The long processing time of transactions remains an obstacle

[413] However, the BitPay card itself does not process the payment in Bitcoins. It is a two-step process. Firstly, the BitPay card is directly connected to the individual's BitPay eWallet and can be "loaded" with Bitcoins via said eWallet. However, it can also be loaded with US dollars. Secondly, the payment is made in US dollars. All Bitcoins which were transferred to the BitPay Card are exchanged to US dollars under current exchange rate. The balance is subsequently always kept in US dollars and the consumer is free to use the card like a usual payment card or even withdraw US dollars in cash from an ATM machine. For further information on BitPay Visa Prepaid Card please see: '*Load dollars using your Bitcoin wallet, spend anywhere*', available at: https://bitpay.com/card/, last accessed 19.8.2018.

[414] Please see '*Bitcoin exchanges*', available at: https://bitcoin.org/en/exchanges, last accessed 19.8.2018.

[415] Please see '*Coinbase adds support for PayPal and Credit Cards*' (2016), available at: https://blog.coinbase.com/coinbase-adds-support-for-paypal-and-credit-cards-21968661d508, last accessed 19.8.2018.

[416] Numbers for 2017, reports from '*PayPal Reports Fourth Quarter and Full Year 2017 Results*' (2018), https://investor.paypal-corp.com/releasedetail.cfm?ReleaseID=1055924, last accessed 19.8.2018.

[417] Please see I. Kar, '*PayPal is warming up to bitcoin*' (2016), available at: https://qz.com/713528/paypal-is-warming-up-to-bitcoin/, last accessed 19.8.2018.

[418] M. Swan, op. cit. no. 38, p. 11.

[419] Please see J. Wilmoth, '*PayPal Files Patent to Improve Cryptocurrency Transaction Times*' (2018), available at: https://www.ccn.com/paypal-files-patent-improve-cryptocurrency-transaction-times/, last accessed 19.8.2018.

to mainstream acceptance and use of cryptocurrencies, for more details please see section 4.5 of this thesis.

## Annex III. – Ripple

Bitcoin is not the only representative of cryptocurrencies. In order to describe the differences between centralized and decentralized transaction systems, this section will briefly focus on Ripple (i.e. Ripple Protocol Consensus Algorithm) as a representative of semi-centralized transaction systems[420].

Ripple shares some basic features and setting with Bitcoin. It is also based on a decentralized ledger, public and private keys and very similar encryption. However, a node does not have to download the whole content of the ledger. Ripple tries to prevent "bloating" and capacity issues by implementing two ledgers – one contains all transactions in Ripple currency (XRP), similarly to Bitcoin (referred to as "state tree"), the other, however, contains only most recent transactions confirmed by the network (called "transaction tree").

In 2004, when the Ripple system was first presented, it had yet not acquired features of blockchains as per Bitcoin's design and was essentially based on limited trust. Each node had to trust at least one other node which then had its own mini network of trusted nodes (frequently compared to Facebook friends network). Transactions were then processed even between complete strangers connected by chain of "friends". The currency was created as corresponding to debts resulting from nodes' interaction.[421] Nonetheless, the system did not grow as expected and in 2012 the network got "blockchainized". As a result, users can chose from two ways of transaction processing: either they know the sender and thus can transact directly, or they do not know or trust the sender and use a gateway. Gateways, while not necessary required, are usually exchanges/trading places which have earned the trust of the network and ensure safe processing.

The most interesting part is that Ripple does not require mining because the consensus is not reached by a proof. Instead each node in the network has a list of trusted nodes "*that are not likely to collude against them*" which is called a UNL ("unique node list"). A consensus is reached by voting – nodes compare the latest version of the ledger and then vote which transaction was received soonest, which is true etc. Due to the fact that nodes vote only

[420] The description of the Ripple network is primarily based on V. Buterin, '*Introducing Ripple: A Detailed Look at Cryptocurrency's New Kid on the Block*' (2013), available at: https://bitcoinmagazine.com/articles/introducing-ripple/, last accessed 19.8.2018.

[421] For more detailed explanation see Ibid.

when one of their UNL nodes is involved, the majority (80 %[422]) and consensus are reached very quickly, in a matter of few seconds. This gives Ripple a major edge over Bitcoin and other similar systems – validation of transactions is a lot more energy efficient. From another point of view, there might also be certain consequences. For instance, as Ripple does not need mining and does not provide incentives, its total supply of XRP 100 billion is owned by the founder and will be slowly distributed firstly among users and then among the general public, probably on the basis of auction.[423] This entails significant deflationary effect.[424] Also, while Ripple is well adapted for currency exchange services[425] and payment services and cooperation with financial institutions, such as the example of *Fidor Bank* in Germany, as the network imposes a minimal transaction value threshold (XRP 50, for creation of address XRP 200), the system is not suitable for micropayments, e.g. in connection with IoT. This only proves the vast versatility of the blockchain technology and the fact that not every blockchain is the same.

[422] A. M. Puertas, R. Teigland, op. cit. no. 101, p. 286.

[423] Ibid, p. 286: "*As of 2017, Ripple has sold XRP 40billion. In May 2017, Ripple announced that they would place XRP 55 billion in an escrow account with a precise schedule to eliminate the fear of an unexpected shock in the money supply. The escrow account contains 55 contracts of XRP 1 billion that expire on the first day of every month. The amount that is not sold is returned to the escrow account and offered after the original 55 contracts have expired.*"

[424] V. Buterin, op. cit. no. 410: "*Unlike BTC, where the total number of currency units in existence increases more and more slowly with every passing year until eventually stabilizing at a permanent 21 million in 2140, the number of XRP starts off at an all-time maximum of 100 billion and then immediately starts permanently decreasing as transaction fees are paid*."

[425] L. Lee, op. cit. no. 154, p. 32.

## Annex IV. – Ethereum

Ethereum is based on a blockchain ledger which works similarly to the one of Bitcoin with the rule of the longest chain and currently deployed proof-of-work mechanism for confirmation of transactions and creation of blocks. It might be worth to mention that Ethereum is planning to switch to proof-of-stake with its upgrade called *Casper*.[426] Ethereum ensures adoption of new confirmation mechanism by making the proof-of-work exponentially more difficult, until it becomes virtually impossible.[427] The miners are rewarded in Ether which is the platform's currency, also similarly to Bitcoin. But that is where the similarities end.

Firstly, transaction fees are not just based on the size of a block. Ethereum comes up with a more sophisticated solution, in order to mitigate or make up for the amounts of computational energy that are wasted for the proof-of-work mechanism. In particular, users have to pay for that energy upfront by way of a fee called gas. Gas is like a fuel for processing of the transaction and is paid in Ether. Due to the fact that Ethereum is primarily intended for self-executing contracts, the more complicated the execution of contract, the more gas is needed during its life-cycle. If a smart contract runs out of gas, the contract is not executed. On the other hand, if some amount of gas is left after all actions in a smart contract have been completed the rest is given back to the originator of the transaction. This is why gas has also been referred to as *execution fee*.[428] Furthermore, the amount of gas can also affect the speed of processing, namely, if the transaction fees are higher, the likelihood that it will be picked up by one of the miners is higher as well.[429]

Secondly, the processing time in Ethereum can be measured in seconds, i.e. the problems which miners have to solve are not as difficult as in Bitcoin.[430] This raises doubts in relation to orphan blocks and double-spend attacks. The higher orphan rates were resolved by

---

[426] I. Bashir, op. cit. no. 157, p. 249: "*An Algorithm named Casper has been developed, which will replace the existing Proof of Work in Ethereum. This is a security deposit based on the economic protocol where nodes are required to place a security deposit before they can produce blocks. Nodes have been named bonded validators in Casper, whereas the act of placing the security deposit is named bonding.*"

[427] Ibid, p. 244

[428] Ibid, pp 214-245.

[429] Ibid, p. 245.

[430] A. M .Puerstas, R. Teigland, op. cit. no. 101, p. 293.

implementation of stale blocks which are added to calculations to ensure that longest chains are the true ones.[431]

Thirdly, due to Ethereum's focus on smart contracts, the network has two kinds of accounts: (i) so-called externally owned accounts which can only send transactions, similarly to Bitcoin, and cannot execute a code of smart contract, and (ii) contract accounts which can execute smart contracts. However, the distinction should be removed in the near future and all accounts should be enabled to execute smart contracts.[432]

Fourthly, it uses a Turing-complete protocol on top of the blockchain layer. Turing-completeness refers to an "*ability to run any coin, protocol, or blockchain*"[433] and is ensured by Ehtereum's programming language called Solidity which has been often compared to JavaScript, the basis of many applications, such as Gmail or Facebook.[434] The language is stack-based, not binary like Bitcoin which is what enables creation and execution of smart contracts, as it enables unlimited number of contract stages. "*With Bitcoin, the transactions are binary – the Bitcoins are either spent or not spent. With Ethereum, the contract does not have to be fulfilled or not fulfilled, but can be in stage one pre-negotiation, stage two offer, etc.*"[435] Another thing which makes Solidity well-suited for smart contracts is that it is contract-oriented (as opposed to object-oriented) which enables it to understand "*concepts such as identity, ownership, and protection forms*."[436]

[431] I. Bashir, op. cit. no. 157, p. 214. The stale blocks are referred to as Uncles or Ommers in Ethereum.

[432] Ibid, p. 236.

[433] M. Swan, op. cit. no. 38, p. 21.

[434] L .Lee, op. cit. no. 154, p. 114; also A. M. Puertas, R. Teigland, op. cit. no. 101, p. 292.

[435] L. Lee, op. cit. no. 154, p. 115.

[436] A. M. Puerstas, R. Teigland, op. cit. no. 101, p. 292.

## List of Abbreviations

| | |
|---|---|
| **AIFMD** | Alternative investment fund managers directive |
| **AML** | Anti-money laundering |
| **AMLD** | Anti-money laundering directive |
| **BTC** | Bitcoin cryptocurrency |
| **CEO** | Chief executive officer |
| **CFD** | Cryptocurrency contracts for differences |
| **CJEU** | Court of Justice of the European Union |
| **CPU** | Central processing unit |
| **CZK** | Czech Crowns |
| **DAO** | Decentralized organization |
| **Dapp** | Decentralized application |
| **EBA** | European Banking Authority |
| **ECB** | European Central Bank |
| **EEA** | European Economic Area |
| **ESMA** | European Securities and Markets Authority |
| **ETC** | Ethereum Classic cryptocurrency |
| **ETH** | Ethereum cryptocurrency |
| **EU** | European Union |
| **EUR** | Euro |
| **EVM** | Ethereum virtual machine |
| **GDPR** | General data protection regulation |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **ICO** | Initial coin offering |
| **ID** | Identification |

| | |
|---|---|
| **IoT** | Internet of things |
| **IP** | Intellectual property |
| **IPO** | Initial public offering |
| **IT** | Information technology |
| **KYC principle** | Know-your-customer principle |
| **MiFID** | Markets in financial instruments directive |
| **MP** | Member of Parliament |
| **NIS Directive** | Network and information systems directive |
| **PSD2** | Payment services directive 2 |
| **SEPA** | Single Euro Payments Area |
| **SPV** | Simplified Payment Verification |
| **TEU** | Treaty on European Union |
| **TFEU** | Treaty on Functioning of the European Union |
| **UK** | United Kingdom |
| **UNL** | Unique node list |
| **USA** | United States of America |
| **USD** | US dollar |
| **VAT** | Value added tax |
| **VC** | Virtual cryptocurrency |
| **XRP** | Ripple cryptocurrency |

# Bibliography

## Legal Documents

Consolidated version of the Treaty on European Union (2012)

Consolidated version of the Treaty on the Functioning of the European Union (2012)

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax [2006] OJ L 347 (11 December 2006)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281 (23 November 1995)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167 (22 June 2001)

Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC [2003] OJ L 345 (31 December 2003)

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 [2009] OJ L 267 (10 October 2009)

Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 [2011] OJ L 174 (1 July 2011)

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L 173 (12 June 2014)

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money

laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141 (5 June 2015)

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241 (17 September 2015)

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337(23 December 2015)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194 (19 July 2016)

Directive (EU) 2018/843 of the European Parliement and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156 (19 June 2018)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on copyright in the Digital Single Market, COM/2016/0593 final - 2016/0280 (COD) [2016]

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD) [2017]

Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 [2014] OJ L 173 (12 June 2014)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119 (4 May 2016)

**Case Law of the CJEU**

Case C-22/70 *Commission v Council* [1971] ECLI:EU:C:1971:32, cited as „Case C-22/70 *Commission v Council* [1971] ECLI:EU:C:1971:32“

Case C-380/03 *Germany v Parliement and Council* [2006] ECLI:EU:C:2006:772, cited as „Case C-380/03 *Germany v Parliement and Council* [2006] ECLI:EU:C:2006:772“

Case C-114/12 *Commission v Council* [2014] ECLI:EU:C:2014:2151, cited as „Case C-114/12 *Neighboring rights* [2014] ECLI:EU:C:2014:2151“

Case C-131/12 *Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, cited as „Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317“

Case C-360/13 *Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and Others* [2014] ECLI:EU:C:2014:1195, cited as „Case C-360/13 *PRCA v NLA and Others* [2014] ECLI:EU:C:2014:1195“

Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECLI:EU:C:2015:718, cited as „Case C-264/14 *Hedqvist* [2015] ECLI:EU:C:2015:718“

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, cited as „Case C-582/14 *Patrick Breyer* [2016] ECLI:EU:C:2016:779“

Opinion of the AG on Case C-264/14 *Skatteverket v David Hedqvist* [2015] ECLI:EU:C:2015:498, cited as „AG Opinion on Case C-264/14 *Hedqvist* [2015] ECLI:EU:C:2015:498“

**Opinions and Advisory Documents**

CJEU, Opinion 1/13 (Grand Chamber) [2014] ECLI:EU:C:2014:2303, cited as "CJEU, Opinion 1/13 (Grand Chamber) [2014] ECLI:EU:C:2014:2303"

EBA, '*EBA Opinion on 'virtual currencies''* (2014), EBA/Op/2014/08

EBA, '*Warning to consumers on virtual currencies*' (2013), EBA/WRG/2013/01

ECB, '*Virtual Currency Schemes*' (2012), ISBN: 978-92-899-0862-7

ECB, '*Virtual Currency Schemes – a Further Analysis*' (2015), ISBN: 978-92-899-1260-1

ENISA, '*Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector*' (2016), ISBN: 978-92-9204-200-4

ESMA, '*Additional information on the agreed product intervention measures relating to contracts for differences and binary options*' (2018), ESMA35-43-1000

ESMA, EBA and EIOPA, '*ESMA, EBA AND EIOPA warn consumers on the risks of Virtual Currencies*' [2018], available at: https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies, last accessed 10.8.2018.

ESMA, '*ESMA alerts firms involved in Initial Coin Offering (ICOs) to the need to meet relevant regulatory requirements*' (2017), ESMA50-157-828

ESMA, '*ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs)*' (2017), ESMA50-157-829

Opinion of Advocate General Kokott in Case C-264/14 *Hedqvist* [2015] ECLI:EU:C:2015:498, cited as "AG opinion in Case C-264/14 *Hedqvist* [2015] ECLI:EU:C:2015:498"

UK Financial Conduct Authority, '*FCA statement on the requirement for firms offering cryptocurrency to be authorised*' (2018), [online] available at: https://www.fca.org.uk/news/statements/cryptocurrency-derivatives, last accessed 19.8.2018

**Books**

BARON, Joshua, O'MAHONY, Angela, MANHEIM, David, DION-SCHWARZ, Cynthia, *National Security Implications of Virtual Currency*', 1st ed., RAND Corporation, 2015, ISBN: 978-0833091833

BASHIR, Imran, *Mastering Blockchain: Distributed ledger, decentralization and smart contracts explained*, 1st ed., Packt Publishing, 2017, ISBN: 978-1-78712-544-5

BORCHARDT, Klaus-Dieter, *The ABC of European Union law*, 6th ed., EU Publications Office, 2011, ISBN: 978-92-20690-5

CRAIG, Paul, DE BÚRCA, Gráinne, *EU law: text, cases, and materials*, 6th ed., Oxford University Press, 2015, ISBN: 978-0198714927

LENAERTS, Koen, VAN NUFFEL, Piet, BRAY, Robert, CAMBIEN, Nathan, *European Union Law*, 3rd ed., Sweet & Maxwell, 2011, ISBN: 978-1847037435

SCHÜTZE, Robert, *European Union Law*, 1st ed., Cambridge University Press, 2015, ISBN: 978-1107416536

STROUKAL, Dominik, SKALICKÝ, Jan, *Bitcoin: peníze budoucnosti*, 1st ed., Ludwig von Mises Institut, 2015, ISBN: 978-80-87733-26-4

SVOBODA, Pavel, *Úvod do evropského práva*, 5th ed., C. H. Beck, 2013, ISBN: 978-80-7400-488-9

SWAN, Melanie, *Blockchain: Blueprint for a New Economy*, 1st ed., O'Reilly Media, 2015, ISBN: 978-1-491-92049-7

TICHÝ, Luboš, ARNOLD, Reiner, ZEMÁNEK, Jiří, KRÁL, Richard, DUMBROVSKÝ, Tomáš, *Evropské právo*, 5th ed., C. H. Beck, 2014, ISBN: 987-80-7400-546-6

TOMÁŠEK, Michal, TÝČ, Vladimír, and coll., *Právo Evropské unie*, 2nd ed., Leges, 2017, ISBN: 978-80-7502-184-7

VOIGT, Paul, VON DEM BUSSCHE, Axel, *The EU General Data Protection Regulation (GDPR)*, 1st ed., Springer International Publishing, 2017, ISBN: 978-3-319-57959-7

**Chapters**

BARNARD, Catherine, SNELL, Jukka, *Free movement of persons and the provision of services* in BARNARD, C., PEERS, S., *European Union Law*, 2nd ed., Oxford University Press, 2017, ISBN: 978-0198789130

BONAIUTI, Gianni, *Economic Issues on M-Payments and Bitcoin* in GIMIGLIANO, Gabriella, *Bitcoin and Mobile Payments: Constructing a European Union Framework*, 1st ed., Palgrave Studies in Financial Services Technology, 2016, ISBN: 978-1-137-57512-8

FELLÄNDER, Anna, SIRI, Shahryar, TEIGLAND, Robin, *The three phases of FinTech* in TEIGLAND, R., SIRI, Shahryar, LARSSON, Anthony, PUERTAS, Alejandro M., BOGUSZ, Claire I., *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*, 1st ed., Routledge, 2018, ISBN: 978-1-351-18362-8

FLYNN, Leo, *Free movement of capital* in BARNARD, C., PEERS, S., *European Union Law*, 2nd ed., Oxford University Press, 2017, ISBN: 978-0198789130

HOFMANN, Herwig C. H., *General principles of EU law and EU administrative law* in BARNARD, C., PEERS, S., *European Union Law*, 2nd ed., Oxford University Press, 2017, ISBN: 978-0198789130

HOLMBERG, Håkan, *How to scale Bitcoin: A payment network that no one controls* in TEIGLAND, R., SIRI, Shahryar, LARSSON, Anthony, PUERTAS, Alejandro M., BOGUSZ, Claire I., *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*, 1st ed., Routledge, 2018, ISBN: 978-1-351-18362-8

KASIYANTO, Safari, *Security Issues of New Innovative Payments and Their Regulatory Challenges* in GIMIGLIANO, Gabriella, *Bitcoin and Mobile Payments: Constructing a European Union Framework*, 1st ed., Palgrave Studies in Financial Services Technology, 2016, ISBN: 978-1-137-57512-8

PUERTAS, Alejandro Moreno, TEIGLAND, Robin, '*Blockchain: The Internet of Value*' in TEIGLAND, R., SIRI, Shahryar, LARSSON, Anthony, PUERTAS, Alejandro M., BOGUSZ, Claire I., *The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond*, 1st ed., Routledge, 2018, ISBN: 978-1-351-18362-8

SNELL, Jukka, *The internal market and the philosophies of market integration* in BARNARD, C., PEERS, S., *European Union Law*, 2nd ed., Oxford University Press, 2017, ISBN: 978-0198789130

**Journal Articles**

AMETRANO, Ferdinando M., '*Hayek Money: The Cryptocurrency Price Stability Solution*' (2016), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270, last accessed 19.8.2018

ASKARI, Mamun U. R., '*Significance of Ever-evolving Cybersecurity Landscape: Challenges and Possible Pathways*' (2018), National Journal of Cyber Security Law, Vol. 1 Issue 1

ATHANASSIOU, Phoebus, '*Legal Working Paper Series: Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks*' (2017), European Central Bank, No 16/October 2017, ISBN: 978-92-899-3015-4

ATZORI, Marcella, '*Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*' (2016), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713, last accessed 19.8.2018

BAKER, Edward D., 'Trustless Property Systems and Anarchy: How Trustless Transfer Technology Will Shape the Future of Property Exchange' (2015), 45 Sw. L. Rev. 351, pp 351-376

BELL, Tom W., '*Copyrights, Privacy, and the Blockchain*' (2016), 42 Ohio N.U. L. Rev. 439, pp 439-470

BERBERICH, Matthias, STEINER, Malgorzata, '*Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers*' (2016), 2 Eur. Data Prot. L. Rev. 422, pp 422-426

BIRUYUKOV, Alex, KHOVRATOVICH, Dmitry, TIKHOMIROV, Sergei, '*Privacy-preserving KYC on Ethereum*' [2018], Reports of the European Society for Socially Embedded Technologies, ISSN: 2510-1591

BOTOS, Horia M., '*A Blockchain Intelligence Analysis*' (2017), 13 Res. & Sci. Today 42, pp 42-47

BURBIDGE, Rosie, '*The Blockchain Is in Fashion*' (2017), 107 Trademark Rep. 1262, pp 1262-1267

CHRISTIN, Nicolas, '*Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace*' (2012), Cornell University Library, available at: https://arxiv.org/abs/1207.7139, [online] last accessed 19.8.2018

CHRISTOPHER, Catherine M., '*The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*' (2016), 17 Nev. L.J. 139, pp 139-180

GRUBER, Sarah, '*Trust, Identity and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?*' (2013), 32 Quinnipiac L. Rev. 135, pp 135-208

HAESLY, Kenneth B. II, '*How to Solve a Problem Like Venezuela: An Argument for Virtual Currency*' (2016), 22 Law & Bus. Rev. Am. 261, pp 261-269

HEADON, Tobby, '*Ghosts in the Machine: Copyright and Temporary Copies*' (2011), Computers & Law Magazine of SCL, Vol. 22 Issue 4

IBÁÑEZ, Louis-Daniel, O'HARA, Kieron, SIMPERL, Elena, '*On Blockchains and the General Data Protection Regulation*', EU Blockchain Forum, [online] available at: https://www.eublockchainforum.eu/knowledge, last accessed 19.8.2018

JUELS, Ari, KOSBA, Ahmed, SHI, Elaine, '*The Ring of Gyges: Using Smart Contracts for Crime*' [2016], The 2016 ACM SIGSAC Conference, [online], available at: https://www.researchgate.net/publication/310821111_The_Ring_of_Gyges_Investigating_the_Future_of_Criminal_Smart_Contracts, last accessed 19. 8. 2018

KASIYANTO, Safari, '*Regulating Peer-to-Peer Network Currency: Leesons from Napster and Payment Systems*' (2015), Journal of Law, Technology and Public Policy, Vol. 1 No. 2, pp. 40-73.

KIVIAT, Trevor I., '*Beyond Bitcoin: Issues in Regulating Blockchain Transactions*' (2015), 65 Duke L. J. 569, last accessed 18.2.2018

LEE, Larissa, '*New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market*' (2016), 12 Hastings Bus. L.J. 81, pp 81-132

LEVY, Karen E. C., '*Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law*' (2017), Engaging Science, Technology and Society Vol. 3 (2017)

LOOTSMA, Yvonne, '*Blockchain as the Newest Rechtech Application – the Opportunity to Reduce the Burden of KYC for Financial Institutions*' (2017), Banking & Financial Services Policy Report, Vol. 36, Number 8, pp 16-21

MARIAN, Omri, '*Are Cryptocurrencies Super Tax Havens?*' (2013), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863, last accessed 19.8.2018

NAKAMOTO, Satoshi, '*Bitcoin: A Peer-to-Peer Electronic Cash System*' [2008], [online], available at: https://bitcoin.org/bitcoin.pdf, last accessed 19.8.2018

NĚMEC, Libor, '*K právní regulaci kryptoměn, díl I.*' (2018), Právní rádce, [online], available at: https://pravniradce.ihned.cz/c1-66168650-k-pravni-regulaci-kryptomen-dil-i, last accessed 19.8.2018

O'SHIELDS, Reggie, '*Smart Contracts: Legal Agreements for the Blockchain*' (2017), 21 N.C. Banking Inst. 177, pp 177-194

PERUGINI, Maria L., DAL CHECCO, Paolo, '*Smart Contracts: a preliminary evaluation*' (2015), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2729548, last accessed 19.8.2018

RASKIN, Max, '*The Law and Legality of Smart Contracts*' (2017), 1 Geo. L. Tech. Rev. 305, pp 305-341

SANCHEZ, Edgar G., '*Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens*' (2017), 28 U. Fla. J.L. & Pub. Pol'y 167, pp 167-192

STANLEY, Rebecca L., BUCKLEY, Ross P., '*Protecting the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses*' (2016), 17 Melb. J. Int'l L. 83, pp 83-106

ŠTIKA, Martin, '*Má naprosto svobodná virtuální měna bitcoin místo v právním státě?*' (2017), Bulletin advokacie, 5/2018, pp. 29-34, [online] last accessed 19.8.2018

TSUKERMAN, Misha, 'The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future' (2015), 30 Berkeley Tech. L.J. 1127, pp 1127-1169

VALCKE, Peggy, VANDEZANDE, Niels, VAN DE VELDE, Nathan, '*The Evolution of Third Party Payment Providers and Cryptocurrencies under the EU's Upcoming PSD2 and AMLD4*' (2015), SWIFT Institute Working Paper No. 2015-001, SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2665973, last accessed 19.8.2018

VERELLEN, Thomas, '*The ERTA Doctrine in the Post-Lisbon Era: Note under Judgment in Commission v Council (C-114/12) and Opinion 1/13*' (2015), 21 Colum. J. Eur. L. 383, [online] last accessed 17.8.2018

VONDRÁČKOVÁ, Aneta, '*Regulation of Virtual Currency in the European Union*' (2016), Prague Law Working Papers Series (Faculty of Law, Charles University), 2016/III/3

WRIGHT, Aaron, DE FILIPPI, Primavera, '*Decentralized Blockchain Technology and the Rise of Lex Cryptographia*' (2015), SSRN [online], available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, last accessed 19.8.2018

ZETZSCHE, Dirk A., BUCKLEY, Ross P., ARNER, Douglas W., '*The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*' (2017), EBI Working Paper Series, 2017-007

**Studies**

BOUCHER, Philip, NASCIMENTO, Susana, KRITIKOS, Mihalis, '*How blockchain technology could change our lives*', (2017) EPRS, Scientific Forensic Unit (STOA), ISBN: 978-92-846-0549-1

BRITO, Jerry, CASTILLO, Andrea, '*Bitcoin: A Primer for Policymakers*' (2013), Mercatus Center, George Mason University

HODUN, Milosz, '*Doctrine of Implied Powers as a Judicial tool to build Federal Polities: Comparative Study on the Doctrine of Implied Powers in the European Union and the United States of America*', School of Law, Reykjavik University

SHARMIN, Sadia, '*Music Copyright Management on Blockchain: Is it legally viable?*' (2018), Uppsala Universitet

SZCZEPAŃSKI, M., '*Bitcoin: Market, economics and regulation*' (2014), EPRS

'*Regulation of Cryptocurrency Around the World*' (2018), The Law Library of Congress, Global Legal Research Center

ROSENFELD, Meni, '*Analysis of hashrate-based double-spending*' (2012), Cornell University Library, available at: https://arxiv.org/abs/1402.2009, last accessed 19.8.2018

**Online News Articles**

ARMERDING, Taylor, '*The 17 biggest data breaches in 21st century*' (2018), available at: https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, last accessed 19.8.2018

BIGGS, John, '*As Auroracoin "Airdrop" Approaches, What Does It Mean When A Nation Adopts A Cryptocurrency?*' (2014), available at: https://techcrunch.com/2014/03/01/as-auroracoin-airdrop-approaches-what-does-it-mean-when-a-nation-adopts-a-cryptocurrency/?guccounter=1, last accessed 19.8.2018

BRANDOM, Rusell, '*How an experimental cryptocurrency lost (and found) $53 million*' (2016), available at: https://www.theverge.com/2016/6/17/11965192/ethereum-theft-dao-cryptocurrency-million-stolen-bitcoin, last accessed 19.8.2018

BUNTINX, Jean-Pierre, '*BNP Paribas Sees Smart-Contracts in the Future of Legal Code*' (2016), available at: https://news.bitcoin.com/bnp-paribas-smart-contracts-legal-code/, last accessed 19.8.2018

BUTERIN, Vitalik, '*Introducing Ripple: A Detailed Look at Cryptocurrency's New Kid on the Block*' (2013), available at: https://bitcoinmagazine.com/articles/introducing-ripple/, last accessed 19.8.2018

CHENG, Evelyn, '*Japanese cryptocurrency exchange loses more than $500 million to hackers*' (2018), available at: https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html, last accessed 19.8.2018

COOK, James, '*The CEO of bitcoin exchange Mt Gox described what it was like to discover he had been hacked: 'It felt like I was about to die'*" (2018), available at:

https://www.businessinsider.com/mt-gox-ceo-mark-karpeles-hacked-i-was-about-to-die-2018-3, last accessed 19.8.2018

CORDELL, Drew, '*Fidor Bank Partners with Kraken to Create Cryptocurrency Bank*' (2014), available at: https://www.ccn.com/fidor-bank-partners-kraken-create-cryptocurrency-bank/, last accessed 19.8.2018

CZARNECKI, Jacek, '*Why Blockchain Firms Shouldn't Ignore New EU Cybersecurity Laws*' (2017), available at: https://www.coindesk.com/why-blockchain-firms-shouldnt-ignore-europes-new-cybersecurity-laws/, last accessed 19.8.2018

DARRAH, Kim, '*Estonia pushes ahead in race to issue first state-backed cryptocurrency*' (2018), available at: https://www.worldfinance.com/markets/estonia-pushes-ahead-in-race-to-issue-first-state-backed-cryptocurrency, last accessed 17. 8. 2018

DAS, Samburaj, '*Bitcoin Stock Exchange Operator Pleads Guilty to Securities Fraud*' (2018), available at: https://www.ccn.com/bitcoin-stock-exchange-operator-pleads-guilty-to-securities-fraud/, last accessed 17. 8. 2018

DAS, Samburaj, '*Exclusive: Malta PM Confirms Parliament Will Pass Three Cryptocurrency Bills*' (2018), available at: https://www.ccn.com/breaking-exclusive-malta-pm-confirms-parliament-will-pass-three-cryptocurrency-bills/, last accessed 17. 8. 2018

DELAHUNTY, Thomas, '*Two Thirds of US, EU Crypto Exchanges Fail to Verify Customer Identities*' (2018), available at: https://www.newsbtc.com/2018/06/06/68-of-u-s-eu-cryptocurrency-exchanges-and-wallets-fail-to-verify-customer-identities-research/, last accessed 19.8.2018

DEL CASTILLO, Michael, '*JP Morgan, Credit Suisse Among 8 in Latest Bank Blockchain Test*' (2016), available at: https://www.coindesk.com/jp-morgan-credit-suisse-among-8-in-latest-bank-blockchain-test/, last accessed 19.8.2018

FARRELL, Maureen, '*Strategist predicts end of Bitcoin*' (2013), available at: https://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html, last accessed 19.8.2018

FARQUHAR, Peter, '*The US Supreme Court just spoke about a Bitcoin future for the first time*' (2018), available at: https://www.businessinsider.com.au/the-us-supreme-court-just-spoke-about-a-bitcoin-future-for-the-first-time-2018-6, last accessed 19.8.2018

FENECH, Gerald, '*Crypto Exchange HitBTC Adds Support for Euro-Pegged Stablecoin 'EURS"* (2018), available at: https://www.ccn.com/crypto-exchange-hitbtc-adds-support-for-euro-pegged-stablecoin-eurs/, last accessed 19.8.2018

FENECH, Gerald, '*Malta Regulator Opens Consultation after Publishing Cryptocurrency, Blockchain Bills*' (2018), available at: https://www.ccn.com/malta-regulator-opens-consultation-after-publishing-cryptocurrency-blockchain-bills/, last accessed 19.8.2018

FENECH, Gerald, '*Stasis Onboards First Institutional Client for EURS Stablecoin*', available at: https://www.ccn.com/stasis-onboards-first-institutional-client-for-eurs-stablecoin/, last accessed 19.8.2018

HAJDARBEGOVIC, Nermin, '*Bitcoin Ransomware Now Spreading via Spam Campaigns*' (2015), available at: https://www.coindesk.com/bitcoin-ransomware-now-spreading-via-spam-campaigns/, last accessed 19.8.2018

HANKIN, Aaron, '*Most major cryptocurrency exchanges lack sufficient background checks, research report says*' (2018), available at: https://www.marketwatch.com/story/most-major-cryptocurrency-exchanges-lack-sufficient-background-checks-research-report-says-2018-06-06, last accessed 19.8.2018

GIBBS, Samuel, '*EU seeks to outlaw 'backdoors' in new data privacy proposals*' (2017), available at: https://www.theguardian.com/technology/2017/jun/19/eu-outlaw-backdoors-new-data-privacy-proposals-uk-government-encrypted-communications-whatsapp, last accessed 19.8.2018

HERTIG, Alyssa, '*Blockchain's Once-Feared 51% Attack Is Now Becoming Regular*' (2018), available at: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/, last accessed 19.8.2018

KELSO, C. Edward, '*Switzerland Formally Considers State Backed Cryptocurrency*' (2018), available at: https://news.bitcoin.com/switzerland-formally-considers-state-backed-cryptocurrency/, last accessed 19.8.2018

KIM, Christine, '*DEA Agent: Speculators Are Using Bitcoin More Than Criminals*' (2018), available at: https://www.coindesk.com/most-bitcoin-transactions-now-used-for-speculation-not-drugs-report/, last accessed 19.8.2018

LIEBKIND, Joe, '*Estonia is Pushing for State-Backed Cryptocurrency*' (2018), available at: https://www.investopedia.com/news/estonia-pushing-statebacked-cryptocurrency/, last accessed 19.8.2018

LONG, Caitlin, '*ICOs Were 45% Of IPOs in Q2 2018, As Cryptos Disrupt Investment Banks*' (2018), available at: https://www.forbes.com/sites/caitlinlong/2018/07/22/icos-were-45-of-ipos-in-q2-2018-as-cryptos-disrupt-investment-banks/, last accessed 19.8.2018

MASTERS, Christine, '*Stasis Launches Euro-Pegged Stablecoin EURS on DSX Exchange*' (2018), available at: https://cryptovest.com/news/stasis-launches-euro-pegged-stablecoin-eurs-on-dsx-exchange/, last accessed 19.8.2018

MCMAHON, John, '*Bahamas is Launching a State Backed Cryptocurrency, is it Legitimate?*' (2018), available at: https://www.newsbtc.com/2018/06/25/bahamas-launching-state-backed-cryptocurrency-legitimate/, last accessed 19.8.2018

MIYAGUCHI, Ayako, '*Kraken.com to Offer Digital Currency Trading in Exclusive EU Partnership with Fidor Bank AG*' (2013), available at: http://www.prweb.com/releases/2013/10/prweb11211586.htm, last accessed 19.8.2018

NOVA, Annie, '*After $500 million Japan cryptocurrency theft, here's how to keep yours secure*' (2018), available at: https://www.cnbc.com/2018/01/29/after-500-million-japan-cryptocurrency-theft-heres-how-to-keep-yours-secure.html, last accessed 19.8.2018

PEASTER, William, '*EU's Controversial Article 13: Considerations for the Blockchain Space*' (2018), available at: https://bitsonline.com/eu-gdpr-article-13-copyright-blockchain/, last accessed 19.8.2018

PRISCO, Giulio, '*A Major Dutch Bank Is Considering a Cryptocurrency Wallet for Its Customers*' (2018), available at: https://bitcoinmagazine.com/articles/major-dutch-bank-considering-cryptocurrency-wallet-its-customers/, last accessed 19.8.2018

ROBBINS, Seth, '*Liberty Reserve Case Exposes New Frontiers in Laundering Digital Cash*' (2013), available at: https://www.insightcrime.org/news/analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash/, last accessed 19.8.2018

SIMPSON, Andrew G., '*Toyota, MIT Lab Eye Using Blockchain in Insurance Rating of Driverless and Shared Vehicles*' (2017), available at: https://www.insurancejournal.com/news/national/2017/05/23/451913.htm, last accessed 19.8.2018

SHEN, Lucinda, '*Meet 'Paypal for Crypto,' a New Way to Pay With Bitcoin and Litecoin*' (2018), available at: http://fortune.com/2018/02/15/bitcoin-paypal-coinbase-commerce/, last accessed 19.8.2018

VINCENT, James, '*EU sends controversial internet copyright reforms back to the drawing board*' (2018), available at: https://www.theverge.com/2018/7/5/17535874/eu-copyright-law-article-11-13-rejected-first-vote, last accessed 19.8.2018

WILMOTH, Josiah, '*PayPal Files Patent to Improve Cryptocurrency Transaction Times*' (2018), available at: https://www.ccn.com/paypal-files-patent-improve-cryptocurrency-transaction-times/, last accessed 19.8.2018

YOUNG, Joseph, '*Mark Karpeles Will End Up Taking $859 Million From Mt. Gox Bankruptcy*' (2017), available at: https://www.ccn.com/mark-karpeles-will-end-taking-859-million-mt-gox-bankruptcy/, last accessed 19.8.2018

YOUNG, Joseph, '*Most Complex dApp on Ethereum Already Has Millions of Dollars at Stake*' (2018), available at: https://www.ccn.com/most-complex-dapp-on-ethereum-already-has-millions-of-dollars-at-stake/, last accessed 19.8.2018

ZHAO, Wolfie, '*Lichtenstein Bank Opens Up Cryptocurrency Investment for Clients'* (2018), available at: https://www.coindesk.com/liechtenstein-bank-opens-up-cryptocurrency-investment-for-clients/, last accessed 19.8.2018

'*2 Canadian banks hacked, 90.000 customers' data stolen*', available at: https://www.csoonline.com/article/3276275/data-breach/2-canadian-banks-hacked-900-00-customers-data-stolen.html, last accessed 19.8.2018

**Websites and Blogs**

ACHESON, Noelle, '*PSD2 and the blockchain*' (2017), available at: http://www.fintechblue.com/2017/05/psd2-and-the-blockchain/, last accessed 19.8.2018

'*Bitcoin exchanges*', available at: https://bitcoin.org/en/exchanges, last accessed 19.8.2018

'*Coinbase adds support for PayPal and Credit Cards*' (2016), available at: https://blog.coinbase.com/coinbase-adds-support-for-paypal-and-credit-cards-2196-8661d508, last accessed 19.8.2018

'*Coinbase Commerce –the Easiest Way for Merchants to Accept Digital Currency*' [2018], available at: https://medium.com/@coinbasecommerce/coinbase-commerce-the-easiest-way-for-merchants-to-accept-digital-currency-54ba64966f8d, last accessed 19.8.2018

'*DAPP Rankings*', available at: https://www.stateofthedapps.com/rankings, last accessed 19.8.2018

DEVRIENDT, Anne-Morgane, '*e-Privacy: What happened and what happens next*' (2017), available at: https://edri.org/e-privacy-what-happened-and-what-happens-next/, last accessed 19.8.2018

DUCUING, Charlotte, '*Fifty shades of cloud on the internet: the blockchain infrastructure layer as a cloud computing service*' (2018), available at: https://www.law.kuleuven.be/citip/blog/fifty-shades-of-cloud-on-the-internet-the-blockchain-infrastructure-layer-as-a-cloud-computing-service/, last accessed 19.8.2018

'*Elliptic Curve Digital Signature Algorithm*', available at: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm, last accessed 19.8.2018

‘*EU Blockchain Observatory and Forum*’ (2018), available at: https://ec.europa.eu/digital-single-market/en/eu-blockchain-observatory-and-forum, last accessed 17. 8. 2018.

‘*European Union (EU) (182 texts)*’, available at: http://www.wipo.int/wipolex/en/profile.jsp?code=EU, last accessed 19.8.2018

FELTEN, Ed, ‘*Understanding Bitcoin's transaction malleability problem*’ (2014), available at: https://freedom-to-tinker.com/2014/02/12/understanding-bitcoins-transaction-malleability-problem/, last accessed 19.8.2018

HUDGENS, Ross, ‘*The 100 Most Popular Google Keywords [Infographic]*’ (2018), available at: https://www.siegemedia.com/seo/most-popular-keywords, last accessed 17. 8. 2018

INSOM, Poramin, ‘*Zcoin’s Zerocoin bug explained in detail*’ (2017), available at: https://zcoin.io/zcoins-zerocoin-bug-explained-in-detail/, last accessed 19.8.2018

‘*In support of the ePrivacy Regulation*’ [2017], available at: https://medium.com/@wireapp/in-support-of-the-eprivacy-regulation-36fe8197b2cb, last accessed 19.8.2018

KAR, Ian, ‘*PayPal is warming up to bitcoin*’ (2016), available at: https://qz.com/713528/paypal-is-warming-up-to-bitcoin/, last accessed 19.8.2018

KOETSIER, John, ‘*Bitcoin Is The Second Most-Searched Global News Term Of 2017* (2018)’*, available at:* https://www.forbes.com/sites/johnkoetsier/2017/12/13/bitcoin-is-the-second-most-searched-global-news-term-of-2017/, last accessed 17. 8. 2018

‘*Load dollars using your Bitcoin wallet, spend anywhere*’, available at: https://bitpay.com/card/, last accessed 19.8.2018

LUNDKVIST, Christian, ‘*Introduction to zk-SNARKs with examples*’ (2017), available at: https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b, last accessed 19.8.2018

‘*Merchant Solutions*’, available at: https://www.bitcoin.com/merchant-solutions/, last accessed 19.8.2018

NOVAK, Nejc, '*EU Introduces Crypto Anti-Money Laundering Regulation*' [2018], available at: https://medium.com/@nejcnovaklaw/eu-introduces-crypto-anti-money-laundering-regulation-d6ab0ddedd3, last accessed 19.8.2018

'*PayPal Reports Fourth Quarter and Full Year 2017 Results*' (2018), https://investor.paypal-corp.com/releasedetail.cfm?ReleaseID=1055924, last accessed 19.8.2018

'*PoW 51% Attack Cost*', available at: https://www.crypto51.app/, last accessed 19.8.2018

'*Secp256k1*', available at: https://en.bitcoin.it/wiki/Secp256k1, last accessed 19.8.2018

'*Securing your wallet*', available at: https://bitcoin.org/en/secure-your-wallet, last accessed 19.8.2018

SIRER, Emin G., '*What Did* Not *Happen At Mt. Gox*' (2014), available at http://hackingdistributed.com/2014/03/01/what-did-not-happen-at-mtgox/, last accessed 19.8.2018

Sources of Malleability, available at: https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki, last accessed 19.8.2018

STANKOVIC, Stefan, '*US Cryptocurrency Regulation: Policies, Regimes & More*' (2018), available at: https://unblock.net/us-cryptocurrency-regulation/#h3, last accessed 19.8.2018

'*Study on opportunity and feasibility of a EU blockchain infrastructure*' (2017), available at: https://ec.europa.eu/digital-single-market/en/news/study-opportunity-and-feasibility-eu-blockchain-infrastructure, last accessed 17.8.2018

REDA, Julia, '*EU copyright reform/expansion*' (2018), available at: https://juliareda.eu/eu-copyright-reform/, last accessed 19.8.2018

'*The most infamous data breaches*' (2018), available at: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/, last accessed 19.8.2018

'*Top 100 Cryptocurrencies By Market Capitalization*', available at: https://coinmarketcap.com/, last accessed 19.8.2018

**Speeches**

'*Virtual currencies ante portas*' by Yves Mersch, Member of the Executive Board of the ECB at the 39th meeting of the Governor's Club Bodrum, Turkey, 14 May 2018, available at: https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en-.html, last accessed 19.8.2018

## Blockchain na evropské úrovni

## Abstrakt

Cílem této diplomové práce je poskytnout základní přehled technologie blockchain, jejích vlastností a potenciálního využití, včetně přehledu evropských předpisů, které se této technologie mohou za určitých podmínek dotýkat. V první kapitole diplomová práce poskytuje právní rámec primárního práva EU, který zakládá nebo může založit pravomoc EU zabývat se technologií blockchain, v závislosti na její právní kvalifikaci (zejména v souvislosti s vnitřním trhem – zejména volný pohyb služeb či kapitálu).

V druhé a třetí kapitole je uveden základní popis funkcionalit blockchainu a kryptoměn a souvisejících služeb. Detailní popis je poskytnut v přílohách I-IV této diplomové práce. Zároveň je posouzen právní status a regulace kryptoměn, které tvoří základ technologií založených na blockchainu, a to jak na evropské úrovni, tak na úrovni členských států a dalších světových jurisdikcí. Součástí posouzení je i nedávný rozsudek SDEU *Hedqvist*, dle kterého se na dvousměrné směnárenské služby (nákup kryptoměn za fiat měny a naopak) uplatní výjimka z povinnosti odvést DPH v souladu s VAT směrnicí. Vzhledem k odůvodnění SDEU i generálního advokáta může tento rozsudek v budoucnu významně ovlivnit vývoj interpretace právního statusu kryptoměn a blockchainu obecně. Kromě kryptoměn je rovněž provedena analýza smart contracts, včetně potenciálních problémů, které mohou z právního hlediska nastat. Tyto se budou týkat zejména procesních otázek.

Ve čtvrté kapitole je posouzeno deset nejvýznamějších a nejzajímavějších aspektů technologie blockchain, které mohou jednak představovat přínosy a výhody, které tato technologie může za určitých okolností přinést, ale také potenciální komplikace nebo slabá místa, která bude třeba vyřešit, aby se vůbec mohlo uvažovat o implementaci této technologie do každodenních procesů podniků i obyčejné populace.

**Klíčová slova:** blockchain, kryptoměny, platební služby, vnitřní trh, měna, zákonné platidlo, smart contracts, Bitcoin, Ethereum, Hedqvist

## Blockchain at the European Level

## Abstract

The objective of this master thesis is to provide a basic overview of the blockchain technology, its features and its potential utilization, including an overview of European legal regulations that might be applicable to the technology, under certain conditions. In the first chapter, the master's thesis sets forth the legal framework of the EU primary law that establishes or can establish the EU's competence to act in the matters of blockchain technology, depending on its legal qualification (especially in the context of the internal market – namely the free movement of services and capital).

The second and third chapters provide essential description of features of blockchain and cryptocurrency and related services. A more detailed description is provided in Annexes I-IV of this thesis. Further, the legal status and applicable regulation of cryptocurrencies are assessed at the European and national levels and in terms of other global jurisdictions. The assessment also includes the recent CJEU's judgment in the case *Hedqvist*, according to which bidirectional exchange services (purchase of cryptocurrency for fiat currency and *vice versa*) are to be exempted from VAT obligation under the VAT directive. In line with the CJEU's reasoning and the Advocate General's opinion, this judgment may significantly affect the future development of the interpretation of legal status of cryptocurrencies and blockchain in general. Apart from cryptocurrencies, an analysis of smart contracts, including potential issues which might occur from the legal point of view, is provided as well. In particular, these issues will concern the procedural legal questions.

The fourth chapter lays down ten most significant and interesting aspects of the blockchain technology which, under certain circumstances, can be considered as beneficial and advantageous, however, some can also represent potential complications or weak spots that need to be addressed to enable widespread implementation of the technology in the day-to-day processed of businesses and general population to even be considered.

**Key Words:** blockchain, cryptocurrency, payment services, internal market, currency, legal tender, smart contracts, Bitcoin, Ethereum, Hedqvist