TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV
FACULTY OF LAW
CIVIL LAW DEPARTMENT

MYKOLAS ROMERIS UNIVERSITY
MYKOLAS ROMERIS LAW SCHOOL
INSTITUTE OF PRIVATE LAW

IRYNA ARKHYPCHENKO
Private Law

THEORETICAL AND LEGAL PERSPECTIVE OF CIVIL LIABILITY IN CRYPTOCURRENCY RELATIONS

Master thesis

Supervisors:
Simona Drukteinienė
Doctor of Juridical Sciences, Professor
of the Institute of Private Law at Mykolas Romeris Law School,
Mykolas Romeris University

Bogdan Voyevodin
Candidate of Juridical Sciences (Ph.D.), Associate Professor
of the Civil Law Department of the Law Faculty of Taras
Shevchenko National University of Kyiv

Vilnius – Kyiv, 2020

TABLE OF CONTENTS

ABBREVIATIONS

CISG	–	United Nations Convention on Contracts for the International Sale of Goods
CPI	–	Consumer Price Index
DL	–	distributed ledger
DLT	–	distributed ledger technology
EBA	–	European Banking Authority
ECB	–	European Central Bank
FATF	–	Financial Action Task Force on Money Laundering
GDPR	–	General Data Protection Regulation
P2P	–	peer-to-peer
PECL	–	Principles of European Contract Law
PoS	–	Proof of Stake
PoW	–	Proof of Work
UPICC	–	UNIDROIT Principles of International Commercial Contracts

INTRODUCTION

Problem of research. The issue of legal liability in cryptosphere is still full of grey areas due to the decentralized structure of the system and lack of legal regulation in most countries. Unlike tax law field, where obligations and liability of a person who gains cryptocurrency or profit out of a transaction with cryptocurrency are covered with certain regulations in many states, civil liability disputes in cryptocurrency relations are full of inconsistencies, unclarity, and confusion due to the novelty of cryptocurrency phenomenon. The importance and the machinery of civil liability regulations need more clarification for the actors of cryptocurrency relationships.

Relevance of the final thesis. The development of cryptographic e-money has long historical roots originated the in early 1980s when the work of an American cryptographer David Chaum[1] was published. After almost 30 years the first decentralized cryptocurrency Bitcoin emerged. This event became a trigger for the creation of over 6,000 altcoins (alternative variants of Bitcoin, or other cryptocurrencies).

From the point of legal relevance of the thesis, policymakers have not yet developed cryptocurrency specific frameworks because governments were not prepared for such a rapid development of cryptocurrency. Due to the lack of regulations, state authorities and courts of different jurisdictions do not have consistent approaches towards cryptocurrency-related disputes and claims.

For proper regulation of these relationships, it is essential to deal with the substance and peculiar nature of cryptocurrencies and the distributed ledger technology (hereinafter the DLT), like blockchain, that is decentralized control through which each cryptocurrency work. Different organizations and state authorities provide warnings for cryptocurrency users and publish their findings on cryptocurrency functionality and, at the same time, they manage to not provide clear answers on the most urgent questions cryptocurrency actors may have. The long-lasting *status quo* on account of cryptocurrency leads to financial losses of cryptocurrency investors and cryptocurrency companies.

The courts of different jurisdictions receive unfamiliar to them cryptocurrency claims and judges without clear guidelines towards cryptocurrencies have to deal with gaps in law, therefore, cryptocurrency cases are characterized as long-lasting ones.

From the point of the scientific relevance of the thesis, academic researches on cryptocurrency are fragmentary, one-sided or incomplete and most of them only outline the problems in the cryptocurrency domain without proper analysis of such problems or their solutions.

[1] Allen Taylor, “David Chaum: Godfather of Digital Currency,” Blockchain Times, Accessed 4 February 2020, https://blockchaintimes.news/2018/10/19/david-chaum-godfather-of-digital-currency/

The cryptocurrency field needs unambiguous, harmonized, and more importantly, universal rules that would prevent financial losses of cryptocurrency business and users. Cryptocurrency should be treated similarly in different jurisdictions just like governments treat currency in a like manner. In our view, cryptocurrency should be analyzed through financial, technological and legal perspectives collectively to provide comprehensive and unambiguous research.

Scientific novelty and overview of the research on the selected topic. Different scholars, as well as international and regional organizations, in their reports looked into prospects and challenges related to cryptocurrencies and the blockchain technology.

All researchers in their works refer to cryptocurrency history and functioning and just a few address legal issues. In particular, the cryptocurrency phenomenon was explored by C. Rose[2], I. Cvetkova[3], Rico Shirakawa, U. Korwatanasaku,[4] W. Srokosz, T. Kopyscianski,[5] etc.

A great insight into the topic was made in the book "*FinTech Law and Regulation*" – the result of 31 contributing authors[6]. The writers covered *inter alia* legal and regulatory changes in the area of payments, banking, and fundraising that were driven by technology development, legal and regulatory challenges regarding cryptocurrency and the DLT, compliance problems in FinTech as well as the impact of technology change in the financial sector on the legal profession[7].

Alexander Savelyev,[8] *Jakub J. Szczerbowski*[9]*, Monica di Angelo, Alfred Soare, Gernot Salzer*[10]*, Lin William Cong* and *Zhiguo He*[11] analyzed smart contracts and application of standard

[2] Chris Rose, "The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution," *International Business & Economics Research Journal (IBER)*, 14, 4 (2015), https://www.researchgate.net/publication/297750676_The_Evolution_Of_Digital_Currencies_Bitcoin_A_Cryptocurrency_Causing_A_Monetary_Revolution

[3] Iryna Cvetkova, "Cryptocurrencies legal regulation," *BRICS Law Journal* 5, 2 (2018), https://www.researchgate.net/publication/326195399_Cryptocurrencies_legal_regulation

[4] Rico Shirakawa, Jacinta Bernadette, and Upalat Korwatanasakul, "Cryptocurrency Regulations: Institutions and Financial Openness," *ADBI Working Paper 978* (Tokyo: Asian Development Bank Institute, 2019), https://www.adb.org/publications/cryptocurrency-regulations-institutions-financial-openness

[5] Witold Srokosz and Tomasz Kopyscianski, "Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability," Journal of Teaching and Education 5 (2015), http://www.universitypublications.net/jte/0402/pdf/F5N180.pdf

[6] Jelena Madir ed., *FinTech Law and Regulation* (Cheltenham: Edward Elgar Publishing Limited, 2019).

[7] Ibid.

[8] Alexandr Savelyev, "Contract law 2.0: "Smart". Contracts as the beginning of the end of classic contract law," *Information & Communications Technology Law* 26 (2017), https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1301036

[9] Jakub J. Szczerbowski, "Place of smart contracts in civil law. A few comments on form and interpretation," Proceedings of the 12th Annual International Scientific Conference NEW TRENDS 2017 (Znojmo: Private College of Economic Studies Znojmo, 2017), https://ssrn.com/abstract=3095933

[10] Monica di Angelo, Alfred Soare, Gernot Salzer, "Smart Contracts in View of the Civil Code," *SAC* '19 (2019), https://publik.tuwien.ac.at/files/publik_278278.pdf

[11] Lin William Cong, Zhiguo He, "Blockchain Disruption and Smart Contracts," The Review of Financial Studies 35, 5 (2019), https://doi.org/10.1093/rfs/hhz007

contract law provisions to such agreements. In particular, J. *Szczerbowski* proposed a new form of contracts – blockchain form. *Monica di Angelo et al*. tried to clarify how smart contracts correspond to the provisions of the Austrian Civil Code as well as shortcomings of automated agreements.

Franziska Boehm and *Paulina Pesch* tried to analyze the *Bitcoin nature* and *characteristics of contracts with the use of Bitcoin* under German and US law.[12] Miklós Király investigates the possible application of the Vienna Convention on International Sales of Goods (hereinafter the CISG) to contracts with Bitcoin. He also refers to the exchange rate fluctuation risk, change of circumstances in crypto contracts and late payment interest.[13]

Darren J. Sandler explores the possibility for crypto mining contracts to be investment contracts in the United States and analyses relevant case law to prove that many companies publicly offer unregistered securities.[14]

We did not find any relevant research that examines *tortious liability* in the cryptocurrency sphere.

Significance of research. The deep analysis presented in the research defines ones and for all the status of cryptocurrency in the legal domain. It resolves the problem of ambiguity of approaches among different jurisdictions and/or state authorities inside one country and, hopefully, closes the academic discussion on this account. The findings will also help policymakers to determine the nature of cryptocurrency on the legal level.

The research is significant for practice because it indicates pitfalls in contractual and non-contractual relationships that should be taken into account by participants of cryptocurrency civil relations. The findings will provide solutions and comprehensive answers on previously unexplored questions in academic researches that will help to safeguard the interests of private actors and avoid potential civil liability issues. The analysis will also be relevant for the juridical interpretation of standard rules on civil liability in common law and in the continental system towards cryptocurrency relations. It possibly will help to develop a standardized approach in resolving cryptocurrency disputes in different jurisdictions.

The aim of the research. The aim of the research is to bring light on the nature of cryptocurrency and analyze the applicability of existing rules on civil liability in cryptocurrency relations. The research, where suitable, will also draw the line between the application of standard

[12] Franziska Boehm and Paulina Pesch, "Bitcoin: A First Legal Analysis – with reference to German and US-American law" *Financial Cryptography Workshops* (2014), https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf

[13] Miklós Király, "The Vienna Convention on International Sales of Goods and the Bitcoin," *US-Chine Law Review* 16, 5 (2019), https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf

[14] Darren J. Sandler, "Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?" *Santa Clara High Technology Law Journal* 34, 3 (2018), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1628&context=chtlj

rules on liability and circumstances when a new approach should be taken in civil liability disputes due to the specific nature of cryptocurrency and blockchain technology.

The objectives of the research.

1. To answer the controversial and sore question discussed in the cryptocurrency community: what is a cryptocurrency – money or commodity?
2. Establish whether cryptocurrencies identical in their nature or they have differences which should be taken into account when analyzing crypto relations and liability issues.
3. To analyze the notion and the machinery of the DLT, i.e. the blockchain.
4. To indicate problems and risks that exist in cryptocurrency contractual and non-contractual relations which may raise potential liability issues.
5. To analyze the court practices regarding disputes arising out of cryptocurrency relations and outline possible applications of judicial solutions and findings to future cryptocurrency claims.
6. Relying on the legal analysis performed in the Thesis, to make proposals concerning the better use or more effective use of existing legislation and adopting new rules that would be applied specifically to cryptocurrency legal liability issues.

Research methodology.

- Analysis of scientific literature on civil liability, FinTech and LegalTech development, cryptocurrency, blockchain technology, and smart contracts. Evaluation of the processes and literature that influenced the development of cryptocurrency through the *historical and legal perspective*.
- *Structural and functional methods* in determining cryptocurrency nature.
- *Descriptive multivariate data analysis* towards legal regulations of cryptocurrency and its status worldwide in order to find common patterns among policymakers approaches in different countries.
- *Causal analysis of statistical data* regarding cryptocurrencies to determine variables that cause a rise in the number of cryptocurrency-related claims.
- *A comparative synthesis* of civil liability provisions in the American, the UK's, Singapore's, German, and Ukrainian legislation to determine how they apply to cryptocurrency relations.
- *Comparative analysis* of Terms of Use agreements provided by different cryptocurrency platforms in order to distill clauses that distort the balance of parties' interests.
- *Comparative and predictive data analysis* of Singaporean and the US court practice in the scope of cryptocurrency civil relations aiming to determine future tendencies in the cryptocurrency legal domain. In comparison to other states, the abovementioned countries have more developed case law regarding cryptocurrency issues.

- Studying out the applicability of regional and international frameworks as well as *lex mercatoria* towards cryptocurrency relations such as the CISG, UNIDROIT Principles of International Commercial Contracts (hereinafter the UPICC), Principles of European Contract Law (hereinafter the PECL), and General Data Protection Regulation (hereinafter the GDPR).
- *Classification of cases* regarding cryptocurrency issues that courts might deal with.

Structure of the research.

The general part of the research will be devoted to the exploration of the genesis of the digital currencies in general. There will be also given an explanation of crucial terms, such as crypto assets, digital currency, virtual currency, and altcoins. The final and complete answer that determines whether cryptocurrencies are commodities or money is given. This part gives cryptocurrencies classification on the basis of several different factors. It also compares cryptocurrency and fiat money and explains the DLT that enables cryptocurrency existing. The second part overviews the legal status of cryptocurrency in different jurisdictions throughout the world based on the data provided by the Global Legal Research Center of The Law Library of Congress.[15] Also, actors of cryptorelations will be described.

The next part will explore contractual liability in cryptocurrency relations. The smart contracts phenomenon and their basic machinery will be examined. There will be given a list of most frequent contracts concluded between actors of the cryptocurrency market and their basic features. The analysis of different Terms of Use agreements on account of unfair contractual terms as well as the case law concerning breaches of contracts relating to cryptocurrencies will be presented.

In the finale, the research will present tortious liability in cryptocurrency relations. It will explore the common obligations of cryptocurrency market actors failing to perform of which could bring damage to a party. The analysis of rare case law concerning tortious liability will be given.

Defense statements.

1. *Nature of cryptocurrency*. Cryptocurrencies are *money*, not a commodity, therefore:

- ‘cryptocurrency for goods’ contracts are standard contracts of sale, not of barter.
- in transactions ‘cryptocurrency for fiat currency,’ the law concerning currency exchange and financial transactions should be applicable.

2. *Contractual liability issues in cryptocurrency relations*:

   2.1. Default rules on liability should be applicable to contractual liability in cryptocurrency relations regardless of the uniqueness and novelty of the cryptocurrency phenomenon.

[15] *Regulation of cryptocurrency around the world*, (Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018), https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

2.2. The unintended behavior of the program designed to create automated contracts does not make mistakenly concluded contracts void and it does not justify the breach of the other related contracts between involved parties.

2.3.Neither party will be liable for damage produced by the error in smart contracts. Therefore, parties should provide relevant clauses to the contract which designated to solve performance liability issues.

3. *Non-contractual liability issues in cryptocurrency relations*:

3.1. Potential civil liability may be caused by either the tort of negligence or breach of statutory duty.

3.2. Some contracts may be regarded as *securities* in common law system, thus their offerors are liable for the public offer of unregistered securities and/or false advertisement.

3.3. A cyberattack on crypto-platform could be a cause of liability in the tort of negligence.

3.4. Cryptocurrency related companies owe a duty of care to their platform users, thus are liable for the breach of such duty.

3.5. Contrastingly, independent coders that contribute to the open-source software do not owe a duty of care to the software users, thus not liable for code errors in the tort of negligence.

3.6. Breach of statutory duty resulting in civil liability may happen for breach of only three bodies of law designated for: investors' protection, users' protection, or users' data protection.

1. THE NOTION OF CRYPTOCURRENCY AND BLOCKCHAIN

1.1. Genesis, Nature, and Meaningful Content of Cryptocurrencies

Cryptocurrency has its predecessors – *electronic money, virtual currency, and digital currency.* There is a tendency to confuse terminology throughout scientists: use these terms interchangeably, define one term using the other one, or describe the correlation of terms improperly – e.g. *C. Ross* claims that digital currency is a form of virtual currency[16], overlooking features of virtual and digital currencies, therefore confusing the correlation between the two terms. The mistake will be explained at the end of this paragraph.

1.1.1. E-money

Electronic money (hereinafter the e-money) means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the e-money issuer [17].

According to the *European Central Bank* (hereinafter the ECB), e-money is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions. E-money products can be hardware-based or software-based, depending on the technology used to store the monetary value[18].

E-money is an electronic (virtual) equivalent of cash since it shares various features of cash. The value is stored in a given currency. There is no currency conversion, therefore, no risk of exchange rate fluctuations. E-money requires an issuer – e-money institutions (definition is set out in Directive 2009/110/EC[19]) – who issue the e-money upon license and are bound to convert it back into real money of the same currency.

[16] Chris Rose, "The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution," *International Business & Economics Research Journal (IBER)*, 14, 4 (2015): 617, https://www.researchgate.net/publication/297750676_The_Evolution_Of_Digital_Currencies_Bitcoin_A_Cryptocurrency_Causing_A_Monetary_Revolution

[17] "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 (Text with EEA relevance)," EUR- Lex, Accessed 4 February 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110

[18] "Electronic Money," European Central Bank, Accessed 4 February 2020, https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html

[19] "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

In other words, "e-money is a digital transfer mechanism for fiat currency — i.e. it electronically transfers value that has the legal tender status."[20]

1.1.2. Virtual currency

Virtual currency is a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat (conventional) currency but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically according to the *European Banking Authority* (hereinafter the EBA).[21]

Another definition provided by the *Financial Action Task Force on Money Laundering* (hereinafter the FATF): "a digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status." The key point is that "it is not issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency."[22]

In 2012 the ECB defined virtual currency 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."[23] In a further analysis that came out in 2015, it modified the definition as follows: "it 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."[24] The ECB considers virtual currencies neither as full form of money described in economic literature nor as legal tender[25].

From these definitions we can conclude that virtual currencies have **four main features**:

- they exist exclusively in the *virtual form*: they do not have physical form per se;
- only valid within the *specified community*, e.g. currencies in multiplayer online role-playing games in which a player can either earn or exchange fiat money for virtual

and 2006/48/EC and repealing Directive 2000/46/EC (Text with EEA relevance)," EUR- Lex, Accessed 4 February 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110

[20] "FAFT Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks" (Paris: Financial Action Task Force, June 2014): 4, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[21] "EBA Opinion on 'virtual currencies'" (Paris: European Banking Authority, July 2014): 5, https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1

[22] "FAFT Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks" (Paris: Financial Action Task Force, June 2014): 4, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[23] "Virtual Currency Schemes," (Frankfurt am Main: European Central Bank, October 2012): 13, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[24] "Virtual Currency Schemes – a further analysis," (Frankfurt am Main: European Central Bank, February 2015): 4, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

[25] Ibid.

monies[26]. Once a user bought them, the game's money is only useful in a game. The exchange of real goods from the "real world" to the virtual currency (meaning that players exchange something between themselves) is usually forbidden by games' terms of service[27];

- *unregulated*: there is no centralized banking or state authority that regulates issuing or circulation of a currency;
- they *work across national borders*.

1.1.3. Digital currency

The **digital currency** as a broad term can contain anything that digitally represents value. Digital currency includes e-money: money that is simply a digital representation of government-issued fiat currency. Digital currency can also cover virtual currency.[28]

In one of the FATF report, it is claimed that digital currencies "can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency"[29]. Even though these terms are viewed as identical by media and some scientists, it is an intrinsically incorrect approach.

Digital representation is a representation of something in the form of digital data, i.e. computerized data that is expressed using discrete, discontinuous values to embody information, as contrasted with continuous, or analog signals that behave in a perpetual manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system[30].

It is important to remember that digital currency is an umbrella term, meaning it is inherently unspecific.

To understand C. Ross's mistake and define a flaw in the digital currencies definition given by the FATF report, we would need to look into ancient philosophy works of Aristotle. In *Physics*, the philosopher speculates about the form and the matter. A thing's form is its definition

[26] Mark Coeckelbergh, *Money Machines: Electronic Financial Technologies, Distancing, and Responsibility in Global Finance* (New York: Routledge, 2016), 166.

[27] "Riot Games® Terms of Service," Riot Games, Accessed 11 February 2020, https://www.riotgames.com/en/terms-of-service

[28] J. W. Biggs, "Introduction to Digital Currency," Bookdown, Accessed 11 February 2020, https://bookdown.org/Jack_Biggs/Cryptocurrency/what-is-digital-currency.html

[29] "FAFT Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks" (Paris: Financial Action Task Force, June 2014): 4, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[30] Ibid, 13.

or essence. The form is not the same as the shape. "A statue may be human-shaped, but it is not a human, because it cannot perform the functions, characteristics of humans: thinking, perceiving, moving, desiring, eating, and growing, etc."[31] The matter explains what the thing is made of – the bricks that constitute a thing. If we apply these ideas to the terminology mentioned here (digital, virtual currency, and cryptocurrency), it is clear that digital data or digital representation is the matter of those units, because these currencies are made of zeros and ones – binary representation of information.

Aristotle stated that we need to answer *four questions* to give a full account of the nature of an object:

- what the thing is made of (*matter*)?
- what the thing is, or how it is defined (*form*)?
- what made the thing come into existence, who or what created it ("*moving cause*")?
- what the thing is for, what its purpose or function is (the *final cause*)?

Yet, it is already enough to answer the first two to get a perception of the thing's nature.

It is a logical mistake to state that digital currency is a form of virtual currency, meaning that it is a digital representation of virtual currency, which, in turn, are digital bricks that make virtual currencies, because it does not give an understanding what digital currency is. This flawed definition just gives a mere grasp of what the currency made of (matter). *Analogous flawed definitions* would be as follows: a bill is a form of paper money, a coin is a form of metallic money. The implication that arises from these flawed definitions is that there are other types of money made out of metal or paper.

Aristotle also stated that "the same stuff which makes up one object can later be used as the matter of another: for instance, when one melts down a bronze statue and then molds it into some jewelry, it is the same bit of bronze throughout."[32] Thus, a binary representation is a foundation for a lot of different things – e-money, virtual money, crypto assets, texts, pictures, sounds, etc.

Just like we cannot divide into types paper money or metallic money (besides by the material they made of – different wood or metal; or relation of money to different countries – Ukrainian hryvnia, US dollar), we cannot separate digital money into categories in the fashion made by some scientists or in media.

[31] Thomas Ainsworth, "Form vs. Matter," *Stanford Encyclopedia of Philosophy (Spring 2016 Edition)* (Stanford: Metaphysics Research Lab, Stanford University, 2016), https://plato.stanford.edu/archives/spr2016/entries/form-matter/

[32] Ibid.

Given the above, scientific society may avoid the term "digital currency" to define virtual currencies, cryptocurrency or e-money, because using it leads to confusion and inaccuracy. Digital currency is neither a separate phenomenon nor the type of money, this term mistakenly used to describe the matter of other virtual objects.

1.1.4. Cryptocurrency

Cryptocurrency. The takeaway from definitions given by the EBA[33], ECB[34], International Monetary Fund[35], Committee on Payments and Market Infrastructures, a body of the Bank for International Settlements[36], the World Bank[37] and other institutions is that *cryptocurrencies* are a subset of virtual currencies. Then, in their papers and reports, the term 'virtual currencies' is defined.

In *FinTech: Law and Regulation*, cryptocurrencies are defined as a "type of crypto assets, which is a digital representation of value that is neither issued by a central bank or a public authority nor necessarily attached to a fiat currency, but is used by national or legal persons as a means of exchange and can be transferred, stored or traded electronically."[38] This explanation gives only one new piece of information about cryptocurrency – *a type of crypto assets*[39] – the rest is a variation of a virtual currencies' definition.

[33] "EBA Opinion on 'virtual currencies'" (Paris: European Banking Authority, July 2014): 11, https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1

[34] "Virtual Currency Schemes," (Frankfurt am Main: European Central Bank, October 2012): 13, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[35] Dong He et al., "IMF Staff Discussion Note. Virtual Currencies and Beyond: Initial Considerations" (Washington, DC: International Monetary Fund, January 2016): 7, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

[36] "Digital currencies" (Basel: Bank for International Settlements, November 2015): 4, https://www.bis.org/cpmi/publ/d137.pdf

[37] Harish Natarajan et al., "FinTech note, no. 1: Distributed Ledger Technology (DLT) and blockchain" (Washington, D.C.: World Bank Group, 2017): IV, http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

[38] Jelena Madir ed., *FinTech Law and Regulation* (Cheltenham: Edward Elgar Publishing Limited, 2019), xxv.

[39] *H. Arslanian* and *F. Fischer* "use the word ***crypto assets*** to encapsulate the spectrum of innovations happening in the space" of financial system and services (cryptocurrencies, ICO, blockchain, etc.), cited from Babu Pillai, Kamanashis Biswas, and Vallipuram Muthukkumarasamy, "Blockchain Interoperable Digital Objects" in *Blockchain – ICBC 2019: Second International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings, James Joshi et al.* (Cham: Springer, 2019), 86.

Crypto-assets are a type of digital assets, recorded on a blockchain ledger, which utilizes techniques such as cryptography, distributed consensus, peer-to-peer-network, and smart contracts in order to create, transact, and verify in a decentralized manner, cited from Babu Pillai, Kamanashis Biswas, and Vallipuram Muthukkumarasamy, "Blockchain Interoperable Digital Objects" in *Blockchain – ICBC 2019: Second International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings*, James Joshi et al. (Cham: Springer, 2019), 86.

E. Dourado and *J. Brito* state that “cryptocurrency is the name given to a *system* that uses cryptography to allow the secure transfer and exchange of digital tokens in a distributed and decentralized manner. These tokens can be traded at market rates for fiat currencies”[40]. The system is a “regularly interacting or interdependent group of items forming a unified whole”[41]. The authors, thus far, stated that cryptocurrency is a set of elements not defining them specifically, therefore, this definition does not exhaustively explain the nature of cryptocurrencies per se.

Cryptocurrencies are the most developed application of blockchain technologies as established in another World Bank’s paper dedicated to cryptocurrencies and the blockchain[42].

To sum up, hitherto, all we can say about cryptocurrency through analysis of these definitions is that cryptocurrencies are:

- type of crypto assets;
- type of virtual currencies;
- a system that uses cryptography;
- an application that uses blockchain technology.

The problem of these definitions is that they do not explain what constitutes cryptocurrency, there is no given clear and fair definition of the phenomenon, furthermore, they just complicate everything giving more terms that require definitions.

The first cryptocurrency that came into being was Bitcoin. So it is only logical to start analyzing cryptocurrency features and requirements of its existence to answer the question of what cryptocurrency is.

First of all, the etymology of the word “***crypto***” is transparent and appears to be from the Greek language (κρύ̓πτω). Crypto- means *concealed, hidden, or secret*[43]. Nowadays it is associated with ***cryptography*** – “a field of computer science and mathematics that focusses on techniques for secure communication between two parties while a third-party is present. This is based on methods like encryption, decryption, signing, generating of pseudo-random numbers, etc.”[44]

[40] Eli Dourado, and Jerry Brito, “Cryptocurrency,” *The New Palgrave Dictionary of Economics, Online Edition* (2014): 1, https://www.researchgate.net/publication/298792075_Cryptocurrency

[41] “System,” Meriam Webster dictionary, Accessed 11 February 2020, https://www.merriam-webster.com/dictionary/system

[42] World Bank, “Cryptocurrencies and Blockchain,” Europe and Central Asia Economic Update (May) (Washington, D.C.: World Bank, 2018): 21, http://documents.worldbank.org/curated/en/293821525702130886/pdf/Cryptocurrencies-and-blockchain.pdf

[43] “crypto-,” Online Etymology Dictionary, Accessed 7 February 2020, https://www.etymonline.com/word/crypto-

[44] Mohamed Barakat, Christian Eder, and Timo Hanke, *An Introduction to Cryptography* (September 2018): 1, https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf

Indeed, cryptography is used for enabling cryptocurrencies to exist. A lot of cryptographic techniques are used to facilitate Bitcoin transactions.

Secondly, Bitcoin or other cryptocurrencies is neither "coin", nor "currency". These are just *high-level abstractions* made by developers for regular people to give a basic understanding of Bitcoin functions. In the abovementioned definitions, a cryptocurrency (in this case, Bitcoin) has *digital representation*. Indeed, one can think of Bitcoin as of a piece of information encoded somewhere (where exactly we will elaborate on in the following subsections). In the context of Aristotle's work, it is *a* ***matter*** of cryptocurrencies.

Thirdly, there are vital parts that enable Bitcoin existence, such as:

1) the Internet;
2) peer-to-peer (hereinafter the P2P) network of nodes;
3) encryption techniques;
4) blockchain.

If any of these elements disappear – the whole system falls apart. Thus, we would partially agree with *E. Dourado* and *J. Brito*, cryptocurrency is a complex term that describes a specific system. It is a conduit by which people can transact over the Internet. Referring to Aristotle's ideas, it would be ***the form*** of this phenomenon.

"Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypherpunks[45] mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept were published in 2009 in a cryptography mailing list by S. Nakamoto"[46]. Answering the *third Aristotle's question* ***(moving cause)***, S. Nakamoto is a person (a group of people) who created the first Bitcoin and the first block in the blockchain.

The main objectives for creating the first cryptocurrency are (*answer to the forth Aristotle's question –* ***final cause***):

1) decreasing transactions cost[47];
2) removing middleman – financial institutions – between parties who are willing to make a transaction[48];

[45] ***Cypherpunks*** is a group of coders and researchers that proliferate the use of encryption for data protection. Cited from "Cypherpunk definition," SearchSecurity.com, Accessed 12 February 2020, https://searchsecurity.techtarget.com/definition/cypherpunk

[46] "Frequently Asked Questions," Bitcoin, Accessed 12 February 2020, https://bitcoin.org/en/faq

[47] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009): 1, https://bitcoin.org/bitcoin.pdf

[48] Ibid.

3) creating a decentralized payment system – to eliminate state involvement and its influence on demand and supply of money;
4) achieving an acceptable level of transactions' anonymity. It is not as anonymous as cash operations, however, Bitcoin is designed to secure private users' data[49];
5) increasing control of individuals over their money[50];
6) increasing transparency[51]: all the information about transactions is available to the whole community and stored in the blockchain;
7) establishing more secure payments (this what cryptography is needed for)[52].

To sum up, ***cryptocurrency*** is an electronic online payment system existence of which depends on public trust, will and agreement to accept virtual money as a means of exchange (a social contract); it is backed up by cryptography and relies on blockchain technology, as well as the interaction between nodes that exist in the network. As a supplement and summary to this subchapter, we present Diagram 1 of Annex 1 which depicts incorrect correlation of discussed terms prevailing in scientific and media society as well Diagram 2 of Annex 1 which displays the correct one.

1.1.5. Cryptocurrency vs. Fiat money vs. Commodity money vs. Commodity

Money is usually defined *through functions they perform* in economic literature. *D. A. Martin* notices that "the problem of definition is dismissed by diverting attention to the functions of money as if they could be fulfilled simultaneously by some unspecified thing"[53]. Legal definitions of money are rare, however, those that exist echo economical view on money (see *California Commercial Code*[54]). The term "*currency*" is used to describe coins and paper money which are considered legal tender in a particular state, e.g. *Singapore Currency Act* defines "currency as currency notes and coins which are legal tender in Singapore"[55].

[49] "Frequently Asked Questions," Bitcoin, Accessed 12 February 2020, https://bitcoin.org/en/faq

[50] Ibid.

[51] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009): 6, https://bitcoin.org/bitcoin.pdf

[52] "Frequently Asked Questions," Bitcoin, Accessed 12 February 2020, https://bitcoin.org/en/faq

[53] David A. Martin, "The Medium is not Money," *Journal of Economic Issues (Association for Evolutionary Economics)* 6, no. 2/3 (1972): 68, http://web.a.ebscohost.com.skaitykla.mruni.eu/ehost/detail/detail?vid=13&sid=88792afb-84fd-4628-8423-86b4748a2c43%40sdc-v-sessmgr01&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=4725151&db=bth

[54] "California Commercial Code," § 1201(b)(24), FindLaw, Accessed 16 February 2020, https://codes.findlaw.com/ca/commercial-code/com-sect-1201.html

[55] The Currency Act, Singapore Statutes Online, Accessed 16 February 2020, https://sso.agc.gov.sg/Act/CA1967

Money performs three main **functions**: *medium of exchange, store of value, unit of account*[56]. The last one is "derivative and insufficient to designate a good as money" *in D. A. Martin's and W. T. Newlyn's* opinions[57]. Moreover, "modern money, the medium of exchange, and the unit of account are each distinct entities"[58], meaning that currency does not necessarily perform all three functions of money. *D. A. Martin* argues that it is insufficient to establish money functions that a unit could perform to explain what money is. We would like to emphasize this opinion because further analysis refers to very subjective terms on which different theories and approaches exist. The discussion regarding the nature of money, their functions, and qualities continues. Our aim in this section is showing that cryptocurrency, in perspective, can successfully function as money and defining cryptocurrency as a commodity (Hong Kong[59] and Austria[60]) is a mistake.

Characteristics (qualities) of money: *divisible, portable, acceptable, scarce, durable, stable*[61]. It is important to notice that all units that are/were used as a medium of exchange possess these features to some extent. It means that, for example, shells, which were used a long time ago as money, are somewhat scarce compared with gold, they are not divisible in contrast with tobacco; gold is more durable than fiat paper money. Therefore, if some unit does not have some qualities or only slightly satisfy a characteristic, it does not necessarily mean this item cannot work as a medium of exchange.

A **medium of exchange** is an object that is accepted in trade not to be used for production or consumption but to be traded later for something else that will be used for such purposes. When a Commodity serves as a medium of exchange, it is referred to as **Commodity Money**. When an object with no intrinsic value serves as a medium of exchange, it is referred to as **Fiat Money**. Fiat money has value simply because agents believe in that. It is an endogenous property of money — its liquidity — that gives it value[62].

Accessibility plays a key role in considering a unit as a medium of exchange. An appropriate environment and conditions are prerequisites for money to be acceptable.

[56] Klaus Kultti, "A model for money as a store of value" (Helsinki: Faculty of Social Sciences, Dep. of Economics, 2010), 2 https://helda.helsinki.fi/bitstream/handle/10138/18007/amodelfo.pdf?sequence=1

[57] W. T. Newlyn, *Theory of Money* (Oxford: Clarendon Press, 1962): 1-2, quoted in David A. Martin, "The Medium is not Money," *Journal of Economic Issues (Association for Evolutionary Economics)*, 6, 2/3 (1972): 68,

[58] David A. Martin, "The Medium is not Money," *Journal of Economic Issues (Association for Evolutionary Economics)*, 6, 2/3 (1972): 68,

[59] *Regulation of cryptocurrency around the world*, (Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018), 108-109 https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

[60] Ibid, 30.

[61] Amanda Lim Pui Sze, "Functions and Characteristics of Money," UK Essays, Accessed 13 February 2020, https://www.ukessays.com/essays/economics/functions-characteristics-money-6335.php?vref=1

[62]Olivier Ledoit, and Sébastien Lotz, "The Coexistence of Commodity Money and Fiat Money" (Zürich: University of Zurich, Department of Economics, 2011): 3, http://www.econ.uzh.ch/static/wp/econwp024.pdf

Firstly, units need to be *convenient in use*. They should have high *liquidity*, meaning that they can be "quickly and easily transformed into other goods at a low transaction cost, usually without appreciable loss in value."[63] "The quicker you can sell off an asset as close to your asking price as possible, the more liquid an exchange is considered to be."[64] Besides, it should *be easy to store and accumulate* units, as well as to have quick access to them.

Commodity money was used a long time ago where no alternatives existed. Its use was inconvenient in nature. To receive such money, one should put labor into it (grow and harvest or mine gold and mint coins, etc.). The storage of money was a challenge too: people needed to find a specific place for money accumulation and to invest in its security, inaccessibility for intruders. The liquidity of miscellaneous commodities can vary.

Fiat currency is accessible because it is the most liquid asset among others. People have a variety of choices on how to store their money: bank deposits (checkable and savings deposits), store money at home, etc. Due to technology development, people have access to their saving via mobile, desktop, and web applications.

Regarding *cryptocurrency*, we would have to distinguish between *market liquidity* and cryptocurrency *liquidity as an asset*. Cryptocurrencies' market liquidity depends on several factors: high trading volumes, the number of active traders, low commissions, a variety of crypto exchanges[65]. The liquidity of a cryptocurrency depends on which exchange it is traded on[66]. Cryptocurrencies are relatively illiquid compared to other assets,[67] especially cryptocurrencies with low market capitalization[68] possess low liquidity problem. Only Bitcoin and Ethereum are liquid enough[69]. This is now *the main* challenge that keeps cryptocurrencies away from becoming a full-fledged medium of exchange. On the other hand, it is not a verdict for cryptocurrencies. The crypto market is risky, nonetheless, in perspective, its liquidity could be improved as long as high trading volumes will be maintained, many active traders remain on the market, and diversity of liquid crypto exchanges with low fees will be available.

[63] James Gwartney et al., *Economics: Private and Public Choice* (Mason: Cengage Learning, 2008), 264.

[64] "Cryptocurrency and Bitcoin Liquidity," Kraken, Accessed 16 February 2020, https://www.kraken.com/features/liquidity

[65] Ibid.

[66] Hio Loi, "*The Liquidity of Bitcoin,*" *International Journal of Economics and Finance* 10, 1 (2018): 20, https://www.researchgate.net/publication/321628021_The_Liquidity_of_Bitcoin

[67] Simon Trimborn, Mingyang Li, and Wolfgang K. Härdle, "Investing with cryptocurrencies - A liquidity constrained investment approach," *Journal of Financial Econometrics* (2017): 23, http://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2017-014.pdf

[68] ***Market capitalization (market cap)***, in cryptocurrency terms, means the current price of a coin times the total number of coins in the market, and often referred to as circulating supply.

[69] Vladyslav Shovkovyi, "What Investment Opportunities Do Cryptocurrencies Provide?" (master thesis, Kyiv School of Economics, 2018), 11, https://kse.ua/wp-content/uploads/2019/03/Vladyslav-Shovkovyi6.pdf.pdf

Regarding the *storage of cryptocurrencies*, they are stored in the blockchain entries rather than on physical objects, e.g. servers. Each node existing in the network has a copy of the whole chain of transactions. To gain access to owners' cryptocurrencies, a person has to possess a wallet.

Secondly, logically following from the previous statements, a prerequisite for money to be a medium of exchange is people's will and desire to accept units in trade. Also, people would pay for goods and services with such units if merchants and service providers are willing to accept payments in these units. Phycological and legal aspects play an important role here. Regarding the legal issue, it is necessary for the law to allow transactions with specific units or, at least, not prohibit them explicitly. The phycological aspect would be omitted here because its analysis is not the primary aim of this thesis.

Commodity money is no longer accepted as a medium of exchange, they were in circulation throughout different historical periods. *Fiat money* is an accepted medium of exchange nowadays. *Cryptocurrencies* are widely used for trading and not yet for purchasing goods and services. Although cryptocurrencies are still developing in this regard, some companies such as Microsoft[70], Overstock[71], KFC Canada,[72] etc. already accept bitcoins and other cryptocurrencies.

Cryptocurrencies can serve as a medium of exchange over the medium run if there is a growth of active users, governmental support, and relatively high liquidity is reached.

Store of value. A *store of value* is an item that people can use to transfer purchasing power from the present to the future[73]. People need to make savings for making transactions in the future. *Commodity*, *fiat money,* and *cryptocurrency* can be used to hold people's wealth. "However, there are some disadvantages of using *fiat money* as a store of value. The value of a unit of money – e.g. a dollar– is measured in terms of what it will buy. Its value, therefore, is inversely related to the price level in the economy. When inflation rises, the purchasing power of money declines – as does its usefulness as a store of value."[74]

Being a store of value depend on the ***scarcity*** of money, meaning that units cannot be easily found or duplicated. It is a widely known fact that governments cat influence the demand and supply of money by increasing currency availability. According to an investor, *R. Price*, fiat currency does not store value anymore. He argues that "global central banks have eroded 'store of

[70] "How to use Bitcoin to add money to your Microsoft account", Microsoft, Accessed 17 February 2020, https://support.microsoft.com/en-us/help/13942/microsoft-account-how-to-use-bitcoin-to-add-money-to-your-account

[71] "How do I pay with Bitcoin?", Overstock, Accessed 17 February 2020, https://help.overstock.com/help/s/article/Bitcoin

[72] "KFC Canada Is Accepting Bitcoin for Fried Chicken", Coindesk, Accessed 17 February 2020, https://www.coindesk.com/kfc-canada-is-accepting-bitcoin-for-fried-chicken

[73] Joshua Gans et al., *Principles of Economics* (South Melbourne: Cengage Learning Australia, 2014), 702.

[74] James Gwartney et al., *Economics: Private and Public Choice* (Mason: Cengage Learning, 2008), 264.

value' characteristic..." The reason for such a situation is the massive creation of currency by governments. "The less scarce, the worse an asset holds its value"[75]. This opinion reflects a known macroeconomics rule.

In contrast, *a cryptocurrency*, e.g. Bitcoin, satisfy scarcity quality perfectly, therefore, it is a convenient store of value, because this cryptocurrency has a steady supply – "only 21 million bitcoins will ever be created."[76] The limited amount of supply is a common characteristic for most cryptocurrencies.

Unit of account. "Unit of account is a yardstick people use to post prices and record debts"[77]. Units of money are used to measure the exchange value and costs of goods, services, assets, and resources[78]. It is a prevalent opinion that in order to perform this function, money should be stable.

Stability means that money's purchasing power remains steady[79]. Purchasing power is the value of a currency expressed in terms of the number of goods or services that one unit of money can buy. To measure purchasing power in the traditional economic sense, the price of a good or service is compared against a price index such as the Consumer Price Index[80] [81]. "Essentially it attempts to quantify the aggregate price level in an economy and thus measure the purchasing power of a country's unit of currency"[82]. The same could be done regarding cryptocurrency to estimate its purchasing power. It is not the option though for *commodity money* because nowadays it is not used as a medium of exchange. However, commodity money is the most stable among the three types of money that we compare due to stable intrinsic value.

National currencies are not stable by definition because their stability depends on monetary policy of governments, i.e. central banks are responsible for maintaining the currencies' value and they have the opportunity to manipulate the inflation-deflation cycles. Venezuela, South

[75] Rob Price, "Fiat currency doesn't store value: Investor shares advice on where we can store our value", IOL, Accessed 10 February 2020, https://www.iol.co.za/business-report/opinion/fiat-currency-doesnt-store-value-investor-shares-advice-on-where-we-can-store-our-value-32713407

[76] "Frequently Asked Questions," Bitcoin, Accessed 12 February 2020, https://bitcoin.org/en/faq

[77] Joshua Gans et al., *Principles of Economics* (South Melbourne: Cengage Learning Australia, 2014), 702.

[78] James Gwartney et al., Economics: Private and Public Choice (Mason: Cengage Learning, 2008), 264.

[79] National Bank of Belgium, "A Stable Currency," (Brussels: National Bank of Belgium, 2013):52, http://www.nbbmuseum.be/doc/chap5e.pdf

[80] Adam Hayes, "Purchasing Power," Investopedia, Accessed 10 February 2020, https://www.investopedia.com/terms/p/purchasingpower.asp

[81] ***Consumer Price Index*** measures the average change in prices over time that consumers pay for a basket of goods and services, commonly known as inflation. Cited from James Chen, "Consumer Price Index – CPI," Investopedia, Accessed 10 February 2020, https://www.investopedia.com/terms/c/consumerpriceindex.asp

[82] James Chen, "Consumer Price Index – CPI," Investopedia, Accessed 10 February 2020, https://www.investopedia.com/terms/c/consumerpriceindex.asp

Sudan, Zimbabwe[83], to name a few, are countries that struggle with hyperinflation due to unsatisfactory governmental monetary policy.

Cryptocurrencies are not stable as well. *I. G. A. Pernice* et al. points out that despite increased attention to cryptocurrencies and their popularity, users remain unenthusiastic regarding cryptocurrency acceptance as standard means of payment precisely because of large fluctuations in currency prices. "Stablecoins" – a new generation of cryptocurrencies – try to tackle the instability problem nowadays[84]. As an illustration, while Tether – a stablecoin that binds Tether "value to the price of national currencies like the US dollar, the Euro, and the offshore Chinese yuan"[85] – might promise some sort of stability, it still depends on fiat currency (that is true of all existing stablecoins nowadays), therefore, they are not stable as well.

Stability, acceptability, unit of account, medium of exchange, and store of value are intrinsically subjective terms. Their perception highly depends on people's judgments about the world. Stability even belongs to a philosophic domain. There is nothing stable per se. The value of a currency will never be stable as long as rules of demand and supply exist. With that in mind, it is natural for society to adapt in response to changes. For this reason, the volatility of the cryptocurrency market should not be an obstacle for society to consider and accept cryptocurrency as money and to believe that they can serve as a unit of account.

It is pertinent to include additional criteria for comparative analysis, such as an *issuer of money and intrinsic value*.

Issuer. *Fiat money* has issuer – a national central bank. *Cryptocurrency* does not have an issuer in most cases. Referring to *S. Nakamoto's* white paper, cryptocurrency is generated in the system and was designed as an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them[86]. Any type of *commodity* can fulfill the role of commodity money[87], therefore, commodity money are ether, handmade, manufactured, or mined.

[83] Suzette Shultz , "Three Countries in Hyperinflation," The Borgen Project, Accessed 13 February 2020, https://borgenproject.org/three-countries-in-hyperinflation/

[84] Ingolf G. A. Pernice et al., "Monetary Stabilization in Cryptocurrencies – Design Approaches and Open Questions" paper presented at Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland (2019): 1, https://www.researchgate.net/publication/334995475_Monetary_Stabilization_in_Cryptocurrencies_-_Design_Approaches_and_Open_Questions

[85] "Main," Tether, Accessed 29 February 2020, http://tether.to/

[86] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (Bitcoin Project, 2009): 4, https://bitcoin.org/bitcoin.pdf

[87] Thomas Herold, "What is Commodity Money?" Herold Financial Dictionary, Accessed 10 February 2020, https://www.financial-dictionary.info/terms/commodity-money/

Intrinsic value. *Commodity money* is that type of money that possesses intrinsic value on its own, independent of any governing body. This means the money itself contains its worth[88] just for the reason of mere existence. In other words, we can calculate and estimate the intrinsic value of a commodity. By contrast, *fiat money* does not possess intrinsic value, they are worthless of themselves " in the form of consumption or as input into production."[89] They are valuable just because governments claimed so and not because they are valuable in nature. The same is also the case for *cryptocurrency* apart from government support. Both cryptocurrency and fiat money are accepted as a means of exchange because people have faith in the future usage of cryptocurrency for transactions. "People are willing to accept it because they know it could be used to purchase real goods and services."[90]

It should be pointed out that intrinsic value is meaningless in economics. All value is subjective, meaning it is a result of acts of valuing by people[91]. Almost any item could be used as a medium of exchange as long as society accepts it as such.

Regarding ***cryptocurrency being a commodity***, this approach is wrong for the following reasons.

Natural and fungible. "**A commodity** is a basic good used in commerce that is *interchangeable* with other goods of the same type." *Basic good* means that a commodity has been grown or extracted from their natural state and brought up to a minimum grade for sale in a market place [92]. It is obvious that *cryptocurrencies* are not coming from nature and are not derived from natural resources. They are *fungible* but this characteristic is entirely different for cryptocurrencies. They are fungible all the way but commodities can vary in quality so we cannot say that they are fully interchangeable. Only commodities of the same type and quality can be equal. We cannot assess the quality of cryptocurrency, as well as of fiat money, just like we can do it with commodities (e.g. wheat grade and quality requirements for futures contracts).

It may be an argument that cryptocurrency is an *intangible commodity*, meaning that you cannot see or touch it. One example of intangible commodities we encounter in the economic literature is services. Another instance, according to the Commodity Futures Trading Commission (hereinafter the CFTC),[93] is an emission allowance. While it is obvious that cryptocurrencies are

[88] Ibid.

[89] David Andolfatto, "A Model of Fiat Money" (October 2008): 1, http://www.sfu.ca/~dandolfa/olg2008.pdf

[90] James Gwartney et al., *Macroeconomics: Private and Public Choice* (Mason: Cengage Learning, 2009), 264.

[91] Detlev S. Schlichter, *Paper Money Collapse*: *The Folly of Elastic Money* (Hoboken, NJ: John Wiley & Sons, 2014), 35, https://books.google.com.ua/books?id=gVvOAwAAQBAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false

[92] James Chen, "Commodity," Investopedia, Accessed 19 February 2020, https://www.investopedia.com/terms/c/commodity.asp

[93] Matthew F. Kluchenek, "The Status of Environmental Commodities Under the Commodity Exchange Act," Harvard Business Law Review, Accessed 19 February 2020, https://www.hblr.org/2015/01/the-status-of-environmental-commodities-under-the-commodity-exchange-act/

not services, one may insist that cryptocurrency may be similar to the emission allowance commodity. However, it is a mistaken assumption due to the exitance of the criteria listed below.

Input. “Commodities are most often used as inputs in the production of other goods or services”[94]. Cryptocurrency does not have derived products, it cannot be processed to create a new good or used while delivering services. Returning to the emission allowance, they are directly needed in the production of goods, moreover, it is impossible to produce anything following the law if a manufacturer does not have these allowance, therefore, such commodity can be regarded as input in the production.

Consumption. This criterion directly derives from the previous one. Commodities are destroyed in their existing form in the process of production. They are modified and they disappear completely when they end up with consumer (wheat becomes flour which becomes bread that is consumed by people; crude oil becomes petroleum which is consumed by cars; emission allowance burn when a manufacturer reaches the limits of pollution specified in the emission allowance). *Cryptocurrencies* cannot be consumed, they continue to exist in the blockchain because they are not commodities and their main purpose is to function as fiat currencies.

Supply chain. All commodities have a supply chain[95]. There are two implications from this fact:

1) there is *a substantial gap in time between the production* of commodity *and its receiving* by a consumer;
2) *more than two participants are present in a supply chain*: a party that grows or extracts a commodity, processes a commodity, carrier, a storage provider, consumer, etc. There may be a party that performs several functions and there may be more intermediaries that work with a particular commodity before this commodity goes to a consumer. It does not, however, change the fact that the supply chain exists.

Cryptocurrencies do not have a supply chain. The production of cryptocurrency stems from protocols that govern blockchains. In most cases, new cryptocurrencies emerge due to the mining activities of network participants. When a currency is mined it is already in circulation, it is already owned by someone, the ledger is cryptocurrency’s final destination.

Amount of production. Depending on demand changes, commodity producers can increase the supply of commodities by scaling up production or decrease it by bringing down production activity. It is impossible with most *cryptocurrencies* because miners receive a reward

[94] James Chen, “Commodity,” Investopedia, Accessed 19 February 2020, https://www.investopedia.com/terms/c/commodity.asp

[95] David Bucha and Charlie Errington, “Commodities demystified: A Guide to Trading and Global Supply Chain,” (Singapore: Trafigura Group, 2019), 10, https://www.commoditiesdemystified.info/pdf/CommoditiesDemystified-en.pdf

for mining activity per each block. The amount of received coins is constant and is determined by a protocol (it may decrease with time but it remains constant per each block). Miners and developers have no control over the amount of produced cryptocurrency units.

1.2. Machinery and philosophy of cryptocurrencies. Blockchain technology

This subchapter intends to explain the inner structure of the cryptocurrency system and its main concepts to understand how it works. In the following text, we mostly analyze the Bitcoin system. One should bear in mind that some differences in blockchain functionality could be observed in other systems, however, the basic rules and concepts are the same in most cases.

Blockchain. Cryptocurrencies run on a system that is not regulated by any centralized authority or supervised by any governmental institution or non-governmental organization with a special status. Regardless of a cryptocurrency type, i.e. Bitcoin, Litecoin, etc., each currency is supported by a decentralized P2P network – *blockchain*.

To explain what constitutes blockchain we need to establish the meaning of distributed ledger (hereinafter the DL) and the distributed ledger technology.

The **distributed ledger** is a collection of records (making up a database), where identical copies of each record are held on numerous computers across an organization, a country, multiple countries, or the entire world, either jointly or partitioned by the parties to which each record relates. A blockchain is a type of DL, but not all DL are blockchains. The **DLT** is a software that creates a DL[96].

"Blockchain is a type of distributed ledger taking the form of an electronic database that is replicated on numerous nodes spread across an organization, a country, multiple countries, or the entire world. Records in a blockchain are stored sequentially in time in the form of blocks. Each block typically contains a cryptographic hash of the previous block, a timestamp, and transaction data, which makes it inherently resistant to modification of the data."[97] Due to such type of data structure – the chain or linked list – and *consensus protocol* existence, "any attempt of data tampering can be immediately detected."[98]

Mining. Verification of blocks happens due to ***mining*** – the process of collecting data in a block that would be appended to the blockchain[99]. A ***miner*** is a separate special node (computer with appropriate software) in the network that contributes its computational to verify a transaction.

[96] Jelena Madir ed., FinTech Law and Regulation (Cheltenham: Edward Elgar Publishing Limited, 2019), xxvii.

[97] Ibid., xxiv.

[98] Wenbo Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access* 7 (2019): 1, https://arxiv.org/pdf/1805.02707.pdf

[99] Imran Bashir, *Mastering Blockchain* (Birmingham: Packt Publishing , 2017), 131.

Miners play a crucial role in securing the blockchain. "Roughly one new block is created every 10 minutes."[100]

Consensus refers to the act of more than 50 percent of nodes concluding that a proposed block message is authenticated and verified so that the block can be added to the DL. The consensus is achieved due to ***consensus protocol*** – the ***Proof of Work*** (hereinafter the PoW) – a computer protocol in the form of an algorithm constituting a set of rules for how each participant in the DL should process messages and how those participants should accept the processing done by other participants[101].

Nodes receive a ***reward*** for mining: every time a new block is created, a new set of coins flow into the system[102]. Additionally, nodes collect transactions fee[103].

Transactions. In the cryptocurrency sphere, "***transaction*** is a transfer of coins from one wallet to another"[104]. Cryptocurrency is not stored in a wallet per se, rather they exist in a blockchain transaction history. Wallets are just means of access to owners' cryptocurrency, it facilitates transactions between parties. For this reason, we cannot think of the transaction in a conventional way: the ownership change is peculiar in nature. With cash or e-money transactions there is "movement" of money. Money is taken from the payer/his account and given to the payee/transferred to his account. There is no such thing with cryptocurrency.

When a transaction is made, its details will be broadcast to every node in the network. The transactions made over a set period are collected to form a "block."[105] Miners process transactions by verifying the *ownership* of the currency from source to destination[106].

It follows from S. Nakomoto's work that once a transaction is settled, it is irreversible[107]. It is true for all cryptocurrencies because they all have the underlying blockchain technology.

To make a transaction, a person needs to have a pair of keys (**private** and **public**) and cryptocurrency **address** – the destination of a payment. There can be multiple public keys but only one private. The address is generated from the public key which, in turn, is derived from the private key. "The address is recorded on the blockchain with value or no value at all. An address can

[100] Ibid.

[101] Jelena Madir ed., FinTech Law and Regulation (Cheltenham: Edward Elgar Publishing Limited, 2019), xxv

[102] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009): 1, https://bitcoin.org/bitcoin.pdf

[103] Jimmy Song, *Programming Bitcoin: Learn how to program Bitcoin from scratch* (Sebastopol, CA: O'Reilly, 2019), 100.

[104] Hari Krishnan R., Sai Saketh Y., and Venkata Tej Vaibhav M., "Cryptocurrency Mining – Transition to Cloud," *International Journal of Advanced Computer Science and Applications* 6, 9 (2015): 115, https://www.researchgate.net/publication/283810104_Cryptocurrency_Mining_-_Transition_to_Cloud

[105] Imran Bashir, *Mastering Blockchain* (Birmingham: Packt Publishing , 2017), 119.

[106] Hari Krishnan R., Sai Saketh Y., and Venkata Tej Vaibhav M., "Cryptocurrency Mining – Transition to Cloud," *International Journal of Advanced Computer Science and Applications* 6, 9 (2015): 115, https://www.researchgate.net/publication/283810104_Cryptocurrency_Mining_-_Transition_to_Cloud

[107] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009): 1-3, https://bitcoin.org/bitcoin.pdf

assign its value to another address, creating a transaction of that value. The receiving address may already have a value, and the increase is added to it"[108].

A **private key** is randomly selected numbers and is 256-bit in length[109]. It is used to sign a transaction to prove the ownership of sending cryptocurrencies and to access currencies that were sent to a holder of a private key.[110] The ***curious nature of ownership*** is hidden here. A person might have a legal title to cryptocurrency, however, in case this person loses the private key, he loses control over his money. It remains inaccessible forever in the system. Interestingly, if one wanted to give all money he owns he would have two ways to do it: either transfer coins to another party or give this party the private key. In the latter case, it means that person gives up the ownership of money and his decentralized account. Hence, a private key can represent ownership of money because the owner of the private key can access, use, and dispose of cryptocurrencies related to a particular address.

A **public key** is used for party identification and verification of transactions[111]. It is used to check whether the transaction has the payer's signature signed with the corresponding private key[112].

1.3. Evolution of cryptocurrencies

Looking through white papers of different cryptocurrencies that have emerged in the course of several years, one can notice that the evolution of cryptocurrency and their exitance are driven by shortcomings of Bitcoin. These cryptocurrencies are commonly referred to as ***altcoins*** (currencies that are not Bitcoin) in the media and literature. To describe their functionality and distinction from Bitcoin, we will take several cryptocurrencies that have the biggest market capitalization, statistics of which provided by CoinMarketCap[113], and illustrate cryptocurrencies advantages and disadvantages.

Ethereum (ETH). Ethereum is an open-source, public, blockchain-based DL featuring smart contract functionality. It enables developers to build blockchain applications, i.e. "DApps", with business logic that is executed in a trustless environment while leveraging the high

[108] Nick Furneaux, *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence* (Indianapolis: Wiley Publishing, Inc. 2018), 67-68.

[109] Imran Bashir, *Mastering Blockchain* (Birmingham: Packt Publishing , 2017), 116.

[110] Jelena Madir ed., FinTech Law and Regulation (Cheltenham: Edward Elgar Publishing Limited, 2019), xxx- xxxi

[111] Mehmet Aydar et al., "Private Key Encryption and Recovery in Blockchain," (2019): 4-5, https://www.researchgate.net/publication/334361184_Private_key_encryption_and_recovery_in_blockchain

[112] Rui Zhang, Rui Xue, and Ling Liu, "Security and Privacy on Blockchain," *ACM Computing Surveys* 52, 3, article 51 (July 2019): 5, https://arxiv.org/pdf/1903.07602.pdf

[113] "Top 100 Cryptocurrencies by Market Capitalization," CoinMarketCap, Accessed 20 February 2020, https://coinmarketcap.com/

availability of the Ethereum network[114]. Ethereum has a native cryptocurrency called *Ether*, i.e. ETH, and is used to compensate miners who secure transactions and it will always be needed to execute request operations on Ethereum[115].

Bitcoin was originally designated for currency, therefore, it has a limited range of utilization. Contrariwise, Ethereum is a platform that facilitates new kinds of applications. This is the main distinction of Ethereum from Bitcoin.

Also, Ethereum uses an improved consensus algorithm called *Proof of Stake (*hereinafter the PoS*)*: it reduces centralization risks, offer security against different types of 51% attacks, requires less consumption of electricity due to the algorithm validation process, and more[116]. Additionally, Ethereum uses a new concept – "gas" – to facilitate transactions[117].

Ripple (XRP). As stated at Ripple White Paper, it is a real-time decentralized global network for payment settlements based on an agreement between Ripple and network participants[118]. It is a network where currency can be transferred between entities. Mainly, Ripple is used in the banking sector because RippleNet participants are categorized into two key groups: *network members* (banks and payment providers which represent the biggest pool of Ripple users) and *network users* (corporates, consumers, and others)[119]. XRP is a native currency of Ripple[120].

Key *disadvantages* of Ripple:

- Although, the White Paper states that the network is decentralized, it is not true because the network is run by a privately held company[121]. Furthermore, validation of the transaction is different: Ripple approaches the validation process through designated trusted nodes – validators. It is a subnetwork inside the network. These validators form a consensus on the legitimacy of the

[114] "What is Ethereum?" EthHub, Accessed 20 February 2020, https://docs.ethhub.io/ethereum-basics/what-is-ethereum/

[115] "What is Ether?" EthHub, Accessed 20 February 2020, https://docs.ethhub.io/ethereum-basics/what-is-ether/

[116] "Proof of Stake (PoS)," EthHub, Accessed 20 February 2020, https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/

[117] Vitalik Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralizes Application Platform," (2013): 14, https://static1.squarespace.com/static/5793509acd0f6810d1242921/t/5abfb9cd575d1f2de635e7a5/1522514382746/Ethereum-ETH-whitepaper.pdf

[118] Ripple, "*Solution Overview*," 6, https://static1.squarespace.com/static/5793509acd0f6810d1242921/t/5abfba102b6a28a926f9250c/1522514455093/Ripple-XRP-whitepaper.pdf

[119] Ibid, 8-10.

[120] "XRP," XRP Ledger, Accessed 20 February 2020, https://xrpl.org/xrp.html

[121] "Frequently Asked Questions," Ripple, Accessed 20 February 2020, https://ripple.com/faq

transaction[122]. It proves that the network is a private centralized blockchain. It is fair to say that the centralized nature of Ripple goes against the philosophy and spirit of cryptocurrencies.

- XRPs cannot be mined due to the centralized nature of the network[123].
- XRPs have a limited supply – about 100 billions of tokens and they are already created but not released into circulation. The largest holder of the XRPs is the company itself. The managing staff of the company owns a great deal of XRPs[124]. Ripple release their currency in circulation depending of the demand, meaning that it performs similar functions that central banks do within a state. Theoretically, this fact reveals a risk for manipulated inflation or deflation.

The key *benefits* of Ripple: high speed of transaction, less computing power (and therefore electricity) for transactions' validation, lower transaction costs compared to e.g. SWIFT fees[125].

Litecoin (LTC). "Litecoin is a P2P Internet currency that enables instant, near-zero cost payments to anyone in the world. Litecoin is an open-source, global payment network that is fully decentralized without any central authorities"[126]. Litecoin does not have white papers because originally it was created as a clone of Bitcoin; it is shown on the Litecoin Project repository where the source code is stored[127]. Clone (or fork), in programming, has a very specific meaning: it describes that Litecoin was built based on Bitcoin's programming code. Therefore, if there were whitepapers on Litecoin, it would be almost identical to Bitcoin's.

Benefits:

- Compared with Bitcoin, transactions' validations are four times faster with Litecoin[128].
- Better storage efficiency[129];

[122] Ripple, "*Solution Overview*," 14-15, https://static1.squarespace.com/static/5793509acd0f6810d1242921/t/5abfba102b6a28a926f9250c/1522514455093/Ripple-XRP-whitepaper.pdf

[123] Davis Schwartz, "The Inherently Decentralized Nature of XRP Ledger," Ripple, Accessed 20 February 2020, https://ripple.com/insights/the-inherently-decentralized-nature-of-xrp-ledger/

[124] Marco Cavicchioli, "Ripple: Who owns the most XRP?" Accessed 20 February 2020, https://en.cryptonomist.ch/2020/01/25/ripple-who-owns-the-most-xrp/

[125] Ripple, "*Solution Overview*," 16, https://static1.squarespace.com/static/5793509acd0f6810d1242921/t/5abfba102b6a28a926f9250c/1522514455093/Ripple-XRP-whitepaper.pdf

[126] "What is Litecoin?" Litecoin, Accessed 20 February 2020, https://litecoin.org/

[127] "Litecoin Project," GitHub, Accessed 20 February 2020, https://github.com/litecoin-project

[128] "Main Page: Everything about Litecoin," Litecoin.info, Accessed 22 February 2020, https://litecoin.info/index.php/Main_Page

[129] Ibid.

- It has substantial industry support, trade volume, and liquidity[130].

Disadvantages: since Litecoin is a clone of Bitcoin, as soon as Bitcoin troubling issues resolved, Litecoin will not have anything to offer.

Monero (XMR). Monero is a cryptocurrency that tackles security issues of Ethereum and Bitcoin. This currency is not based on Bitcoin – *CryptoNote protocol* is a basis for Monero[131]. Monero uses three different technologies to hide receiver, sender identities, addresses, and money amount, i.e. ring signatures, ring confidential transactions (RingCT), and stealth addresses [132]. Also, Monero uses Kovri – a hidden network like Tor which "hides the transaction broadcast, so other nodes do not know who created transactions"[133]. The first feature of Monero is that all transactions on the network are private by mandate; there is no way to accidentally send a transparent transaction[134]. The second one: Monero has no limits when it comes to hard block size, in particular, "the block size can increase or decrease over time based on demand. It is capped at a certain growth rate to prevent outrageous growth"[135]. On top of that, the network is fast: transaction validation takes two minutes [136].

The most visible *disadvantage* is that it is hard to bring new features into Monero or implement improvements. It means that the Monero community is not that active compared to e.g Bitcoin or Ethereum. It is implied after viewing users' activity on Monero Forum[137], moreover, it is up to Monero developers to decide which feature to adopt, participants do not have any impact on that process. Another disadvantage is that there are not many wallets that have been developed for Monero[138].

Abovementioned cryptocurrencies are enough to show differences and similarities. Even though Bitcoin is the most popular crypto, one should not assume that altcoins governed by the same rules or uses exactly the same technologies as Bitcoin does.

[130] Ibid.

[131] Brandon Goodell, Sarang Noether, and Arthur Blue, "Compact linkable ring signatures and applications," Cryptology ePrint Archive, Report 2019/654 (2019): 1, https://web.getmonero.org/resources/research-lab/pubs/MRL-0011.pdf

[132] Ibid, 1-2.

[133] "FAQ," Monero, Accessed 22 February 2020, https://web.getmonero.org/get-started/faq/

[134] Ibid.

[135] Ibid.

[136] "Technical Specs," Monero, Accessed 22 February 2020, https://web.getmonero.org/technical-specs/

[137] Monero Forum, Monero, Accessed 22 February 2020, https://forum.getmonero.org/6/ideas

[138] "The Complete Guide to Monero Cryptocurrency," BitDegree, Accessed 22 February 2020, https://www.bitdegree.org/tutorials/monero/#The_Advantages_and_Disadvantages_of_Monero

1.4. Legal status of cryptocurrencies around the world

In June 2018, *Global Legal Research Center of The Law Library of Congress* presented an overarching report on the legal status of cryptocurrencies around the world that covers 130 countries as well as some regional organizations that have issued laws or policies on the subject [139]. Mostly, this paper is dedicated to tax regulation or licensing requirements regarding currencies and there is no information about civil liability that could arise from cryptocurrency relations. However, the report gives an overall understanding of how governments perceive and treat cryptocurrencies.

According to the report, no country recognizes any cryptocurrency as **legal tender**. *D. Goldberg* explained that "legal tender concept originates in contract law"[140]. A ***legal tender*** is simply an object which functions as a mean of exchange that one party gives to another to fulfill his obligation under the contract if the form of payment is not specified in the agreement. The payee cannot refuse to take the object that is recognized as legal tender on the grounds that he wanted to receive another form of payment. To avoid parties' disagreement regarding means of exchange each country, in most cases, gives the status of legal tender to the currency it issues[141].

We present three tables drown up based on the report – *Tables 2, 3, and 4 of Annex 3* – to show whether states have statutes or other documents that regulate cryptocurrencies issues and how governments view cryptocurrencies in general and for tax purposes.

After analysis of the report and completing tables (*Table 3 and 4*), one can discover how states remain lost in the cryptocurrency sphere and confused by their nature. There is no unambiguous and final definition of cryptocurrencies adopted by all countries. Cryptocurrencies (virtual currencies) may be defined as one thing in general but for tax purposes, they are defined as other things. *The U.S. Internal Revenue Service* considers virtual currencies to be property[142], *the U.S. Securities and Exchange Commission* regards initial coin offering (hereinafter the ICO) as securities[143] , the judge *A. Nathan* in criminal proceeding proclaimed that bitcoins are money that accepted as payment for goods and services[144], the *U.S. CFTC* stated that bitcoin and

[139] *Regulation of cryptocurrency around the world*, (Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018), https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

[140] Dror Goldberg, "Legal Tender," Working Papers (Ramat Gan: Bar-Ilan University, Department of Economics, 2009): 6, https://www.biu.ac.il/soc/ec/wp/2009-04.pdf

[141] Ibid, 3-5.

[142] Matthew Blumenfeld et al., "Regulatory Brief. Carving up crypto: Regulators begin to find their footing," (New York: PwC, 2018): 3, https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/cryptocurrency.pdf

[143] Ibid, 2.

[144] Jamie Redman, "New York Judge Classifies Bitcoin As Money," Bitcoin.com, Accessed 24 February 2020, https://news.bitcoin.com/judge-classifies-bitcoin-money/

cryptocurrencies are properly defined as commodities[145]. When state authorities and judges cannot make their minds about the nature of cryptocurrencies, it signals the lack of research and awareness on the topic. This situation disrupts the economy, creates either legal vacuum or controversy among deferent legal documents, thus, spreads confusion among participants of the crypto-market.

Table 2 shows that states are divided into **four groups**:

1) states that maintain *status quo* regarding cryptocurrencies and do not develop any status that may regulate cryptocurrencies;
2) states that impose an *explicit ban* of cryptos forbidding any transactions with them;
3) *implicit ban* where it is difficult for the citizenry to access the crypto-market;
4) states *that regulate some cryptocurrency issues* (taxation, anti-money laundering & anti-terrorism financing, or both).

Some states are more progressive than others which try to keep pace with the times, namely, Switzerland and Lichtenstein. In the Swiss Canton of Zug, bitcoin and ether are functioning on the same level as fiat money: the *Commercial Register Office* accepts such payment for administrative costs and as a contribution for creating a company; municipal services can be paid in bitcoin up to CHF200[146]. Virtual currencies assume the functions of legal tender in Lichtenstein, however, the *Financial Market Authority* pointed out that virtual currencies do not constitute fiat currency[147].

Also, the *Isle of Man*, which is a Crown Dependency of the United Kingdom, frequently referred to as "Bitcoin Island," remains one of the most progressive lands concerning cryptocurrency regulations[148].

The current state of affairs reflects the reluctance of most states to face inevitable changes in technologies. Governments are responsible for citizenry and business protection, thus, postponing the adoption of needed regulation will only bring damages which could be avoided if states were more eager to figure out the nature of cryptocurrencies.

The comparative *Table 1 of Annex 2* presents a summary of this Chapter and reflects features of e-money, virtual, digital currencies, and cryptocurrencies.

[145] Scott D. Hughes, "Cryptocurrency Regulation and Enforcement in the U.S.," *Western State University Law Review* 45, 1 (2017): 5, http://www.scotthugheslaw.com/documents/CRYPTOCURRENCY-REGULATIONS-AND-ENFORCEMENT-IN-THE-US-2.pdf

[146] *Regulation of cryptocurrency around the world*, (Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018): 77, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

[147] Ibid, 71-72.

[148] Ibid, 66-67.

2. CONTRACTUAL LIABILITY IN CRYPTOCURRENCY RELATIONS

2.1. Contractual rights and obligations of cryptocurrency private legal relations participants and their liability

For the sake of brevity, we displayed all private actors in *Table 5 of Annex 4* and provided all the necessary information about them. The Table may be referred to at any point for the clarification of an actor's role in the cryptocurrency market.

2.1.1. Mining Contractual relationships

Regular mining. Mining of cryptocurrencies can be conducted through solo mining, mining pools, and cloud mining[149]. Solo mining is not subject to contractual relations, whereas such relations arise in the case of mining and cloud mining pools.

*A **mining pool*** is an allied group of miners who are jointly and continuously trying to mine a block. The term "miner" in this definition refers to a participant of a mining pool and does not correspond to the narrow definition used in the subchapter dedicated to the blockchain. There is, in most cases, an organization or company which manages a mining pool and may provide additional services. Depending on the existence and the role of "mining manager," a payment that a company receives from miners, a contribution that miners make, and the protocol that governs a mined cryptocurrency(-ies) several types of mining pools may be distinguished.

Mining pools *by the protocol that* governs blockchain (*the main two types*):

1. mining pools engaged in mining cryptocurrency that uses ***PoW*** protocol;
2. pools that mine ***PoS*** cryptocurrencies[150].

This distinction matters because the protocol that governs cryptocurrency determines pool participants' actions. It is necessary to allocate computing power to increase the probability of mining the next block and receive a reward in cryptocurrencies in the PoW blockchains. The PoS protocol requires a validator node to store an amount of cryptocurrency in a digital wallet. The more cryptocurrency recorded on the validators' account, the higher the odds of obtaining the reword for the next created block. Therefore, participants are supposed to contribute their

[149] Inna Ershova and Elena Trofimova, "Майнинг и предпринимательская деятельность: в поисках соотношения," *Актуальные проблемы российского права* 103, 6 (July 2019): 77, https://cyberleninka.ru/article/n/mayning-i-predprinimatelskaya-deyatelnost-v-poiskah-sootnosheniya

[150] Darren J. Sandler, "Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?" *Santa Clara High Technology Law Journal* 34, 3 (2018): 257-260, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1628&context=chtlj

computational power in the first case; sending owned cryptocurrency to one central wallet is needed in the second scenario.

Mining pools according to the *presence or absence of managing operator*:

1. ***Centralized pools*** have an operator that manages pool's work. The server that is managed by the operator constitutes just one node in a blockchain[151]. Such pools often have official webpages with posted General Terms and Conditions as well as remuneration terms (either included in the mentioned document or posted as a separate document).
2. ***Decentralized pools*** comprise independent miners where each miner represents one node in a blockchain, e.g. P2Pool, BitPenny, Eligius[152]. Decentralized pools protect the initial idea behind cryptocurrencies – decentralization – but they are not as successful as centralized ones. BitPenny stopped functioning in 2011[153], Eligius web page has not been accessible since 2017.[154] Due to their decentralized nature, nobody could be held accountable for any disruption in the network, damages, or losses.

There are other classifications such as distinguishing mining pools *by a model of remuneration payment* (proportional, Pay Per Last N Shares, Pay Per Share, etc.),[155] *a variety of mining coins* (single pool and multipool),[156] etc. but we mentioned just two the most relevant.

Mining contracts have nonconforming nature. Signing a regular contract, parties receive some goods or services in a more or less stipulated period, contrastingly, it is not the case with mining contracts. Firstly, mining companies do not make an invitation to negotiate the terms of the contract, instead, they propose standard Terms and Conditions agreements on the website. Secondly, there is a great degree of uncertainty in such contractual relationships due to the technical difficulty of the next block mining. These contracts are also highly pricy. With every newly mined block the level of complexity of the next puzzle to be solved arises, therefore, the solution requires more resources from miners. These resources require additional expenditure from miners part, e.g. utilities, equipment depreciation and need of its renewal, etc. All these do not

[151] "Пулы для майнинга — самые прибыльные пулы в 2020," Coinpost, Accessed 7 March 2020, https://coinpost.ru/p/pul-dlya-majninga-samye-pribylnye-puly-v-2019-godu#loc-20

[152] Ibid.

[153] "Bitpenny Closes Indefinitely," Bitcoin Miner, Accessed 7 March 2020, http://www.bitcoinminer.com/bitpenny-closes-indefinitely/

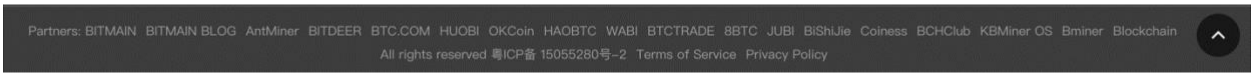
[154] Jamie McCormick, "Eligius Bitcoin Mining Pool Review," Bitcoins In Ireland, Accessed 7 March 2020, https://bitcoinsinireland.com/eligius-bitcoin-mining-pool-review/

[155] Anton Sizov et al., "Лучшие пулы для майнинга криптовалюты на 2020 год," Майниг Криптовалюты, Accessed 8 March 2020, https://mining-cryptocurrency.ru/luchshie-puly-dlya-majninga/

[156] "Пулы для майнинга — самые прибыльные пулы в 2020," Coinpost, Accessed 7 March 2020, https://coinpost.ru/p/pul-dlya-majninga-samye-pribylnye-puly-v-2019-godu#loc-20

guarantee the profit: consumers only purchase the probability of successful mining and managing services from mining companies. Neither centralized pool managers nor decentralized mining pools offer stability. The time when the next block will be found by a particular pool, i.e. miners receive their portion of mined cryptocurrency, is unknown. The amount of crypto that a miner will receive varies. There is a theoretical possibility that a miner will make all the necessary payments for receiving crypto but ultimately he does not receive any cryptocurrency. The purpose of the contract is to gain crypto, however, if the purpose is not met there is no one to blame because parties agreed to such terms of the contract.

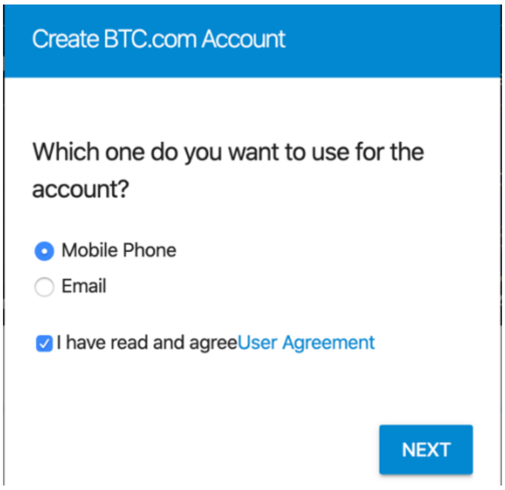
Mining pool companies provide a link to a user service agreement most frequently in the footer[157] of a web page and on the form of user registration. If a user registers on the website, it is considered as an acceptance of the agreement. More often than not, the registration form does not contain a checkbox where a user forced to take actions to accept the agreement (Antpool[158]) or contain already checked field signifying a user acceptance (BTC.com[159]). This approach in the interface significantly lowers the probability that the user reads the agreement.



Partners: BITMAIN BITMAIN BLOG AntMiner BITDEER BTC.COM HUOBI OKCoin HAOBTC WABI BTCTRADE 8BTC JUBI BiShiJie Coiness BCHClub KBMiner OS Bminer Blockchain

All rights reserved 粤ICP备 15055280号-2 Terms of Service Privacy Policy

Picture 1: Antpool footer (unvivid link to Terms of Services)



Create BTC.com Account

Which one do you want to use for the account?

● Mobile Phone

○ Email

☑ I have read and agreeUser Agreement

Picture 2: BTC.com registration form (already marked checkbox by interface creators of a website)

The role of pool managers, according to several mining pool's terms and conditions[160][161][162], is limited to providing a necessary software enabling users to mine

[157] ***Footer*** is the last bottom section of a web page.

[158] Main, Antpool, Accessed 8 March 2020, https://v3.antpool.com/home

[159] Main, BTC.com, Accessed 8 March 2020, https://pool.btc.com/?_ga=2.106616384.279728806.1583883976-291678957.1583883976

[160] "General Terms and Conditions," Slush Pool, Accessed 8 March 2020, https://slushpool.com/about/tos/

[161] "Antpool User Service Agreement," Antpool, Accessed 8 March 2020, https://v3.antpool.com/copyRight1

[162] "Условия использования," 2Miners, Accessed 8 March 2020, https://2miners.com/ru/terms

cryptocurrencies. The software itself provides the possibility to create a user account, connect to the mining pool, request mined coins, track the activity of participating nodes, etc. The main obligation of the managers is to accept the input of users, e.g. computing power, use it for mining, track how much work was done by a particular node, and distribute remuneration according to the remuneration and payment rules.

Mining companies try to limit their responsibility in terms of use as much as possible. Analyzing the general terms and conditions of one of the biggest mining pools by hash rate distribution[163] – Antpool – we pinpointed *three main clauses* that worth consideration. They are designated to limit the liability of the company before the user or restrict a particular user's right.

I. Force majeure clause. Antpool included in the force majeure clause following incidents: hacking, computer viruses, "*collapse or failure of use of the system operated by Antpool due to any Force Majeure or any other cause beyond the control of the Company*"[164], among others.

A cyber-related event being a force majeure could be disputable. Minor, middle-sized, or even considerable cyber-attacks could be and should be prevented by service providers especially when companies manage someone's money. To this effect, IT security policies, adherence to industry standards (e.g. ISO 27000), implementation of a business continuity approach, requirements for cryptocurrency insurance, compliance with IT disaster recovery procedures should be implemented by such companies[165]. These standards will help to reduce the possibility of network penetration and disruption by malware and hacking. Companies may be reluctant to do so due to the lack of special authorities supervision and regulation. Thus, policymakers should consider the adoption of required regulation on that occasion which will contribute to maintaining the balance between parties' rights and obligations in consumer contracts.

Some companies may use a broader language in contracts and do not list specifically cyber-events as being a force majeure, e.g. 2miners[166]. In this case, a company may be held liable for breach of contract and corresponding damage.

Classic Maritime Inc v Limbungan Makmur SDN BHD & Anor case might apply to the contractual liability of service providers. In this case "the Court of Appeal has awarded substantial damages to the innocent party after a force majeure event, in circumstances where the party seeking to rely on the force majeure event to excuse liability would not have been able to perform

[163] "Hashrate Distribution: An estimation of hashrate distribution amongst the largest mining pools," BLOCKCHAIN, Accessed 8 March 2020, https://www.blockchain.com/en/pools

[164] "Antpool User Service Agreement," Antpool, Accessed 8 March 2020, https://v3.antpool.com/copyRight1

[165] Craig Rogers, Wendy Boucrot, Michael Bahar, "Is a cyber-attack "Force Majeure"? Je ne crois pas!" Lexology, Accessed 8 March 2020, https://www.lexology.com/library/detail.aspx?g=9f8784de-aa99-4eed-ab92-79a3353582bf

[166] "Условия использования," 2Miners, Accessed 8 March 2020, https://2miners.com/ru/terms

its obligations under the contract (even if the force majeure event had not occurred)". It means that it is not enough for the party to show that force majeure event occurred, the party should also prove that he would perform the obligation if the preventing event has not happened [167]. If courts of different jurisdictions adopted such an approach, service providers would also need to prove their capacity to perform their obligation if cyber-event had not taken place.

II. Accuracy and reliability of content disclaimer. The Antpool stated that it "*does not guarantee the accuracy, completeness or reliability of any content or information contained on, transmitted via, linked to, downloaded from, or obtained otherwise from, the Website by the User* [..]. *And Antpool is not responsible for any products, services, information or materials purchased or obtained by the User due to the content or information on the Website. The User shall be solely responsible for the risks associated with its use of the information on the Website*."[168]

Given that an official mining pool's webpage is the only source of critical and decisive information about provided services and products, placing a disclaimer in the consumer agreement considerably shifts the balance in the contractual relationships towards the service provider. Any inaccurate, misleading information placed on the official webpage that led to damages, in theory, would not give rise to suing the company for it.

Not only the language used in the disclaimer is important for limiting the liability of a company, but also the placement of such disclaimer on the webpage plays an important role. Websites are prone to hide essential parts of users' agreement and make them unnoticeable among other website content, hence, the user is more likely to overlook this information. Such behavior of service providers may be assessed by courts and interpreted as intent to burry vital information for users, thus putting the user in an unfavorable position. "This weakens the argument that a business intended to fully disclose or disclaim whatever it is the subject of the website disclaimer. It may defeat the purpose of using a disclaimer altogether in the eyes of the courts." The disclaimer will not guarantee exempt from liability. "The facts and circumstances specific to the situation or alleged claim will be evaluated in each determination of liability by a court of law". [169]

III. Arbitration clause is common for Terms and Conditions agreements.

The Antpool included such clause as follows: "*any dispute between the User and Antpool shall first be resolved through negotiation in good faith. In case of failure to reach an agreement through negotiation, such dispute shall be referred to and finally settled by arbitration* [...]". The

[167] Mark Goodrich, Hirra Tung, "Force Majeure: substantial damages even if you cannot perform" (New York: White & Case LLP, July 2019): 1, https://www.whitecase.com/sites/default/files/2019-07/force-majeure-substantial-damages-even-if-you-cannot-perform.pdf

[168] "Antpool User Service Agreement," Antpool, Accessed 8 March 2020, https://v3.antpool.com/copyRight1

[169] Phil Nicolosi, "When Is A Website Disclaimer Effective?" Phil Nicolosi Law, P.C. (Blog), Accessed 9 March 2020, https://www.internetlegalattorney.com/when-is-website-disclaimer-effective/

wording indicates a ***binding arbitration***. This clause is placed as the last one in the agreement and only sets forth the arbitration procedure requirements. The average users will not realize that they *lose the rights* to sue the company in the national courts, to join a class action, to appeal. The opt-out condition is also not included in the text of the document. The user is forced to accept the agreement as it is. The same problem is viewed in this clause as it was with the disclaimer: placement of the information, additionally, the language and extent of the clause wording do not fully inform a user about lost rights.

The importance of placement and used language is shown in *Long v. Provide Commerce Inc.* case. “Where a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice”. It means that a user is not bound by the arbitration clause for the reason that he was not given proper notice that the clause existed.[170]

Also, Terms and Conditions agreements viewed as consumer contracts may be assessed by courts in general with regard to the fairness of agreement terms. There is legislation in different jurisdiction which address this issue: Council Directive 93/13/EEC on unfair terms in consumer contracts in European Union[171], Consumer Rights Act 2015[172] and Unfair Terms in Consumer Contracts Regulations 1999[173] in the UK, partially Federal Trade Commission Act and related state law in the US[174] and Civil Codes and other statutes of civil law system countries.

Such documents aim is to protect consumers from unfair behavior of professionals using standard terms. The factual setting of non-negotiated and lengthy standard terms used against consumers who typically do not read a single word of what they accept. These may lead to significant imbalance in the parties’ rights and obligations. The behavior of service providers may conflict with the abovementioned legislation and a more wide doctrine of good faith in contractual dealings[175].

[170] *Long v. Provide Commerce Inc*. B257910 (March 17, 2016), FindLaw, Accessed 9 March 2020, https://caselaw.findlaw.com/ca-court-of-appeal/1729412.html

[171] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, EUR-lex, Accessed 9 March 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0013

[172] Consumer Rights Act 2015, legislation.gov.uk, Accessed 9 March 2020, http://www.legislation.gov.uk/ukpga/2015/15/contents/enacted

[173] The Unfair Terms in Consumer Contracts Regulations 1999, legislation.gov.uk, Accessed 9 March 2020, http://www.legislation.gov.uk/uksi/1999/2083/contents/made

[174] Rebekah B. Kcehowski, “Consumer contracts Q&A: United States,” (Toronto: Thomson Reuters, 2017) https://www.jonesday.com/-/media/files/publications/2017/08/consumer-contracts-qa-united-states-thomas-reuters/files/consumer-contracts-qanda-united-states/fileattachment/consumer-contracts-qanda-united-states.pdf

[175] Rita de la Feria, Stefan Vogenauer, *Prohibition of Abuse of Law: A New General Principle of EU Law?* (Oxford : Hart Publishing, 2011), 247.

Cloud mining. *R. H. Krishnan, Y. S. Saketh, and V. T. Vaibhav* declare that “the term “**cloud mining**” is coined for carrying out mining operations, associated with various cryptocurrencies like Bitcoins, on a cloud network.”[176] It can be also defined as “an economic arrangement in which a person pays another person or entity to engage in cryptocurrency mining on their behalf and receives the transaction fees, cryptocurrency or a portion thereof that is generated from such mining efforts.”[177]

Cloud mining is highly risky because companies that provide the opportunity for such activity advertise the offer on the web do not comply with regulation requirements if they exist in a particular jurisdiction. They may locate their facilities and technologies outside the place of business which makes it harder to check whether their allegations and promises are backed up by something. Thus, the cloud mining realm is inundated with fraud and unjust enrichment.

D. J. Sandler rises the matter of cloud mining contracts being ***investment contracts***, i.e. ***security***. He analyzes the US legal frameworks that might apply to cloud mining contracts and the offerors of such agreements[178]. The Canadian province of Quebec also views the cloud mining participation as a security[179]. This approach may be adopted by other jurisdictions. If this happens than investors in the cloud mining will be offered additional remedies and companies will have to comply with state regulations on that matter.

D. J. Sandler draws an analogy between cloud mining arrangements and investment contracts using *the Howey test* that has become a legal standard and was described in the *SEC v. W. J. Howey Co. case* by the Supreme Court. “***A contract constitutes an investment contract*** that meets the definition of security if there is:

1. an investment of money;
2. in a common enterprise;
3. with an expectation of profits;

[176] Hari Krishnan, Sai Saketh Y. Venkata Tej Vaibhav M., “Cryptocurrency Mining – Transition to Cloud,” *International Journal of Advanced Computer Science and Applications* 6, 9 (2015): 121, https://thesai.org/Downloads/Volume6No9/Paper_15-Cryptocurrency_Mining_Transition_to_Cloud.pdf

[177] Hari Krishnan et al., Cryptocurrency Mining – Transition to Cloud, International Journal of Advanced Computer Science and Applications 6, 9 (2015): 115, cited from Darren J. Sandler,” Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?” Santa Clara High Technology Law Journal 34, 3 (2018): 252, https://digitalcommons.law.scu.edu/chtlj/vol34/iss3/1

[178] Darren J. Sandler,” Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?” *Santa Clara High Technology Law Journal* 34, 3 (2018), https://digitalcommons.law.scu.edu/chtlj/vol34/iss3/1

[179] Lubomir Tassev, “In the Daily: Liberstad Coin, Mining Contracts, Luxembourg Law”, Bitcoin.com, Accessed 9 March 2020, https://news.bitcoin.com/in-the-daily-liberstad-coin-mining-contracts-luxembourg-law/

4. derived solely from the efforts of others (e.g., a promoter or third party), "regardless of whether the shares in the enterprise are evidenced by formal certificates or by nominal interest in the physical assets used by the enterprise."[180]

In the *Howey case* W. J. Howey Co. and Howey-in-the-Hills Service, Inc. offered land sales contracts. The lend was designated for the citrus orchard. Under the contract, buyers purchased land under a uniform price per acre or fraction thereof and they had to sign "a service contract, after having been told that it was not feasible to invest in a grove unless service arrangements were made, and the superiority of Howey-in-the-Hills Service, Inc. was stressed for this purpose". The court found that buyers could not access the land and make agriculture business by themselves due to the small size of parcels (narrow strips that were one tree wide), they fully rely on Howey-in-the-Hills Service, Inc. and were entitled to receive a portion of the profit made from agricultural business led by the company. Therefore, the Supreme Court established that defendants offered something other than a land sales contracts in conjunction with management services:

> *They are offering an opportunity to contribute money and to share in the profits of a large citrus fruit enterprise managed and partly owned by respondents. They are offering this opportunity to persons who reside in distant localities and who lack the equipment and experience requisite to the cultivation, harvesting, and marketing of the citrus products Such persons have no desire to occupy the land, or to develop it themselves; they are attracted solely by the prospects of a return on their investment*[181]*.*

In the end, the Supreme Court concluded that investment contracts language used by a company cannot hide contracts' real nature[182].

Thus, *D. J. Sandler* compares the features of cloud mining contracts with respect to each point of the Howey test and concludes that such contracts may be found investment contracts by the courts in the US. This status, however, mostly depends on two main factors: an appraisal of whether the common enterprise exists (different circuit courts in the US have a different approach to this matter) and whether a mining company engages in PoW or PoS mining.

Defining cloud mining contracts as being securities has substantial consequences for investees and investors. States adopt securities acts which are a "measure designed to provide

[180] Sec. & Exch. Comm'n v. W.J. Howey Co., 328 U.S. 293, 298-99 (1947) cited from Darren J. Sandler," Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?" *Santa Clara High Technology Law Journal* 34, 3 (2018): 269, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1628&context=chtlj

[181] Ibid, 270.

[182] Ibid.

enhanced disclosure to investors, either directly or through the specific and general deterrent effects of civil, criminal, and administrative remedies". Not only these acts require the registration of securities that are offered privately, but they also provide civil remedies for fraud. They also lower the requirements for recovery, e.g. strict liability for misrepresentations and omissions in registration statements, imposing liability for negligence, and shift the burden of proof on that issue to the defendant, etc.[183] Although cloud mining contracts create contractual relations between investors and investees, the status of securities gives rise to civil remedies available for investors which are based on the law of torts.

2.1.2. Crypto exchanges, P2P decentralized trading platforms, and online crypto wallets

All the abovementioned information regarding consumer contracts applies to user agreements displayed on cryptocurrency exchange platforms' websites. However, state supervision regarding crypto exchanges is more developed, compared to those that exist regarding mining pools. There is a growing tendency amongst crypto exchanges to accept liability for hacking. According to the report of Yonhap News Agency, the Fair Trade Commission (hereinafter the FTC) stated that 5 Korean crypto exchanges modified the terms of service and now can be liable for damages caused by cyberattacks or system malfunctions regardless of negligence occurrence. This happened after crypto exchanges had received a corrective recommendation from the FTC in April 2018[184]. Moreover, such exchanges became a target for the security audit by state authorities[185]. Due to these facts, cryptocurrency exchanges do not use a force majeure clause or disclaimers as mining pools operators do to avoid liability. To illustrate, one of the biggest crypto exchanges on the Korean market, which fell victim to hacking, has already announced that aggrieved users will receive their lost money. Additionally, it adopted disaster recovery procedures that are absent in mining pools companies[186].

Technological development allows for decreasing human involvement in many processes. It triggered the growth of *algorithmic trading*[187] that is now implemented by many

[183] James D. Gordon, "Defining a Common Enterprise in Investment Contracts" Ohio State Law Journal 72, 1 (2011): 63, https://kb.osu.edu/bitstream/handle/1811/71438/OSLJ_V72N1_0059.pdf

[184] "Cryptocurrency exchanges change their terms of service: FTC", Yonhap News Agency, Accessed 9 March 2020, https://en.yna.co.kr/view/AEN20190617005300320?section=search

[185] Jason Chan, "S. Korean cryptocurrency exchanges take responsibility for losses from hacks," Asia Crypto Today, Accessed 9 March 2020, https://www.asiacryptotoday.com/s-korean-cryptocurrency-exchanges-take-responsibility-for-losses-from-hacks

[186] Elizabeth Jamie, "No Worries: Bithumb will Reimburse Lost Money of Users," BTCNN.com, Accessed 9 March 2020, https://www.btcnn.com/no-worries-bithumb-will-reimburse-lost-money-of-users/

[187] ***Algorithmic trading*** is a process for executing orders utilizing automated and pre-programmed trading instructions to account for variables such as price, timing, and volume. An algorithm is a set of directions for solving a problem.

exchange platforms. The fact that the process is automated raises an interesting question: *does technical glitch in the software allows for departure from conditions laid down in a contract and exempt a breaching party form contractual liability*?

One of the first cases addressing this issue became *B2C2 Ltd v Quoine Pte Ltd*, a decision of *S. Thorley* – the Singapore International Commercial Court judge. In this case, contractual principles and trust law were applied to cryptocurrency trading.

The action was brought to the court by B2C2 Ltd, an electronic market maker company registered in England and Wales, regarding breach of a contract and breach of trust by Quoine, a Singapore-registered company that operates a currency exchange platform. The claim arose out of transactions that happened on the Quoine's platform on 19 April 2017 when B2C2 placed orders to sell Ethereum in exchange for Bitcoin. Due to the incorrect behavior of the Quoine's software, the abovementioned trades were executed at a rate approximately 250 times the Ethereum and Bitcoin market exchange rate, in favor of B2C2's trades. Those transactions were executed by computer programs with no human involvement. When the Quoine's CTO noticed the abnormal exchange rate he realized the error and reversed debit and credit transactions in question.[188]

In this prominent case ***four important facts*** were established by the judge:

1. Unilateral reversal of transactions is a *breach of the contract* regardless of the *technical glitch* that caused the abnormal exchange rate at which those transactions were executed.

2. How a company presents updated or new terms to the existing agreement or uploads a completely new agreement matters when the existing contract enables the company to do so without prior notice to the counterparties.

3. Where transactions are executed by computer programs without any human involvement *the knowledge and intention of the program creator or a qualified programmer, not an average prudent man,* is taken into consideration.

4. Holding a cryptocurrency by crypto exchanges or any other crypto platform *may constitute a trust*.

The Quoine's Terms and Conditions (hereinafter the Agreement) contained an express term: "once an order is filled, you are notified via the Platform and such an action is

Computer algorithms send small portions of the full order to the market over time. Cited from James Chen, "Algorithmic Trading," Investopedia, Accessed 10 March 2020, https://www.investopedia.com/terms/a/algorithmictrading.asp

[188] "B2C2 Ltd v. Quoine Pte Ltd.," SGHC(I) 03 (2019): 1-2, 27-28 https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/b2c2-ltd-v-quoine-pte-ltd_a1cd5e6e-288e-44ce-b91d-7b273541b86a_8de9f2e2-478e-46aa-b48f-de469e5390e7.pdf

irreversible."[189] The Quine than stated that it was entitled to reverse the transactions due to the following allegations:

1. The agreement contained *implied terms* that allowed for such action, specifically:
   I. "Quoine may reverse any trades which are executed at an abnormal rate or price as a result of any technical and/or system failure and/or an error affecting the Platform"[190];
   II. "Quoine may reverse any trades resulting from orders placed in breach of the terms of the 2014 Terms & Conditions, including any trades resulting from any orders which amounted to market manipulation and/or abuse and, therefore, an "unauthorized use" of the Platform."[191]
2. Risk Disclosure Statement was posted by Quoine on 22 March 2017. The defendant claimed that this *Statement is considered as a part of the Agreement*. Information in the uploaded document expressly allowed the company to reverse the transactions.
3. The reversal of the transaction was lawful because the *contracts* between B2C2 and the Counterparties were *void* based on *unilateral mistake doctrine at common law* and *in equity*.
4. The reversal of the transaction was just due to mutual mistake.

On the first defense statement the judge commented that implied terms are designed to fill the gaps in an agreement and could not contradict an express clause, however, the Agreement does not have gaps or ambiguity regarding irreversibility of an order or a transaction and implied terms do contradict the express term of the Agreement[192].

On the second defense statement, S. Thorley said that the Agreement allowed Quoine to alter the Agreement's content at any time without prior notice of the user and unilateral amendments are not unlawful per se but how the users' attention is drawn to the modification of terms plays an important role. Also, the party who amends the terms should give understanding to the other party that the posted document has a contractual effect and should be read in conjunction with the Agreement. Quoine failed to properly draw users' attention to the contract's changes and to identify that the uploaded document is a part of the existing Agreement. For these reasons, Risk Disclosure Statement should not serve to amend the Agreement and the defendant was not entitled to reverse transactions[193].

[189] Ibid, 112.
[190] Ibid, 57.
[191] Ibid, 58-57.
[192] Ibid, 58-62.
[193] Ibid, 62-75.

The third statement was the most complicated for the court because to render a contract void due to the unilateral mistake two conditions should be met:

1. the mistake regarding the term (or terms) of the contract should be significant. If mistaken party realized the real nature of the term, he might not enter into contractual relations in question at all;
2. the party who wants to enforce the contract should be aware of that mistake.

The difficulty is *threefold*: how does one gain knowledge of the mistake or express an intention when transactions in question were executed by computer programs; what mistake would be fundamental and what the time of its occurrence; whose knowledge should be assessed and taken into consideration (the average man or a professional)?[194]

To establish whether there was a mistake S. Thorley analyzes several related cases such as *Hartog v Colin & Shields [1939] 3 All ER and Chwee Kin Keong and others v Digilandmall.com Pte Ltd [2005] 1 SLR(R)*. After analysis, he takes into consideration the level of human involvement when the conclusion of the contract took place and where computers were used. He also distinguishes the actual knowledge and constructive knowledge. The latter means that a party should know about the mistake and the element of impropriety is present on his part, hence, it justifies a *unilateral mistake in equity*. The former indicates that a party knew for sure that mistake occurred and this is a sufficient reason to establish a mistake at common law[195].

Answering the question mentioned above the judge decided that:

> "*the relevant mistake must be a mistake by the person on whose behalf the computer placed the order in question as to the terms on which the computer was programmed to form a Trading contract in relation to that order. This mistake will have to be in existence at the date of the contract in question but may have been formed at an earlier date. The existence of a relevant mistake will be a question of fact in each case.*"[196]

The judge also concluded that the person's knowledge or intention of which should be taken into consideration is an operator or controller of the machine. It is a person who caused a machine or a program to work in the way it did and not the person who switched it on[197].

[194] Ibid, 86.
[195] Ibid, 75-85, 99-100.
[196] Ibid, 87-88.
[197] Ibid, 89.

The mistake regarding prices indeed happened on the part of B2C2 counterparties, however, the programmer of B2C2 software did not know about the misconception that happened, therefore, the defense statement regarding *unilateral mistake at common law failed.*[198]

Regarding the unilateral mistake in equity, it is necessary to prove that the non-mistaken party, although did not possess actual knowledge, was acting irrationally by concluding the contract and should have been aware of the mistake of another party. Also, the element of impropriety should be established. The judge found that constructive knowledge did take place, the impropriety was absent: mere opportunistic behavior of business entities does not count as unconscionable conduct or sharp practice. Defense statement regarding the *unilateral mistake in equity failed*[199].

The *mutual mistake* was also denied because the party had constructive knowledge of the mistake [200].

Regarding the *trust relationships* the court established that those indeed existed between B2C2 and Quoine for the following reasons:

- The court and parties considered virtual currency as a property that may be held on trust (***certainty of subject matter***)[201].
- Quoine owns, controls, and manages a single cryptocurrency cold wallet where it keeps funds deposited by all traders. Quoine's counterparties assets are managed separately from Quoine's assets. Therefore, "beneficiaries are identifiable from the individual accounts of each of the Members" (***certainty of objects***)[202].
- The expressed words are not required for the creation of a trust. It is sufficient to determine the conduct of supposed grantor, the language used in the documents related to legal relations between parties, and relevant circumstances to determine the ***intention to establish a trust***. The clear evidence that Quoine was determined to hold the assets on trust for the individual member is that it "claimed no title to those assets and acknowledges that it is holding them" separately from its assets "to the order of the Member who can demand withdrawal at any time."[203]

The judge demonstrated that the trust was established. Taken together with a breach of the contract by Quoine and the fact that it was not entitled to reverse the transactions, the reversal in question constitutes the breach of Quoine fiduciary duty and ***the breach of trust***.

[198] Ibid, 95, 99.

[199] Ibid, 99-101.

[200] Ibid, 101-102.

[201] Ibid, 56-57.

[202] Ibid.

[203] Ibid, 57-58.

Although, civil law countries are strangers to the notion of trust as well as a unilateral mistake at common law and in equity, somewhat similar rules on voidable contracts, concluded as a result of defects in contracting process, exist in civil law jurisdictions. Civil law recognizes the free will of contracting parties. If the will is defected it may lead to rendering a contract void, i.e. not enforceable due to the provisions of the law or recognizing a contract voidable giving a possibility to parties to avoid the contract. The range of errors is set out in national Civil Codes and is usually limited to an *error in negotio*, *error in persona, error in corpore, and error in substantia*.[204] Not only national legislation establishes such errors but also some regional documents, e.g. articles 4.103 – 4.104 of the PECL[205] address this issue. Therefore, although *B2C2 Ltd v Quoine Pte Ltd* case was heard in Singapore, common law country, it should be taken into consideration by judges in civil law jurisdictions as well when the dispute concerns transactions with cryptocurrency executed without human involvement.

Inasmuch as software that facilitates cryptocurrencies is governed by the rules of programming, it executes transactions with no direct influence of people, and is mostly open-source, meaning that a lot of engineers contribute to its development, the reasoning of the judge in *B2C2 v. Quoine* becomes extremely valuable for disputes related to cryptocurrency:

- transactions in the blockchain are irreversible by design and if someone implemented a reversal he might be in a breach of a contract or be liable in tort for bringing damages to the third parties. There was an incident at the beginning of Bitcoin history when a transaction was canceled when a developer noticed a bug in the system in August 2010. It was not the reversal of transaction per se: developers just wrote a patch that would fix the bug and went back in transaction history so it looked like the transaction has never happened[206]. Although the Bitcoin community was relatively small back then and the problem was solved quickly, this episode shows that programming manipulation applied to transactions in a blockchain may rise possible liability issues in the future;
- there are people behind the software who could be liable for the way they designed the program;
- companies may be accountable for the bugs in their programs; persons who hold cryptocurrencies may be recognized as settlors.

[204] Basil S. Markesinis, Hannes Unberath, and Angus Johnston, *The German Law of Contract: A Comparative Treatise* (Oxford: Hart Publishing, 2006), 276-277.

[205] Klaus Peter Berger, "The Lex Mercatoria (Old and New) and the TransLex-Principles," Trans-Lex, Accessed 14 March 2020, https://www.trans-lex.org/400200

[206] Kai Sedgwick, "Bitcoin History Part 10: The 184 Billion BTC Bug," Bitcoin.com, Accessed 14 March 2020, https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/

2.1.3. Cryptocurrency users

F. Boehm and *P. Pesch* tried to analyze the *Bitcoin nature* and *characteristics of contracts with the use of Bitcoin* under German and US law. However, they did fail at finding a place of Bitcoin in the legal classification of objects described in the German Civil Code (hereinafter the BGB) which is pretty similar to the ones that exist in Civil Codes of civil jurisdiction countries: authors neither view the cryptocurrency as a physical object nor claim or immaterial good[207].

They tried to explore the nature of contracts involving Bitcoin. Authors do not deny the fact that such contracts are binding in the eyes of the law. However, they disagree that purchase of good with Bitcoin constitute a ***contract of sale*** due to the wording of the BGB which defines such agreement "as a contract that includes the duty to transfer the ownership of a movable thing in exchange for *monetary* payment." The concern in question is that contracts of sale require a transfer of monetary value and authors, in turn, deny the notion of cryptocurrency being money and add that nobody is obliged to take Bitcoin as payment.[208] We disagree with this statement due to the reasons described in Chapter 1, cryptocurrency should be treated as currency and the legal rules that govern currency transactions should apply. Therefore, the purchase of goods with cryptocurrency should constitute a sales contract.

In the authors' opinion, when someone buys Bitcoin with fiat money, it is not a contract of sale either. The given justification is that Bitcoin is not a movable physical thing. They claim that such an agreement could be regarded as a contract of sale if Bitcoin were a right but a cryptocurrency is not a right either. These contracts are also not barter agreements because such contracts are performed without the involvement of money[209]. Authors then refer to the *Kaplanov's* work and propose that such transactions could be named as "atypical work and service contracts". This definition, though, is not applicable in cases when Bitcoin is used to buy goods or services[210]. We partly agree with this explanation (such contracts are not a contract of sale or barter), although, it should be noted that the authors' overall reasoning is narrow due to the following reasons:

1. The BGB indeed recognizes only corporeal objects as things (section 90)[211]. However, this document is archaic. It was ratified in 1896 and formally took effect

[207] Franziska Boehm and Paulina Pesch, "Bitcoin: A First Legal Analysis – with reference to German and US-American law" *Financial Cryptography Workshops* (2014): 7-8, https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf

[208] Ibid, 8

[209] Ibid, 8-9

[210] Ibid, 9.

[211] German Civil Code, Bundesministerium der Justiz und für Verbraucherschutz, Accessed 14 March 2020, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html

on January 1, 1900[212]. The original statute of 1896 already contained the classification of things that remained as it was to this day[213]. There was no e-money or other digital assets back then, therefore, obviously outdated classification cannot cover such innovations. E-money has digital representation and it is an incorporeal substance, consequently, following the letter of law, e-money is not a thing. On the other hand, cash and coins are tangible and fall under the classification of things. Because both e-money and bills (coins) are the same things in different clothing, ***intangibles***, i.e. e-money as well as cryptocurrencies, should also be recognized as ***things***.

2. Section 91 of the BGB has a notion of ***fungible things***[214]. "The thing is fungible when an obligation in connection with it can be discharged or performed by the substitution of an equal number, or weight, or measure, or units of the same class"[215]. Money could be considered as the most fungible things.[216] Although F. Boehm and P. Pesch did not identify a place of the cryptocurrency in the classification, cryptocurrencies should be defined *as intangible, movable, fungible things*.

3. The abovementioned contracts ***are not work and service contracts***. The essence of a contract of work is an obligation to deliver the result of accomplished work specified in the contract. The other instance when these agreements are referred to is employment law. The services part means that a counterparty, in addition to work, provides supplementary services. Such contracts usually require professional knowledge. In cases when Bitcoin is bought with money, there is no work involved and no result to hand out, special knowledge is not required, the nature of services in question is doubtful as well because transactions are almost instant and are made through computer software, not by human per se. There is only a mutual transaction of money.

4. The authors were right that the abovementioned contracts are not contracts of sales or barter, they, however, failed to establish clearly what type of contracts

[212] Nicole Sotelo, "German Civil Code (Bürgerliches Gesetzbuch, BGB) (1900)," Towards Emancipation? Accessed 14 March 2020, http://hist259.web.unc.edu/german-civil-code-burgerliches-gesetzbuch-bgb-1900/

[213] Bürgerliches Gesetzbuch (Vom 18. August 1896), Prof. Dr. Gerhard Köbler (Person Publikationen Projekte), Accessed 14 March 2020, http://www.koeblergerhard.de/Fontes/BGB/BGB1896_RGBl_S.195.htm

[214] German Civil Code, Bundesministerium der Justiz und für Verbraucherschutz, Accessed 14 March 2020, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html

[215] Arnott v. Kansas Pac. Ry. Co., 19 Kan. 95 cited from William Livesey Burdick, *The Principles of Roman Law and Their Relation to Modern Law* (Clark, New Jersey: The Lawbook Exchange, Ltd., 2012), 318.

[216] Ernest Joseph Schuster, *The Principles of German Civil Law* (Oxford: Clarendon Press, 1907), 61.

those are. Through our analysis, we can affirm with certainty that such agreements are ***currency exchange contracts***.

The authors also enumerate some *civil liability problems* that exist in the crypto sphere and address these issues to other researches to be conducted in the future. In particular, they ask who would be liable in case of ***data loss*** or ***data misuse***[217]. First of all, those problems are not crypto-specific, they exist within all entities that use technologies. There are particular regional frameworks such as the GDPR and national statutes, e.g. Data Protection Act in the UK which are designed to protect user data. Such documents indicate liable persons for data incidents. Secondly, authors disregarded the technology behind cryptocurrencies – blockchain – information cannot be lost because data about transactions broadcasted to every node in the network.

They also raise a question about ***enforceability of claims***: the main concern is irreversible transactions. In case of a mistake, there is no central authority who can reverse a transaction[218]. It is true, however, this should not be an obstacle for involved parties and law. The reason why will be covered within the smart contracts subchapter.

Currency choice in contracts

The ***freedom of contract*** principle allows parties to determine preferable terms that will regulate their relationships, therefore, they can establish the currency of the contract.

National legislation may allow paying with foreign currency if the ***contract*** is concluded ***between residents***. For example, the *BGB section 244 (1)* states that "if a money debt stated in a currency other than the euro is payable within the country, then payment may be made in euros unless payment in the other currency has been expressly agreed."[219] After the civil reform in 2018, the *French Civil Code* allows for payments in other than euro currency in special circumstances: if payment "is performed between professionals and when the use of a foreign currency is commonly accepted for the transaction in question."[220] The *Civil Code of Ukraine* states that "obligation shall be expressed in the currency of Ukraine – hryvnia. The parties may determine a monetary equivalent of obligation in the foreign currency"[221]. The monetary equivalent of

[217] Franziska Boehm and Paulina Pesch, "Bitcoin: A First Legal Analysis – with reference to German and US-American law" *Financial Cryptography Workshops* (2014): 9, https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf

[218] Ibid.

[219] German Civil Code, Bundesministerium der Justiz und für Verbraucherschutz, Accessed 14 March 2020, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html

[220] Anaëlle Idjeri, "Reform of French contract law – Ratification Law published on April 21, 2018: Main changes impacting business law," Soulier Avocats, Accessed 14 March 2020, https://www.soulier-avocats.com/en/reform-of-french-contract-law-ratification-law-published-on-april-21-2018-main-changes-impacting-business-law/

[221] Цивільний кодекс України, в редакції від 13.02.2020, Законодавство України, Accessed 14 March 2020 https://zakon.rada.gov.ua/laws/show/435-15

obligation is not the same as payment with foreign currency and according to article 533 of Civil Code monetary obligations shall be fulfilled in hryvnia. Thus, contractual freedom of contracting parties may be restricted in some jurisdictions and the language of civil legislation should be taken into account. Also, statutes usually use the term "foreign currency", meaning the legal tender of another country, while cryptocurrency is not a legal tender of any country. One should bear in mind that the wording of legislation analogous to the Ukrainian Civil Code does not prevent an obligor from paying in other currency, instead, it allows a creditor to refuse payment made with a currency other than the national one. The obligor cannot claim any remedies in national courts basing it on the fact that the creditor did not accept the performance of the obligation in foreign currency or cryptocurrency.

The rules for ***international contracts*** are different: parties may choose the law which governs the contract as well as the preferred currency. If parties did not provide invoice currency in the contract they may refer to the rules of ***lex mercatoria*** to govern their relations, e.g. such transnational rules may be found in the UPICC [222] or the "*Creeping Codification*" codified through the *TransLex Principles*.[223]

The fact that cryptocurrency is money leads to the application of a variety of international instruments which *regulate* ***international contractual relations***. One example is the CISG. Its rules are applied when goods are purchased with cryptocurrency. *M. Király* explores how the CISG may govern such contractual relationships.

The ***payment issue*** is of particular interest due to Bitcoin and other cryptocurrencies volatility.

According to article 14 of the CISG, "a proposal is sufficiently definite if it indicates the goods and expressly or implicitly fixes or makes provision for determining the quantity and the price."[224] Parties do not need to establish the fixed price for goods as well as goods quantity to conclude the contract. M. Király suggests that parties may protect themselves from the cryptocurrency fluctuation if they avoid fixing the price in the contract[225]. If they do so – do not establish the price in any way, explicitly or implicitly, – it means that parties impliedly referred "to the price generally charged at the time of the conclusion of the contract for such goods sold

[222] *UNIDROIT International Institute for the Unification of Private Law* (Rome: International Institute for the Unification of Private Law, 2016) https://www.unidroit.org/english/principles/contracts/principles2016/principles2016-e.pdf

[223] Klaus Peter Berger, "The Lex Mercatoria (Old and New) and the TransLex-Principles," Trans-Lex, Accessed 14 March 2020, https://www.trans-lex.org/the-lex-mercatoria-and-the-translex-principles_ID8

[224] *United Nations Convention on Contracts for the International Sale of Goods* (New York: United Nations, 2010), 5, https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

[225] Miklós Király, "The Vienna Convention on International Sales of Goods and the Bitcoin," *US-Chine Law Review* 16, 5 (2019): 181, https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf

under comparable circumstances in the trade concerned" under the article 55.[226] It binds the price measurement to the time of contract conclusion and this fact can worsen parties' position because the Bitcoin price can change significantly till the time of contract performance. The author then proposes to an adopt open price approach taken in the US Commercial Code:[227] "the price is a reasonable price at the time for delivery."[228]

Another urgently important question is whether cryptocurrency price vacillation justifies applying the ***change of circumstances*** consequences. Concepts of hardship and frustration deal with the change of circumstances. According to Art. 6.2.2 of the UPICC[229] the *hardship* is "a situation where the occurrence of events fundamentally alters the equilibrium of the contract." ***Four criteria*** should be met to establish hardship: an event happens after the contract conclusion; a disadvantaged party did not foresee an event in the moment of conclusion; an event "beyond the control of the disadvantaged party"; the disadvantaged party did not assume the risk of such event. The hardship shift the balance of interest in the contract that had existed before the change of circumstances – the cost of performance increased or the value of performance decreased significantly. A hardship entitles a party to initiate renegotiation of terms with the counterparty, altering or terminating the contract by the court (Art. 6.2.2, 6.2.3).[230] Parties cannot rely on the change of circumstances in most cases because the second and fourth requirements would not be met – contracts involving cryptocurrency are risky, the high volatility is a known fact for cryptocurrency holders[231].

Taken that governments have different approaches to cryptocurrency regulation, application of ***force majeure*** clause should be taken into account. For example, the explicit ban of cryptocurrency in a particular jurisdiction would excuse a buyer from payment in contractually chosen cryptocurrency.

M. Király argues that since cryptocurrency is not a legal tender in any country, it does not have an official ***base rate for the late payment interest*** evaluation. Thus, a contracting party should take advantage of the freedom of contract principle and include the clauses aiming to resolve this

[226] *United Nations Convention on Contracts for the International Sale of Goods* (New York: United Nations, 2010), 17, https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

[227] Miklós Király, "The Vienna Convention on International Sales of Goods and the Bitcoin," *US-Chine Law Review* 16, 5 (2019): 182, https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf

[228] The US Commercial Code § 2305 (1) cited from Miklós Király, "The Vienna Convention on International Sales of Goods and the Bitcoin," *US-Chine Law Review* 16, 5 (2019): 182, https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf

[229]*UNIDROIT International Institute for the Unification of Private Law* (Rome: International Institute for the Unification of Private Law, 2016), 218, https://www.unidroit.org/english/principles/contracts/principles2016/principles2016-e.pdf

[230] Ibid, 218-219, 223.

[231] Miklós Király, "The Vienna Convention on International Sales of Goods and the Bitcoin," *US-Chine Law Review* 16, 5 (2019): 182, https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf

issue. Failing to do so, parties should rely on the court decision which will establish an applicable base rate. The author mentioned then that the cryptocurrency volatility may lead to the following consequence: the amount of the late payment interest may not be sufficient to make up for the Bitcoin's loss in value when it rapidly decreases comparing to the exchange rate of national currencies[232].

Even though cryptocurrency payment has its issues, negotiable (contracts), national and international instruments provide a sufficient amount of tools designated to elevate parties' concerns. The CISG provides ***contractual remedies*** available for the parties in case of a fundamental breach of a contract:

- *a* ***buyer can exercise rights*** to require specific performance[233], award an additional time for sellers' performance[234], accept performance of the seller who executes his right to cure[235] [236], avoid the contract[237], reduce the price when goods do not conform with the contract[238], refuse to accept performance in case the seller delivers exceeded amount of goods or deliver them before the fixed date[239], claim damages[240] and others not mentioned in the Convention;
- *a* ***seller is entitled to*** the same remedies as a buyer is, combined with the right to cure his non-performance[241] and a right to make a specification of the goods if it is not presented by the buyer in the due time,[242] etc.

2.2. Smart Contracts

2.2.1. Definition of smart contracts

Blockchain technology brought disrupting changes into the financial system and offered an alternative approach for payment management. LegalTech and contract law are going through

[232] Ibid, 187.

[233] *United Nations Convention on Contracts for the International Sale of Goods* (New York: United Nations, 2010), 13-14, https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

[234] Ibid, 14.

[235] Ibid.

[236] Jonathan Yovel, "Comparison between provisions of the CISG (Seller's Right to Remedy Failure to Perform: Article 48) and the counterpart provisions of the PECL (Articles 8:104 and 9:303)" (March 2005), Accessed 15 March 2020 http://cisgw3.law.pace.edu/cisg/text/peclcomp48.html

[237] *United Nations Convention on Contracts for the International Sale of Goods* (New York: United Nations, 2010), 14, https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf

[238] Ibid, 16.

[239] Ibid.

[240] Ibid, 13-14, 23-24 (Articles 45, 74, and 77).

[241] Ibid, 14-15.

[242] Ibid, 20.

some changes as well. The concept of smart contracts was born after the ubiquitous usage of cryptocurrency. Implementation and performance of smart contracts require not only the involvement of lawyers but also coders. Everyone is used to the fact that lawyers draft agreements, creation of smart contracts (hereinafter the SC) is different. A lawyer can still be involved in the drafting process although he can only explain essential features of an agreement that will be relevant for the desired outcome when a coder gets his hands on the contract. Nowadays, the most popular platform that facilitates smart contracting is Ethereum.

An American computer scientist *N. Szabo* has played a pioneering role in developing the idea of SCs. He described the idea that software and hardware are able to execute contracts in 1994[243] and elaborated on this matter in the following works. He stressed that "the contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts [...] Smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process."[244] The researcher has written his work before the proliferation of the DLT however specifically the DLT kindled utilization of SCs.

There are many competing conceptions of what a SC is. Those from a computer science background often use the term in a quite different way to lawyers. For lawyers, the term 'contract' connotes a very particular legal relationship of obligations, whereas computer scientists tend to think of SCs more in terms of code[245].

Reflecting this different usage, J. Stark presents two distinct schools of SCs:

- *Smart legal contracts*: This school resonates most with lawyers. This is where the term SC is used to refer to legal contracts, or elements of legal contracts, being represented and executed by software.
- *Smart contract code*: The other school relates less to contracts as a lawyer would understand them, and more to a piece of code (known as a software agent) that is designed to execute certain tasks if pre-defined conditions are met. Such tasks are often embedded within, and performed on, a distributed ledger[246].

Clack, Bakshi, and Braine define smart contracts as follows: "A **smart contract** is an automatable and enforceable agreement. Automatable by computer, although some parts may

[243] Nick Szabo, "Smart Contracts" (1994), Accessed 15 March 2020 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[244] Nick Szabo, "Formalizing and Securing Relationships on Public Networks," Satoshi Nakamoto Institute, Accessed 18 March 2020, https://nakamotoinstitute.org/formalizing-securing-relationships/

[245] Stark, J. "Making sense of blockchain smart contracts" (2016), http://www.coindesk/com/making-sense-smart-contracts cited from "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective" (New York: International Swaps and Derivatives Association, 2017): 4, https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

[246] Ibid, 4-5.

require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code". The authors point out that this definition is designed to cover both concepts mentioned above[247].

2.2.2. Form

Freedom of contract allows parties to choose the form of the contract: written, electronic, or oral. Depending on the jurisdiction, the electronic form may be considered as a subtype of a written form or as a completely independent one. National legislation may require compliance with rules establishing the form of some contracts, e.g. transfer of real property, in most cases, should be embedded in a written contract and, depending on the jurisdiction, require a notarial assurance.

According to N. Szabo, "a **smart contract** is a computerized transaction protocol that executes the terms of a contract."[248] SCs are computer programs written in a specific programming language[249]. Even though such a program is a piece of digital information, anyone can view the code of a SC because it is saved in a computer file and contains real words specific to a programming language. Any program goes through a compilation phase where verbose code is transformed into a binary representation (just zeros and ones) understandable by a computer. However, the original code is still available for a professional to read and this person can identify the purpose of each code line. Therefore, in our opinion, a form of SCs should be recognized as a ***type of written form***.

2.2.3. Contracts formation and their content

Depending on the law system and national legislation, the law would require several conditions to be satisfied. For a contract to have binding nature in *common law system,* the following elements should be present: an offer, an acceptance, an intention to create legal relations, the certainty of terms, and a consideration[250]. In *continental legal* system, consideration is irrelevant for contract formation.

[247] Clack, C., Bakshi, V. & Braine, L. "Smart Contract Templates: foundations, design landscape and research directions" (2016, revised March 2017) cited from "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective" (New York: International Swaps and Derivatives Association, 2017): 5, https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

[248] Nick Szabo, "Smart Contracts" (1994), Accessed 15 March 2020 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[249] Wei-Meng Lee, *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript* (New York: Apress, 2019), 129.

[250] Mindy Chen-Wishart, *Contract law* (Oxford: Oxford University Press, 2018), 41.

There is a legal discussion about the binding nature of a SC. It is viewed that a SC may be not a legal contract because not all elements are present for a contract to have a binding nature. The code is written however it does not pose any obligations on potential contracting parties – there is no ***offer*** and ***acceptance***, no ***consideration***[251]. It is important to remember that the perception of smart contract code should be similar to the stack of paper on which contractual clauses are written. If one party does not pass this paper to another there would be no offer and, therefore, acceptance. The same is true about SCs: a party willing to contract would need to let the other party know that there is a SC written, and it contains certain clauses. The other party then should agree to the terms and accept the offer. Because all transactions occur on the blockchain, the offeree signs transaction with the private key – this could qualify as an acceptance. Only after those steps, the contract is concluded. In common law system, the SC code should also be designed in such a way that it would satisfy the consideration requirement.

As to the ***certainty of terms***, there may be some complications because the terms of a SC are not displayed in a conventional way. An average reasonable person cannot evaluate the programming language code. The signing of a smart contract is somewhat similar to the signing of a regular contract written in Chinese by individuals who do not speak this language. In this case, the parties should completely understand the content of a contract and the drawn implications without knowing the language in which the contract is drafted. Therefore, parties should be vigilant to ensure that the smart contract reflects their true intentions.

SC is a set of instructions written by a developer. Binary (bivalent, Boolean) logic is the basis for all programming languages and its rules influence the code execution. Programming code is a law for a computer. It will execute exactly what is determined by a coder who created the program. Every program is dependent on multiple *conditional if-else statements* and the logic of execution, in very simplistic terms, is as follows: If (A is true) – execute {this line of code}, else if (A is false) run {another line of code}.

A SCs are suitable when an "algorithmically determinable solution" is available. In other words, there is no room in a SC for discretion, reasonableness, or judgment: potential outcomes will be binary in form[252].

The logic governs the law as well. "Logic may be defined as the science of the principles and conditions of correct thinking; or, in other words, the science which directs our mental

[251] "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective" (New York: International Swaps and Derivatives Association, 2017): 5, https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

[252] Adam Sanitt, "Smart Contracts," Norton Rose Fulbright, Accessed 18 March 2020 https://www.nortonrosefulbright.com/en/knowledge/publications/1bcdc200/smart-contracts

operations in the discovery and proof of truth."[253] The if-else structure underlies the wording of legal provisions. If requirements of a provision that regulate particular legal relations are met then a party can expect the application of such rule. No wonder that law and programming have similarities because they utilize the same principles of logic. Therefore the all necessary contractual clauses are objectively determined in a computer program.

2.2.4. Performance of the contract. Liability issues

A breach of a contract may happen if a party does not properly perform a contract as stipulated in the agreement or fail to take actions needed for performance entirely. In case of a fundamental breach of a contract, a party can seek protection and be entitled to remedies. With SCs, the performance process is automated – the sole purpose of the SC code is to execute performance without human involvement. Thus, **in theory** (emphasis added), a breach should not occur as the performance is guaranteed.

To provide the requisite functionality needed by contract practice, the SC system needs to be able to interact with the outside world, otherwise, it could only operate with conditional payments and signals of the users. The SC environment needs to allow SC to send signals to external entities or objects, such as computers or robots, whereby the SC can operate in the real world without human intervention, e.g. a hotel room that unlocks once you make the payment for the room[254].

The facility to receive inputs has been christened '***oracles'***. An 'oracle' is the entity or communication channel by which the SCs system receives information about the external world. Professor *E. T. Tjing Tai* distinguishing **three types of oracles**:

1. ***automated oracles***: a mechanism, a machine, a robot that is capable to send signals about particular events (self-driving car, input/output devices connected to the Internet);
2. ***TTP oracles***: a person, who thereby functions as a trusted third party (a courier who delivered a package). Through this oracles a SC can receive information about "a state of affairs that is fairly complex to determine";
3. ***expert oracles***: an oracle that performs an evaluative role, such as assessment of damage or quality of delivered goods (surveyor, certification agency, conformity assessment body). Although at this time only a human being can perform such a

[253] Nicholas F. Lucas, "Logic and Law" *Marquette Law Review* 3, 4 (1919): 203, https://pdfs.semanticscholar.org/f5dd/674b7aadffbfc05b18fafc89a1373df4cc0c.pdf

[254] Eric Tjong Tjing Tai, "Force Majeure and Excuses in Smart Contracts" *European Review of Private Law* 6, 26 (2018): 3, https://pure.uvt.nl/ws/portalfiles/portal/28903834/Smart_contracts_excuses_ERPL_1_postprint.pdf

role, the author does not rule out that an advanced algorithm can take over such power[255].

The development of technology, as well as awareness of individuals and entities about available technological solutions, are still rudimentary, therefore, the process is only fully automated in case of money transactions. Indeed, there is no need for human involvement to make a transfer from one account to another on a specific date and time when some conditions are met. However, it is only one part of the performance. The conditions for contract triggering depend on individuals' actions or omissions of such. When parties have entered into a contract for the sales of goods in which payment usually goes upfront and such payment is performed with help of the SC, thus, the buyer complied with the contractual terms. The seller though did not deliver goods in time. In this case, the SC should contain relevant conditional statements that will be triggered when any predictable breach occurs. But when the contract is silent regarding arising issues, the aggrieved party is entitled to corresponding remedies and should seek protection in court. The following complications may present themselves when a party fails to perform or when a dispute is brought to court.

Excuses for non-performance, impossibility, illegality. Such excuses may be mentioned in the contract. Evaluation of these events though would require the involvement of an oracle, e.g. expert oracles and alternative dispute resolution, or online dispute resolution services. *E. T. Tjing Tai* argues that "this effectively denies most of the benefits that SCs would have, in particular by breaking the automatic execution of the contract." He also identifies and speculates on several steps to determine the cause of non-performance, deciding whether it is attributable to the debtor or creditor.

He proposes a solution to presume that a *breach is attributable to a debtor* and only allowing a limited set of foreseeable relevant causes as an excuse. The attributability test is based on the fundamental principle of modern civil law – no liability without fault, so the fault is a precondition of the debtor's liability[256]. However, modern contract law has a fairly strict regime of contractual liability,[257] thus, professor views the proposed assumption as fair. "Any remaining, unforeseen causes would simply be at the risk of the debtor." The debtor is still free to decide which risks he would not accept and include them in ***a force majeure clause***.[258] As soon as a cause of non-performance identified by automated or TTP oracles, the inevitable involvement of an

[255] Ibid.

[256] Mindy Chen-Wishart, Alexander Loke, and Burton Ong, *Remedies for breach of contract* (Oxford, New York: Oxford University Press, 2016): 112.

[257] Eric Tjong Tjing Tai, "Force Majeure and Excuses in Smart Contracts" *European Review of Private Law* 6, 26 (2018): 10, https://pure.uvt.nl/ws/portalfiles/portal/28903834/Smart_contracts_excuses_ERPL_1_postprint.pdf

[258] Ibid, 12.

arbiter follows due to multiple circumstances which requires evaluation of non-performance excuse. If force majeure indeed occurred "consequences can be programmed in a straightforward manner. Force majeure stands in the way of invoking a remedy for non-performance, as there is no breach. The creditor may, however, terminate the contract. Termination is also fairly easy to program (although it may require considerable legal acumen to correctly draft rules for everything that has to be arranged around and after termination, such as returning advance payments, valuation of partial performance)."[259]

E. T. Tjing Tai also mentions ***impossibility*** as a special kind of excuse. Determining whether the impossibility exists, whether it is permanent or temporary requires an analysis that cannot be performed by software. The same is true for ***illegality***. Professor's research is overall pessimistic and it generates thoughts that SCs can only list all the unfortunate events that could happen along the way and they still require the help of TTP or expert oracles without much involvement of automated ones. The main problem of SCs is that "contract law is not about *ex ante* regulation (which is what SCs focus on), but rather is designed for *ex post* adjudication."[260] However, the researcher remains confident that SCs have the capacity to become sufficient, convenient, and adequate tool in the future when technologies eliminate its current impediments.

Unilateral and mutual mistake. The nature of such mistakes was already mentioned in our analysis of the *B2C2 v. Quoine* case. We indicated above that certainty of terms may be an issue in SC. The improper perception of the contractual terms nature makes contracts voidable because parties could not be bound to a set of terms that they did not intend. A mistaken party (ies) may bring a case to the court that may render the contract unenforceable due the flaw in the contract.

Courts usually use a subjective and objective test to constitute whether the contract was concluded and on which terms. In the area, questions of "mistake" are often intertwined with questions of interpretation. The court not only would interpret the body of the contract but also the communication of parties that lead to the contract conclusion[261]. The form of the SC makes interpretation a demanding and complicated task. Interpretation of such contracts would require the knowledge of an expert. Also, the SCs form raises risks of pre-contractual misrepresentation or non-disclosure so unconscionable parties conclude a contract that benefits them. The focus of courts in such cases would be made on the negotiation process. The tort law may also provide a plaintiff with remedies in misrepresentation cases.

[259] Ibid, 15.

[260] CASEY & NIBLETT, 'Self-Driving Contracts', p. 24 cited from Eric Tjong Tjing Tai, "Force Majeure and Excuses in Smart Contracts" *European Review of Private Law* 6, 26 (2018): 17, https://pure.uvt.nl/ws/portalfiles/portal/28903834/Smart_contracts_excuses_ERPL_1_postprint.pdf

[261] John Cartwright, *Misrepresentation, Mistake and Non-disclosure* (London: Sweet & Maxwell, 2012), 598 – 600.

Void contracts. The irreversibility of transactions should not constitute a practical problem because another party can always make a second transaction returning the payment of another party. On the other hand, when the ***court renders contract void*** it would create a situation as the contract has never existed. One may think that irreversibility, in this case, is an obstacle because the transaction remains in the blockchain forever. In our view, it is still not an issue. Even though the transaction remains in the DL, as long as parties are able to make corresponding transactions in case of restitution, the irreversibility of original transactions should not be treated as an obstacle. After all, when a person applies for a refund, someone (either other contracting party or bank) should still make one more transaction to send money back to the applying party account.

Oracle mistake. *E. T. Tjing Tai* focuses on excuses for non-performance. But what about a situation when performance has already occurred due to an oracle mistake? *Dr. E. Mik* states that automated oracles "do not constitute infallible sources of truth and cannot guarantee that an off-chain event actually occurred. Moreover, oracles do not create or compute the required information about off-chain events themselves but obtain if from external data sources, such as websites, commercial providers (e.g. Bloomberg), prediction markets (e.g. Augur), answer engines (e.g. WolframAlpha) or other blockchains." Therefore, the blockchain that facilitates smart contracting is supposed to be decentralized, oracles, and sources from which they derive "knowledge", on the other hand, are centralized so the data can be corrupted or insufficient. She suggests several solutions for avoiding disputes between parties and eliminating inconsistencies:

- parties should choose not only oracles but also the data sources from which such oracles receive information. The perfect solution would be if a network of oracles obtained information from multiple sources then received facts would be compared and agreed on by each oracle. Oracles should agree on information to be reliable and only after that, an oracle can trigger the script of a SC[262]. Such solutions already introduced by Oraclize, ChainLink, and Augur[263].
- in cases when different sources present different data on the same event "it may be necessary for the parties to agree on the prevalence of a specific source to avoid later disputes."[264]

[262] Eliza Mik, "Smart contracts: Terminology, technical limitations and real world complexity*" Law, Innovation and Technology* 9, 2 (2017): 23, https://core.ac.uk/download/pdf/132698353.pdf

[263] Jesus Rodriguez, "The Middleman of Trust: The Oracle Paradox and Five Protocols that can Bring External Data into the…" Hackernoon, , Accessed 18 March 2020, https://hackernoon.com/the-middleman-of-trust-the-oracle-paradox-and-five-protocols-that-can-bring-external-data-into-the-df39b63e92ae

[264] Eliza Mik, "Smart contracts: Terminology, technical limitations and real world complexity*" Law, Innovation and Technology* 9, 2 (2017): 23, https://core.ac.uk/download/pdf/132698353.pdf

If parties failed to take such precautions it is highly possible that they will start a dispute resolution procedure in court. An oracle mistake would become even more dramatic when the performance of a SC was necessary for another party to perform another agreement with a different party. The restitution awarded by the court may bring considerable damages to the involved person or entity.

Code error. A "bug" in code may be a reason for a breach of a contract. This breach did not happen due to contracting parties' actions or omissions, therefore, the question arises whether the developer of a buggy SC would be liable for such an event. This situation though may give rise to tortious liability that will be discussed in the further chapter.

All information considered, smart contracts, remain limited to agreements that are not highly reliant on the off-chain events. Smart contracts should be supported by a developed infrastructure of automated oracles such as sufficient web API[265] offered by different entities and platforms, hardware oracles, e.g. sensors within physical objects, sufficient networks of oracles ensuring data efficiency, etc. in order to achieve promised advantages. Even with improved infrastructure, SCs do not completely eliminate human involvement, specifically, when a legal analysis is required to establish relevant facts, i.e. causation, double causation, occurrence of force majeure, impossibility of performance, misperception of terms by the parties, etc.

[265] An **API** is a set of programming code that enables data transmission between one software product and another. Cited from "What is API: Definition, Types, Specifications, Documentation," AltexSoft, Accessed 1 April 2020, https://www.altexsoft.com/blog/engineering/what-is-api-definition-types-specifications-documentation/

3. Non-contractual liability in cryptocurrency relations

Non-contractual liability is covered by civil law provisions and called the *law of delict* in continental legal systems, while common law countries categorize it as *tort law*. The national law of different states can vary when approaching non-contractual liability issues. Therefore, for our comparative analysis we will mostly analyze Ukrainian legislation as an example of a civil law system country, the UK and the US – as common law states. We also consider further only torts and delicts that can emerge in the cryptosphere and omit the others.

3.1. Negligence and the duty of care

3.1.1. The tort of negligence in common law

The ***tort of negligence*** is known in common law legal system. "There is a negligence liability only if the claimant can show that the tortfeasor fell short of the degree of care expected of the 'reasonable person.' Only the *lack of care* amounts to a breach of a duty owed to the claimant will give rise to liability in negligence."[266] Another important requirement for the tort of negligence is *material damages* or the claimant's *loss* caused by the behavior of the tortfeasor. Moreover, the damages need to be "*attributable to* – or not too remote from – the defendant's *breach of duty*."[267]

Existence of the duty of care. The ***duty of care*** is a very complex and abstract notion and the existence of such duty is evaluated by courts in every particular case. It is considered as everyone's responsibility to not cause damage to others through carelessness[268]. In the continental legal tradition, such responsibility embodied in general principles of civil law, e.g. the article 13 of the Civil Code of Ukraine sets boundaries of a person's enjoinment of the rights. In exercising rights, a person must refrain from any action that might violate the rights of others, a person shell act with no intent to harm others and abide by moral principles.

Several cases in common law address this issue. The very first important one is *Donoghue v. Stevenson*[269] where the broad approach is taken for duty of care evaluation: it almost corresponds to a moral principle – do not harm your neighbor. A person should take reasonable care for acts or omissions of such when a person can reasonably foresee that his behavior could

[266] Jenny Steele, *Tort Law: Text, Cases, and Materials* (Oxford: Oxford University Press, 2017), 113.

[267] Ibid, 113-114.

[268] "Duty of Care Lecture," LawTeacher.net, Accessed 1 April 2020, https://www.lawteacher.net/modules/tort-law/negligence/duty-of-care/lecture.php

[269] Donoghue v Stevenson [1932] UKHL 100 (26 May 1932), https://www.uni-trier.de/fileadmin/fb5/FFA/KURSUNTERLAGEN/Anglo-Amerikanisches_Recht/Law_of_Torts/Siry-SS-2012/Donoghue_v_Stevenson__1932__UKHL_100__26_May_1932_.pdf

bring harm to others. The potentially injured parties are usually those who can be closely and directly affected by tortfeasor's behavior and he knows it or should know[270].

The approach taken by Lord Atkins in the previous case is so broad that the modern law needed some requirements and limitations for balancing claimants' and defendants' interests. Therefore, an additional '*three-stage-test*" consisting of ***foreseeability***, ***fairness,*** and ***proximity*** criteria were set out in the *Caparo v. Dickman*[271] case.

In the case of **cryptocurrency platforms** service providers **owe the duty of care to its users** due to the following reasons:

- the ***proximity*** between a platform company and its users exists due to contractual relations between them. *Donoghue v. Stevenson* ("neighborhood test"), as well as *Anns v Merton London Borough Council*[272] case, mention the proximity as the reasonable belief that carelessness of the wrongdoer could likely cause damage to a particular person or a group of individuals or/and companies.
- actions or omission of such made by the platform staff can harm its users because the later continuously use platforms' services. Not all but a lot of negative consequences can be ***foreseen*** by the management or platform's developers;
- the criterion of **fairness** is the vaguest one, therefore, when judges decide on this issue they may show all the possible power of judicial discretion. In our opinion, it would be fair and reasonable decision to admit that duty of care exists and the platform potentially could be liable for its users' losses because the later ones do not have control over the course of business, management decisions, or platform enhancement by the platforms runners' programmers.

As to the **independent coders** that contribute to open-source software development the issue of duty of care is extremely complicated. In our opinion, the three-stage-test evaluation would not be satisfied to acknowledge that coders owe the duty of care to the software users:

- the ***proximity*** between coders and software users exists, however, this ***connection is weak***. A developer can assume that his work would affect the user experience although, first of all, the pull of users is very broad; second of all, the users are not as identifiable as in case of cryptocurrency platforms' users; lastly, users are not unified – they may have a different level of technical skills and knowledge, the software usage

[270] Donoghue v Stevenson [1932] UKHL 100, 8, https://www.uni-trier.de/fileadmin/fb5/FFA/KURSUNTERLAGEN/Anglo-Amerikanisches_Recht/Law_of_Torts/Siry-SS-2012/Donoghue_v_Stevenson__1932__UKHL_100__26_May_1932_.pdf

[271] Jenny Steele, *Tort Law: Text, Cases, and Materials* (Oxford: Oxford University Press, 2017), 115, 165-166.

[272] Anns v. Merton London Borough Council [1978] AC 728, http://www.e-lawresources.co.uk/cases/Anns-v-Merton-London-Borough-Council.php

by a 'reasonable man' with no computer knowledge can vary from the usage of the same software by a somewhat skilled person.

- the most important criterion is the ***foreseeability of code errors***. When the code is written it goes through several testing stages. The author of code tests it himself after that such code should be tested by QA (testing) engineers before deployment. While some errors might be detected on this stage, the others only occur in the run-time, meaning in the process when the program is executed by a user. These errors are a deviation from intended software behavior, developers might expect 'bugs' occurrence, they do not, however, know what type of errors will occur exactly. **Errors in the code after deployment are not foreseeable**.
- we doubt that it would be ***fair*** to impose liability on coders for errors that were not expected or intended. If judges adopt this approach in the future case law and coders will be liable for all errors after deployment, it means that the *strict liability regime* will be applied to such cases. We believe, such an approach is unjustified. Strict liability where the fault is irrelevant goes against the nature of tort of negligence because this delict is fault-based.

The case law regarding negligence issues in the cryptosphere either rare or does not yet exist, therefore, judges in different jurisdictions may found that software developers may owe a duty of care to the end-users or relevant legislation may emerge which will impose the duty of care on coders. In this case, the ***following problems*** arise:

1. To bring a claim to the court, the claimant should identify the defendant. Usually, the claimant may be an ordinary person that does not know much about the software development process. Moreover, identification of the coder whose programming code possibly produced the error requires substantial resources and/or the permission from authorities to request needed information from third parties. Such power only belongs to judges, prosecutors, detectives, or intelligence agencies and they use it to fight crimes. No regular person possesses such power, thus, the *instruments available for claimants for finding the wrongdoer and bringing him to court are inefficient*.
2. In a very unlikely scenario, an injured party may found the coder who supposedly caused the damage. The truth is that *people often remain anonymous on the web*. The biggest platform for code storing and code management where e.g. the source code of Bitcoin stored – GitHub[273] – does not have proper Know-Your-Customer

[273] Main, GitHub, Accessed 1 April 2020, https://github.com/

policies as payment and financial institutions have. No analogous platforms adhere to such policies because it was not needed at the time. Therefore, except for a nickname, email, and other unuseful information for the injured party, the platform cannot give any relevant information for the potential claimant regarding the wrongdoer's identity.

3. Another problem is *application dependencies* (development and production) – external libraries and frameworks written by other developers – that were used for program creation. Those libraries, not the code written by program creators, may cause an error. Identification of a responsible person in such a case is very difficult or merely impossible.

Breach of duty of care. The breach of duty of care occurs when one party behaving in an unreasonable manner case foreseeable damages to the other.

Usually, the ***test of 'reasonable person'*** is used in the evaluation of defendants' behavior. However, if we take into consideration the actors of cryptocurrency relations (coders, cryptocurrency platforms' staff, miners) it is clear that this test is not sufficient because involved people almost always have special and even professional knowledge or skills. Thus, a test of '***the ordinary skilled person in the same area'*** first mentioned in *Bolam v Friern Hospital Management Committee*[274] should apply.

Cases relating to medical negligence can be applied by analogy to cryptocurrency-related claims. *J. Steele* writes about two concerns in such disputes: what is the correct approach to the standard of care in respect of activities which require special skills? How the court will deal with different opinions among practitioners regarding correctness and reasonableness of the defendant's actions? The '*Bolam test',* however, criticized by some scientists and judges, answers these questions: the defendant "is not guilty of negligence if he has acted in accordance with a practice accepted as proper by a reasonable body of medical men skilled in that particular art."[275] Simply, when a medical professional states that he would behave as the defendant did then the defendant highly possible would escape liability. The diverging approach is shown later in the *Bolitho v City and Hackney Health Authority*[276]: a judge may hold that opinion of a particular professional is not reasonable. When the damage arises from the glitch in the program it is possible to assess the reasonableness of a coder's actions/omissions or evaluate some management decision that caused the damage using the test of 'the ordinary skilled person in the same area.'

[274] Jenny Steele, *Tort Law: Text, Cases, and Materials* (Oxford: Oxford University Press, 2017), 129.

[275] Ibid.

[276] Ibid, 130-132.

Yet, medical negligence cases may be of some help with cryptocurrency platforms and cryptocurrency developers negligence claims analysis, there is a substantial and troubling difference between two spheres: a lot of medical standards and instructions exist, there are regulatory bodies over medical practitioners; there is no such thing in the cryptocurrency sphere. Therefore, when judges analyze the defendant's behavior the judgment may be fully based on the subjective opinion of another developer.

Not only injured parties should prove the existence of a duty of care, its breach by a defendant but also ***justify that exactly this breach caused the damage***. Due to the high technicality of cryptocurrency claims, it would be merely impossible to find out, evaluate the causality, and prove this statement in court.

It worth mentioning that when a cryptocurrency platform company is involved in the legal dispute and in the process of facts evaluation the court found out that the damage was caused due to employee negligence, the ***employer would be liable*** for acts of its employee[277].

The case law regarding cryptocurrency issues and negligence is rare and young at the point, however, two cases already exist in the *US – Terpin v. AT&T Mobility*[278] and *Fabian v. LeMahieu*[279].

In the *Terpin v. AT&T Mobility, a* cryptocurrency investor Mr. Terpin claimed that due to negligence on the defendants' part – one of the biggest wireless services providers in the US – fell victim to the cryptocurrency theft. The claimant stated that in 2017 hackers approached his phone number and successfully gained access to his accounts associated with the cell phone number. After that impersonators convinced claimant's business partners to transfer cryptocurrency owed by Mr. Terpin. After that incident, the victim informed the service provider and they severed the client's security protection. However, in 2018 Mr. Teprin was a second-time victim of another hack called "SIM card swap." The claimant alleged that hackers succeeded because the defendant's employee helped to transfer Mr. Teprin's phone number to another SIM card in the control of imposters. The defendant failed to respond and act quickly when found out about the hack which caused Mr. Terpin damage evaluated in 24 million dollar worth of cryptocurrency. The court dismissed the claim because the plaintiff failed to elaborate on how exactly hackers succeeded in the later theft. Although the claim was dismissed, the case is

[277] "An Employer's Liability for Employee's Acts," FindLaw, Accessed 1 April 2020, https://smallbusiness.findlaw.com/liability-and-insurance/an-employer-s-liability-for-employee-s-acts.html

[278] Terpin v. AT&T Mobility, LLC [2019], Order Granting, in Part, and Denying in Part, Defendant's Motion to Dismiss[14]; And Denying Defendant's Motion to Strike [15], https://www.leagle.com/decision/infdco20190722561

[279] Fabian v. LeMahieu [2019], CASE NO. 19-cv-00054-YGR, Order Granting in Part and Denying in Part Motion to Dismiss, https://casetext.com/case/fabian-v-lemahieu

prominent because the plaintiff had good chances of winning if only he had explained the actions of hackers after the SIM card swap and prove all the necessary elements of the tort of negligence.

The *Fabian v. LeMahieu* case is an example of a class action brought by J. Fabian against multiple defendants with multiple claims including negligence claim. The plaintiff alleged that a cryptocurrency platform Nano, its developers, and the marketing team, a cryptocurrency exchange BitGrail located in Italy and its principles were liable for cryptocurrency theft on BitGraile.

The new cryptocurrency "Nano Tokens" (XRB) is similar to Bitcoin but Nuno developed a better, scalable new blockchain that fixed problems existing in the previously created blockchains according to Nano's published promotional materials. XRBs were "promoted, offered, traded, and sold to the public for" Nano's "personal financial benefit."[280] Nano in April 2017 agitated for trading, storing, and purchasing XRBs through BitGrail which allegedly safely accumulated investors funds.

In February 2018, an unauthorized transaction happened on the abovementioned "safe" cryptocurrency exchange and $170 million worth of XRBs were lost. It amounts to 80 percent of XRBs that were held on customers' accounts. The plaintiff stated that he lost all the money from his wallet because of the theft which happened due to the vulnerability of the programming code.

The court utilized a ***six-stage-test*** used in the *Rowland v. Christian* case to evaluate whether that duty extends to the plaintiff:

- the foreseeability of the harm to the plaintiff ;
- the degree of certainty that the plaintiff suffered injury;
- the closeness of the connection between the defendant's conduct and the injury suffered;
- the moral blame attached to the defendant's conduct;
- the policy of preventing future harm;
- the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach and the availability, cost, and prevalence of insurance for the risk involved[281].

Contrastingly to the precious case, Mr. Fabian succeeded in proving the needed elements of the tort of negligence because the court found that five out of six criteria are satisfied. The court held that lack of security on cryptocurrency exchange can result in harm to investors (foreseeability); Nono defendants' conduct could be viewed as morally reprehensible and "and this type of action could further the goal of preventing future harm"; imposing a duty of care would

[280] Fabian v. LeMahieu [2019], CASE NO. 19-cv-00054-YGR, Order Granting in Part and Denying in Part Motion to Dismiss, Accessed 3 April 2020, https://casetext.com/case/fabian-v-lemahieu

[281] Ibid.

not be an undue burden for defendants or the industry; defendants "conduct was proximately connected to plaintiff's injury, even if through the actions of the BitGrail Defendants."[282]

It is an ongoing case and we cannot know the outcome but the probability of winning the case by the plaintiff is very high.

All things considered, cryptocurrency platforms or other service providers may be held liable for cryptocurrencies' thefts or other customers' losses that occurred due to the breach of care. The claimants should carefully evaluate and present their reasoning in court for their claims to succeed.

The ***possible solution to the mentioned problems*** was discussed in the chapter on contractual liability. It may prevent various claims from occurring and be a pointer for juridical analysis in cases of negligence: it is crucially important to adopt modern international standards and frameworks applicable to cybersecurity, code testing, and code design. Every company providing software or offer its services through a web platform, as well as independent coders, should adhere to such standards. Moreover, companies should adopt local internal policies for the same issues, for example, with raising danger from hacking companies should think not only about regular testing of code on account of "bugs" but also consider adoption of penetration testing requirements for their platforms. When a company staff adheres to own standards and international frameworks but the damage still occurs, the company may escape the liability for negligence.

3.1.2.Negligence in the continental law system

The approach taken in continental law system countries regarding non-contractual liability varies from the approach in common law states. Similarly to *corpus delicti (mens rea and actus reus)* in criminal law, it should be proved in court that several criteria are met regarding a delict to make a person liable for the damage. The basis for civil liability in tort – named the general delict[283] – according to article 1166 of the Civil Code of Ukraine:

1. *"Actus reus" for a civil wrong*:
   a. unlawful behavior;
   b. damage;
   c. causality between unlawful acts and the caused damage;
2. *"Mens rea" for a civil wrong*: fault (intention or negligence)[284].

[282] Fabian v. LeMahieu [2019], CASE NO. 19-cv-00054-YGR, Order Granting in Part and Denying in Part Motion to Dismiss, Accessed 3 April 2020, https://casetext.com/case/fabian-v-lemahieu

[283] Legal Commentary on the article 1166 of the Civil Code of Ukraine, ННП Юрисконсульт, Accessed 3 April 2020, https://legalexpert.in.ua/komkodeks/gk/79-gk/1533-1166.html

[284] Article 1166, Цивільний кодекс України, в редакції від 02.04.2020, Законодавство України, Accessed 14 April 2020, https://zakon.rada.gov.ua/laws/show/435-15#n5466

The most important requirement is unlawful behavior on which the existence of civil liability would depend. *O. Terefenko* writes about three theories on unlawful acts or omissions:

1) *normative theory* (M. Agarkova, G. Matveev, Y. Tolstoy, V. Smernova, etc.): unlawful behavior contradicts legislation requirements.
2) *semi-objective or semi-subjective theory*: violation of a personal right and legislation provisions.
3) *legal breach of duty theory* (A. Savytska): unlawful behavior is reduced to the breach of a person's legal duty.

The prevailing approach in Ukrainian case law is that the civil wrong can only exist when a person acted contradictory to requirements set out in statutes. Situations mentioned above that can occur in the cryptosphere do not relate to breach of the law because Ukrainian law does not contain any norms that might be breached when the software is developing.

Logically then, we might think about compensation requirements that can arise from lawful or legally neutral behavior. Ukraine has a body of law that contains particular situations that may arise in this regard. Thus, the compensation should be made for harm caused: by a person in a situation of extreme necessity (emergency); by property requisition (made by state authorities); by the authority's act that takes a particular property out of circulation (the possession of the property is no longer allowed); by self-defense[285]. None of such cases is applicable in the cryptosphere.

Having in mind the peculiarity of Ukrainian legislation and similar rules that exist in civil law system countries, common law is more favorable to injured parties and there is a possibility for winning the case and held a wrongdoer accountable. As to Ukraine, it seems impossible to prove the case in Ukrainian courts until sufficient legislation or standards will be adopted in the sphere of software and web development, cybersecurity, cryptocurrency company management, and accountability.

3.2. Breach of statutory duty

In common law tradition, a defendant who breached ***a statutory duty*** can be sued by a claimant for damages. It means that the defendant breached the duty that arises under the statute (for the UK – the Act of Parliament), not under common law.[286] This fact is particularly relevant

[285] V. Melnyk, "Відшкодування шкоди, завданої правомірною поведінкою," *Актуальні проблеми приватного права : матеріали наук.-практ. конф., присвяч. 94-й річниці з дня народж. В. П. Маслова, Харків, 19 лют. 2016 р.,* (Kharkiv: Право, 2016), http://dspace.nlu.edu.ua/bitstream/123456789/12670/1/Melnyk.pdf

[286] Nicholas J. McBride, Roderick Bagshaw, "Breach of Statutory Duty," *Tort Law* (Harlow: Pearson Education Limited, 2018), https://books.google.com.ua/books?id=l71dDwAAQBAJ

for the cryptocurrency market because, with the growth of the industry, the legislation regarding cryptocurrency is evolving as well. In particular, when a crypto asset falls under the definition of the *financial instrument*, the companies who deal with it should comply with the European Market Infrastructure Regulation ("EMIR"), Markets in Financial Instruments Regulation ("MiFIR"), and Markets in Financial Instruments Directive (MiFID II).[287] This is relevant, for example, for actors involved in crypto derivatives trading (futures, swaps, forwards contracts, and crypto contracts for difference, etc.). Cryptocurrency is usually recognized as a *financial asset*, therefore, cryptocurrency exchanges and crypto wallets companies are in the scope of FATCA and CRS frameworks[288]. We also mentioned that cryptocurrency actors are in the scope of the anti-money laundering law and anti-terrorism financing regulations that require financial institutions and companies that deal with money transactions to monitor transactions made on their web platforms in a specific way (tracing sums that exceed a specific amount, report such transactions to authorities, Know-Your-Customer policies, etc.). We expect that other documents that specifically relate to the cryptocurrency regulation will be created soon: as an example, the Cryptocurrency Act 2020 – a bill recently introduced in the US[289].

Not every breach of statutory duty is civilly actionable because private persons do not enforce most of the statutory duties. Most of the actions are brought to the court by state authorities to stop unlawful behavior or eliminate the negative consequences of the mentioned conduct. N. J. McBride and R. Bagshaw distinguish three cases when a claimant might bring an action to court:

1. ***breach of duty owed to no one in particular***: when a plaintiff *suffered special* damage caused by *public nuisance* committed by defendant; or when a defendant is *a public official* who is accused of *misfeasance in public office*;
2. ***breach of duty owed to a third party***: when the defendant breached one duty owed to a third party together *with another tort in relation to the claimant.*
3. ***breach of duty owed to the claimant***: when the duty imposed on the defendant was in claimant interest or the interest of a specific group of people and the following requirements are met:
   a. statutory duty was imposed on the defendant for interested people to avoid a particular loss or harm. By breaching the duty, the defendant caused to

[287] "MiFID II, Crypto Assets and the Cryptocurrency Market," eflow, Accessed 4 April 2020, https://eflowglobal.com/2019/06/17/mifid-ii-crypto-assets-and-the-cryptocurrency-market/

[288] Anna Szkudlarek, "Cryptocurrency taxes – CRS/FATA: Do you need to disclose your cryptocurrencies?" KENDRIS, Accessed 4 April 2020, https://www.kendris.com/en/blog/crs-fatca-do-you-need-disclose-your-cryptocurrencies

[289] Kevin Helms, "US Lawmaker Introduces Crypto-Currency Act of 2020 While Under Coronavirus Quarantine," Bitcoin.com, Accessed 6 April 2020, https://news.bitcoin.com/cryptocurrency-act-of-2020/

the claimant the specifically *mentioned loss or harm* (the other losses are not included);

b. policymaker intended that such breach of duty would be *civilly actionable*[290].

The last scenario is relevant to cryptocurrency relations. We can outline **three groups of** relevant **legislation** existing on national, regional, and international levels that designed to safeguard the interests of particular groups of persons:

1. legislation that protects ***investors in cryptocurrency***;
2. regulations intended to protect ***users (consumers) of services*** provided through the Internet;
3. ***data privacy*** regulations that lay down rules on personal data protection and free movement of personal information.

I. Cryptocurrency agreements may be viewed as ***securities***. There is a growing tendency in the US to bring to court violators of the Securities Act and the Securities Exchange Act who happen to be involved with cryptocurrency. American authorities are also inclined to consider ICOs as securities public offering. Therefore, many crypto actors should comply with registration and licensing requirements in the US and most of them fail to do so.

The statistic shows that the number of cryptocurrency lawsuits grows rapidly and the prevailing amount is security-related claims, comparing to the disputes regarding other issues[291]:

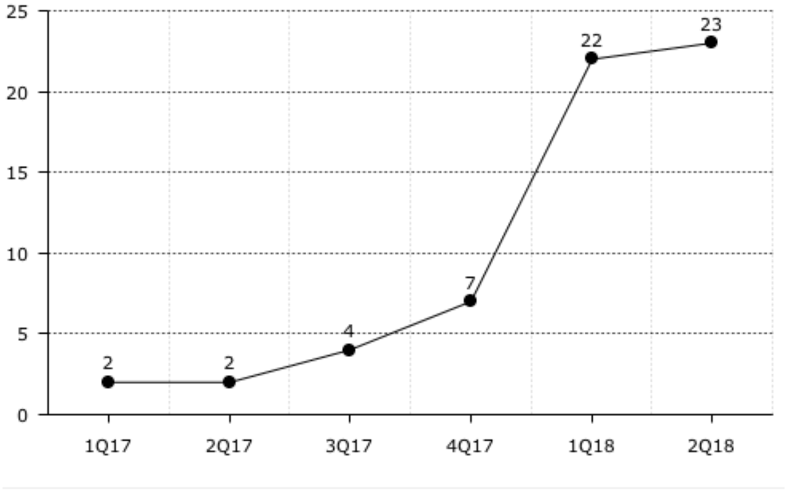


Diagram 1: raising amount of the lawsuits relating to cryptocurrency in the US[292]

[290] Nicholas J McBride, Roderick Bagshaw, "Breach of Statutory Duty," *Tort Law* (Harlow: Pearson Education Limited, 2018), https://books.google.com.ua/books?id=l71dDwAAQBAJ

[291] David Canellis, "Cryptocurrency-related lawsuits are mooning, up 300% from last year," TNW, Accessed 4 April 2020, https://thenextweb.com/hardfork/2018/11/20/cryptocurrency-lawsuits-moon/

[292] Ibid.

We mentioned the ***Howey test*** that is a standard in American law for clarifying whether a contract constitutes securities. The test now is applied to many cryptocurrency deals. As a recent example, 11 cryptocurrency companies were the target of the lawsuits filed in the court of the Southern District of New York on April 3, 2020. The Roche Cyrulnik Freedman, representing Chase Williams, Alexander Clifford, and Eric Lee[293], claimed that each company publicly sells or helps in selling unregistered securities as tokens through crypto exchanges in the form of initial exchange offers or ICOs. The involved defendants presented utility tokens[294] for sale that were unregistered securities [295]. Investors in such utility tokens were promised new benefits and these promises were never fulfilled. "Most of these tokens are now trading at a tiny fraction of their 2017-2018 highs"[296]. Although, it is not yet clear what holding the court will provide regarding this case.

Another prominent and similar to the previous one case has a two-year history – *Zakinov Et al v. Ripple Labs*. The class action headed by the lead plaintiff Bradley Sostack – an investor in XRP – was brought into court on behalf of investors in XRPs against Ripple Labs. The defendant was accused of false advertisement, unfair competition, and sale of unregistered securities[297][298]. Ms. Sostack purchases XRPs "for $300,000 worth of Bitcoin and USDT and suffered over $100,000 in losses as a result of those XRP transactions"[299]. The plaintiff expects the award of damages to all misled investors and the costs of the legal action[300]. The case is ongoing but

[293] Jeff Fawkes, "Lawsuits Filed against Binance, Block.one, BitMEX and Other Crypto-Related Companies," Coinspeaker, Accessed 5 April 2020, https://www.coinspeaker.com/lawsuits-filed-binance-bitmex-block/

[294] ***Utility token*** is a token issued in order to fund the development of an IT systems and/or business model and can typically be used to later on purchase goods or services created by the issuer of that token and can thus oftentimes be seen as usage rights (e.g. right to access to a service or subscription). Cited from Patrick Schueffel, Nikolaj Groeneweg, and Rico Baldegger, *The Crypto Encyclopedia: Coins, Tokens and Digital Assets from A to Z,* (Bern: Growth Publisher, 2019), 61, https://www.heg-fr.ch/media/lbdfnyd1/schueffelgroenewegbaldegger2019_crypto-encyclopedia_eng.pdf

[295] Drbyos, "Simultaneous class action lawsuits filed against 11 bitcoin companies," World Today News, Accessed 5 April 2020, https://world-today-news.com/simultaneous-class-action-lawsuits-filed-against-11-bitcoin-companies/

[296] "Tidal Wave of Lawsuits Accuse Bitcoin (BTC) and Crypto Companies of Selling Unregistered Securities," The Dayly Hodl, Accessed 5 April 2020, https://dailyhodl.com/2020/04/05/tidal-wave-of-lawsuits-accuse-bitcoin-btc-and-crypto-companies-of-selling-unregistered-securities/

[297] Philip Rosenstein, "Investors Allege Ripple CEO Dumped XRP While Touting It," Law360, Accessed 5 April 2020, https://www.law360.com/articles/1257526

[298] Zakinov Et al v. Ripple Labs [2020], Case 4:18-cv-06753-PJH, http://securities.stanford.edu/filings-documents/1066/RLI00_01/2020226_r01x_18CV06753.pdf

[299] Zakinov Et al v. Ripple Labs, Motion to Appoint Lead Plaintiff and Lead Counsel, 1, Accessed 5 April 2020, https://www.docketbird.com/court-documents/Zakinov-Et-al-v-Ripple-Labs-Inc-et-al/OPPOSITION-RESPONSE-re-36-MOTION-to-Appoint-Lead-Plaintiff-and-Lead-Counsel-filed-by-Bradley-Sostack/cand-4:2018-cv-06753-00050

[300] Adrian Zmudzinski, "Lawsuit Alleging Ripple's XRP Is Unregistered Security Moves Forward," Cointelegraph, Accessed 5 April 2020, https://cointelegraph.com/news/lawsuit-alleging-ripples-xrp-is-unregistered-security-moves-forward

revolutionary because it can overturn the cryptocurrency industry and crash the XRP market if the court found that Ripple tokens are securities[301].

In our opinion, such cases in the US would become a trendsetter for other jurisdictions, and possibly new legislation would emerge regulating some cryptocurrency deals as securities offerings.

II. ***Consumer protection*** legislation is highly interrelated with contract law and contractual liability. Therefore, the regulations designed by policymakers could be broken down into three categories by stages of contractual relations:

I. ***pre-contractual stage***: companies should comply with regulations that ensure consumer awareness about relevant, sufficient, and needed information before they enter into contractual relations:

   a. bans on the misleading or false advertisement;
   b. "content and warning labeling, as well as pre-existing conditions evidencing the consumer's 'consent to contract' (capacity to contract, free will, etc.)";
   c. limitation "of freedom of contract by forbidding or sellers obligations to utilize specific conditions in their contracts" such as the imposition of quality standards, price control, interest rate caps regulations";
   d. bans of unfair contractual terms or practices.[302]

II. ***post-contractual stage***:

   a. the fair and affordable conditions of access to redress mechanisms;
   b. rules that shift the burden of proof (in favor of the consumer);[303]
   c. product liability rules.

In *Zakinov Et al v. Ripple Labs* case, plaintiffs referred to the consumer protection legislation (false advertisement of Ripple Labs), the judge, however, did not accept this claim[304]. Although this strategy was not successful for the claimants, we expect that potentially injured parties would use breach of consumer protection statutes by wrongdoers in court more often. In particular, in cases when a company or an individual promotes ICO in violation of consumer

[301] ***Security token*** is an investment vehicle which has the character of a security, i.e. it is bought in anticipation of future profits in form of dividends, revenue share, or price appreciation. Cited from Patrick Schueffel, Nikolaj Groeneweg, and Rico Baldegger, *The Crypto Encyclopedia: Coins, Tokens and Digital Assets from A to Z,* (Bern: Growth Publisher, 2019), 49, https://www.heg-fr.ch/media/lbdfnyd1/schueffelgroenewegbaldegger2019_crypto-encyclopedia_eng.pdf

[302] Jami Solli, Arthur Goujon, and Michael Gaweseb, "A guide to developing consumer protection law" (London: Consumers International, 2011): 10, http://www.fao.org/3/a-at346e.pdf

[303] Ibid

[304] Zakinov Et al v. Ripple Labs [2020], Case 4:18-cv-06753-PJH, http://securities.stanford.edu/filings-documents/1066/RLI00_01/2020226_r01x_18CV06753.pdf

protection legislation, regulations regarding the promotion of products and investors in such ICO incur losses due to ICO's value decline.

One peculiar case relating to consumer protection law violation is a class action case *Gevorkyan v. Bitmain Inc. et al.*[305] The company and other Chinese defendants were accused of unauthorized mining by Bitmain at its clients' expanse, unjust enrichment, unfair business practices, and false advertisement. The plaintiff explained that he bought a mining rig that was extremely difficult and confusing to configure. When Mr. Gevorkyan started the machine it was running in the high consuming mode and all cryptocurrencies mined until the rig was properly configurated had been sent to the defendant. It is also an ongoing case and if the court decides in the plaintiff's favor then there might be a burst of new standards in the sphere of crypto mining products and its offerings.

The rising violation of consumers' interests is also supported by the report provided by *ValuePenguin* dedicated to the growing number of consumer complaints to the Consumer Financial Protection Bureau in the US and other consumer agencies in other states[306].

In particular, the report shows that consumers' complainants against the cryptocurrency exchange Coinbase increased when the Bitcoin price soared up to $20000 per coin in December and dropped down to half of this price within a month. The following graph shows the spike of complaints just when the Bitcoin value started to crash.

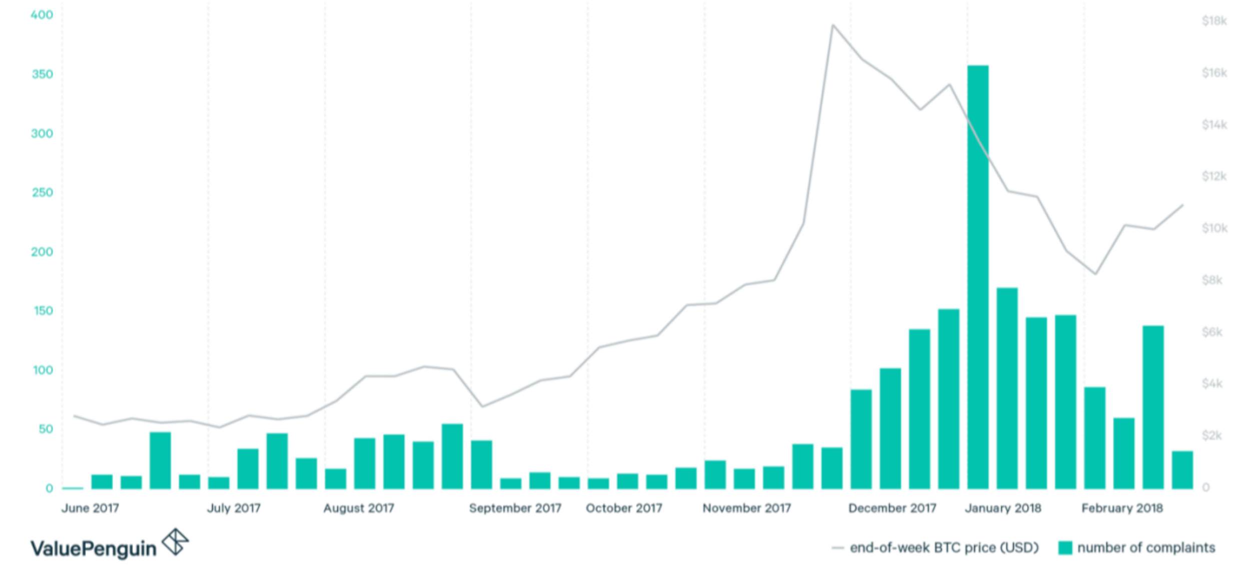


Diagram 2 Raising of consumers' complaints against Coinbase[307]

The resource highlights **five main topics of complaints**:

[305] Gevorkyan v. Bitmain Inc. et al., Case 5:18-cv-07004, https://ru.scribd.com/document/393870365/Bitmain-Class-Action

[306] David Ascienzo, "Cryptocurrency CFPB Complaints Rise as Prices Fall," ValuePenguin, Accessed 6 April 2020, https://www.valuepenguin.com/cfpb-complaints-about-cryptocurrencies

[307] Ibid.

1. money was not available when promised – 40%;
2. other transaction problem – 20.5%;
3. fraud or scam – 11.7%;
4. other service problem – 7.9%;
5. managing, opening, or closing mobile wallet account – 7.9%.

Unfortunately, the only satisfaction the consumers received was either Coinbase's explanation for the issue or some negligible other relief provided by the company in question[308].

III. ***Data protection*** law may be also an issue to worry about for companies involved in cryptocurrency transactions. The first concern is the possibility of data leaks as a result of hacker attacks or vulnerability of the software. Another concern may be the architecture of the blockchain itself – the immutability of data in the blockchain. According to regulations designed to protect user data, e.g. GDPR, data subjects have the main rights towards their personal information: the rights of access, rectification, 'to be forgotten', etc.[309] The last two are impossible to satisfy in the cryptosphere. Once the data is in the DLT, no one can change or delete it. Therefore, the businesses involved in cryptocurrency transactions should take into account such specifics and develop mechanisms of data management that prevent data privacy and data protection claims.

Regarding ***continental system countries***, it is clear from the previous subchapter on the tort of negligence that a plaintiff can bring the claim into court in case there are all elements of delict. Although a breach of statutory duty, contrastingly to the UK law, is not only a breach of the acts of Parliament but also of other regulations issued by the government. When there is only the violation of national statutes – this is the domain of administrative law and state authorities hold wrongdoers liable in court, however, when there is damage to a private person as a result of a breach of statutory duty then it could be the domain of civil non-contractual liability.

To recapitulate, there may be interference between contractual and tortious liability: the presence of tort may constitute a breach of contract, the tort may trigger the invalidity of a contract, or the tort is only present because there has been a breach of a contract, etc.[310] However, we managed to distill the torts that could happen in the cryptocurrency domain – the tort of negligence and breach of duty – and analyze it in isolation from contractual liability. To constitute a tort of negligence, a plaintiff should prove the presence of the necessary tort's elements. For this matter, the US and the UK judges use legal standards (tests) contained in their case law. The breach of

[308] Ibid.

[309] 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), Intersoft Consulting, Accessed 6 April 2020, https://gdpr-info.eu

[310] Christian von Bar, Ulrich Drobnig, and Guido Alpa, *The Interaction of Contract Law and Tort and Property Law in Europe: A Comparative Study* (Munich: Sellier European Law Publishers, 2004), 15-16.

duty can happen regarding the breach of rules enshrined in three bodies of law: consumer protection, data privacy protection, and investor protection law. The relevant statute should contain an intention to make such breach of duty civilly actionable.

CONCLUSIONS

1. Based on the analysis of functions and characteristics of money, features of commodities, and qualities of cryptocurrencies, the research revealed that the cryptocurrencies are different from commodities and they possess features of money. The results confirm that cryptocurrencies could be treated as a financial asset for financial purposes, however, in legal domain cryptocurrency should be perceived similar to foreign currency. Thus, "goods for cryptocurrency" contracts are not barter agreements, but contracts of sale, correspondingly, "cryptocurrency for fiat money" are currency exchange agreements and not contracts of sale. These conclusions are important for the proper understanding of contractual relations existing in the cryptocurrency sphere.

2. The analysis of technical specifications and cryptocurrencies whitepapers showed that different *cryptocurrencies have shared features but they could function differently* due to diverse technologies used for their creation. In particular, cryptocurrencies vary by the possibility to mine coins, limitation of coins ever to be available, the level of centralization, anonymity, consensus protocols, etc. The last three factors are relevant for participants of private relations and courts when they decide on claims related to cryptocurrency.

3. Through analysis of scientific works, cryptocurrency market, and relevant case law we distilled *seven issues that relate to civil liability*: the unclarity of cryptocurrency and crypto assets nature on the legal level; the volatility of cryptocurrencies; abuse of unfair contractual terms in Terms of Services agreements by cryptocurrency platforms; confusing nature of automated and smart contracts and, therefore, liability complications in case of problems with their conclusion and performance; unfair business practices in cryptosphere; the cyber vulnerability of software used for cryptocurrency transactions; uncertainty on account of the duty of care owed by crypto companies and cryptocurrency developers to users.

4. Based on examination of smart contracts nature, cloud mining contracts, and analysis of numerous consumer agreements provided by service providers in the cryptocurrency sphere the results of the research prove that *default rules on contractual liability should apply* to contractual liability in the cryptocurrency relations. The uniqueness and convoluted nature of the cryptocurrency of which contract is concerned should not be of any importance for civil law rules applicability regarding their validity, binding nature, and liability issues for a breach.

5. Regarding *smarts contracts*, the findings present that it is possible to identify all the necessary elements for the conclusion of a binding contract according to civil law tradition rules as well as to common law rules. While smart contracts may bring some benefits and, according to their creators, offer automated performance, meaning no breach of contract could occur, the research showed that smart contracts cannot fully satisfy all demands of civil actors just yet. We

identified *the main problems* with smart contracts: high dependency on third-party oracles, the possibility of illegality, the impossibility of a contract, excuses for not-performance, unilateral or mutual mistakes, oracle mistakes, code errors. Parties should except these risks or anticipate them and include smart contract terms designated to protect their interests. We believe, smart contracts would be a useful tool when there was a well-developed infrastructure of automated oracles.

6. Through analysis of *B2C2 v. Quoine case,* we can prove the hypothesis that the "glitch" in the software – unintended behavior of the program – designed to create automated contracts does not make mistakenly concluded contracts void and such "glitch" does not justify the breach of the other related contract between involved parties. Neither mutual mistake nor unilateral mistake doctrine would help to escape liability.

7. Based on English and American case law analysis, which served as a benchmark for exploring common-law non-contractual liability issues, the research showed that the most common claims brought to courts relate *to the tort of negligence* and the *breach of statutory duty*. The civil law tradition was represented by Ukraine. The continental law countries have the following approach regarding tortious liability: the civil wrong only exists when a person acted contradictory to statutes requirements and the injured party suffered damage caused by the mentioned behavior. Ukraine does not yet have sufficient cryptocurrency legislation or standards, thus, it seems impossible to seek remedies in court until such legislation is adopted.

8. In our analysis, we reached the conclusion that cryptocurrency business actors while providing services owe a duty of care to their platform users because the circumstances satisfy, in most cases, a six-stage-test used *in Rowland v. Christian case* used in the US, as well as *Caparo v. Dickman test* used in the UK for determining whether a party owes a duty of care. Thus, such companies are liable for the breached duty of care. To establish a tort of negligence, a plaintiff would need to prove the presence of the necessary tort's elements and whether the breach occurred and caused the damage to the injured party is for courts to determine in every case.

9. Contrastingly, independent coders that contribute to the open-source software do not owe a duty of care to the software users because the requirements of the abovementioned tests are not satisfied. Thus, in most cases, they are not liable for code errors in the tort of negligence.

10. The analysis of American case law and scientific literature shows that the breach of statutory duty can happen through the breach of rules enshrined in three bodies of law: consumer protection, data privacy protection, and investor protection law. The relevant statute should contain an intention to make such breach of duty civilly actionable. One example is offering cloud mining contracts without registration, which may be considered investment contracts i.e. securities. The plaintiff also needs to prove that such breach caused damage which violated the statute intends to prevent.

RECOMMENDATIONS

1. Policymakers should take into account the nature of cryptocurrencies when they decide on adopting cryptocurrency legislation. In particular, their cross-border character and decentralized nature. In order to support the cryptocurrency industry and at the same time protect the private interests of civil relations actors, states and state authorities should cooperate for international framework development. This framework may be a basis for legislation implemented on a national level. This document should only reflect academic and legal research on cryptocurrency nature and identify once and for all what a cryptocurrency is in law. The proposition then resolves the problem of uncertainty of cryptocurrency status identified in the conclusions and lays down clear and unified rules for cryptocurrency market participants, thus ensuring the consistency among states' legal provisions.

2. Policymakers should also understand that an abundance of codifications or regulations deny the benefits of cryptocurrencies because creators of cryptocurrencies intended to eliminate or at least alleviate state involvement in cryptocurrency flow. They tried to break existing models with a high dependency on third trusted parties in the extremely regulated financial industry – the cause of excessive fees for transactions. The proposed solution is to look into the cryptocurrency problems identified in the research and use existing legislation on consumer protection, data privacy protection, and investor protection in the cryptocurrency domain.

3. The cryptocurrency industry triggered automated contracting development. Such contracts are concluded and performed without human involvement. States should consider enshrining a specific provision within their Civil Codes regarding such contracts because we anticipate the raised number of disputes regarding such contracts in the future. Such provision should reflect scientific views displayed in the relevant researches, such as ours. This will help judges to analyze case circumstances more efficiently and, most importantly, it will accelerate the dispute resolution process.

4. Another problem mentioned in the conclusions is the cyber vulnerability of the cryptocurrency sphere. We propose to adopt *international modern* standards on cybersecurity or amend outdated existing ones, provide recommendations on risks management and IT disaster recovery procedures, promote business continuity approach among cryptocurrency companies. These documents will help to reduce the possibility of network penetration and disruption by malware and hacking. Also, it would be much easier to establish for courts whether a company liable in the tort of negligence in the case of cyberattack that caused financial losses for injured parties. Also, not only crypto companies can protect themselves from losses by adherence to these standards but also build a strong defense strategy in court. Although we propose such standards as soft law instruments, governments may require adhering to these standards on the official level.

5. Because of the rarity of cryptocurrency-related civil cases, judges of different jurisdictions should rely on foreign case law. Although common law tradition is different from civil law, courts could benefit from foreign case law and find necessary answers for their cases.

6. Due to the abuse of unfair contractual terms and unfair business practices in the cryptocurrency domain, we suggest governments and non-governmental organizations start campaigns aiming to educate people interested in the crypto sphere, to draw their attention to nuances in contracts that cryptocurrency platforms provide, etc. It could be done through the constant publishing of electronic materials on official web pages of state authorities or non-governmental organizations. The best strategy to deal with damages and financial losses is preventing them.

7. Further academic studies could address several issued: cryptocurrency derivatives, cryptocurrency market manipulation, cryptocurrency insurance.

Annex 1: Correlation of terms: money, fiat money, e-money, virtual, digital, and cryptocurrency

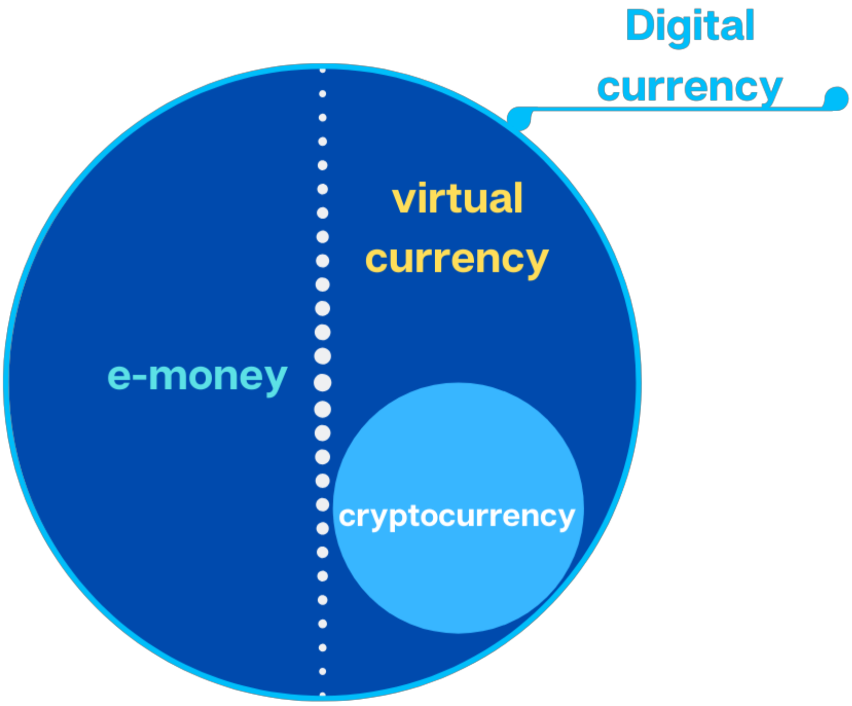


Diagram 3: How the correlation of terms looks like in scientific and media society

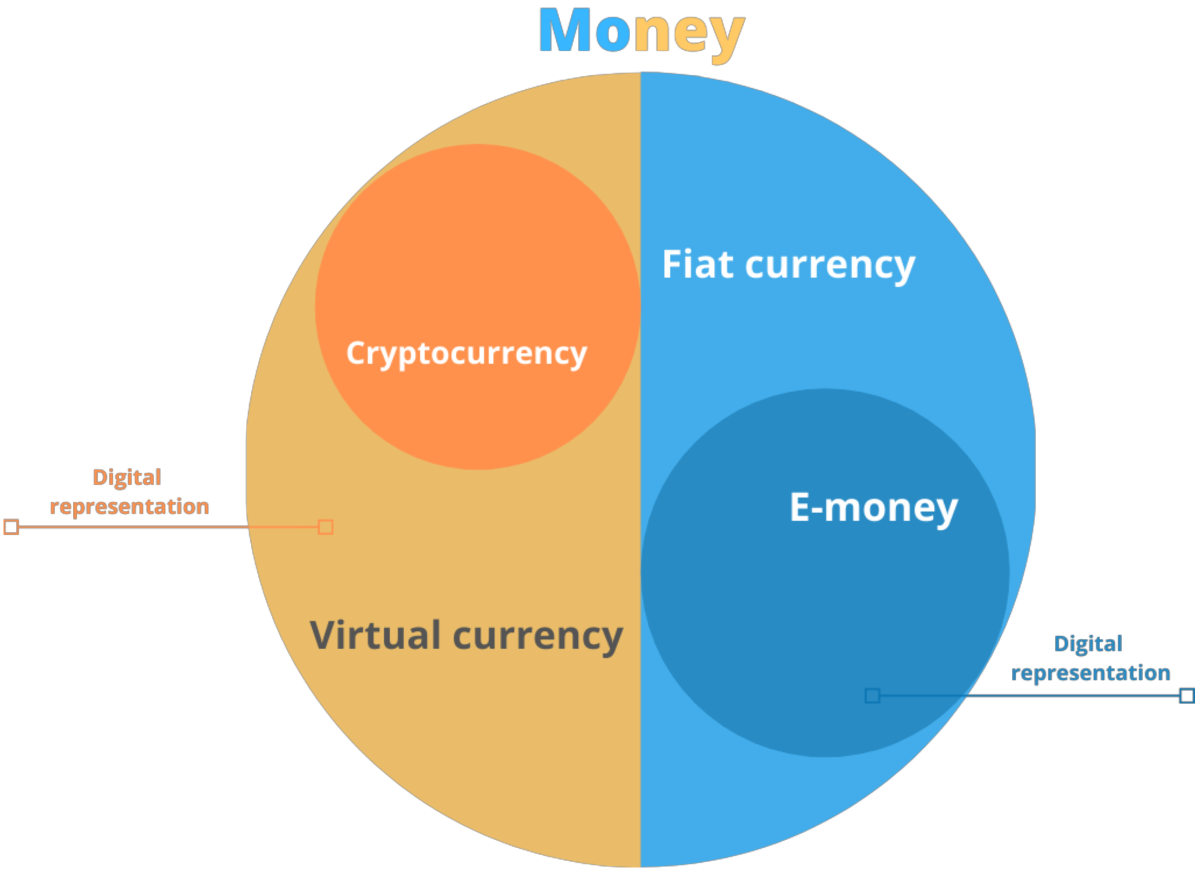


Diagram 4: How the correlation of terms should look like

Annex 2: Comparison of e-money, virtual currency, digital currency and cryptocurrency

Table 1: *Comparison of e-money, virtual currency, digital currency and cryptocurrency*

Aspect	E-money	Virtual Currency	Digital Currency	Cryptocurrency
Electronic representation of legal tender	Yes	No	No	No
Centralized or Decentralized	Centralized	Could be both	Could be both	Centralized / Decentralized / Hybrid (semi-decentralized[311])
Pear-to-pear	No (mostly*)	Yes	Could be both	Yes
Requires issuer	Yes	Yes (mostly)	Could be both	Could be both
Means of exchange	Yes	Could be both	Could be both	Yes

*E-money are not usually transferred pear-to-pear, meaning that exchange of assets or data between parties is made without the involvement of a central authority. However, Vietnamese currency, dong (VND), and Chinese currency, yuan (CNY) – are two fiat currencies that are traded on one of the major cryptocurrency exchange and blockchain ecosystem – Binance. Vietnamese dong was added on the 29th of January, 2020[312]; Chinese yuan – on the 9th of October, 2019[313].

[311] "Majority of Cryptocurrencies Can Be Classified as Centralized, Securities," NewsBTC, Accessed 3 February 2020, https://www.newsbtc.com/2018/10/17/centralized-cryptocurrencies-dominate-market-but-what-about-bitcoin/

[312] "Binance Adds Peer-to-Peer (P2P) Trading for Vietnamese Dong (VND)," Binance, Accessed 3 February 2020, https://www.binance.com/en/blog/421499824684900366/Binance-Adds-PeertoPeer-P2P-Trading-for-Vietnamese-Dong-VND-

[313] Marie Huillet, "Binance Launches P2P Trading for Chinese Yuan," Cointelegraph, Accessed 3 February 2020, https://cointelegraph.com/news/binance-launches-p2p-trading-for-chinese-yuan

Annex 3: Legal status of cryptocurrency in different jurisdictions

Table 2: *countries in respect to existing regulation of cryptocurrencies*

Regulation of cryptocurrencies	Countries
No legislation	Belize, Bermuda [314], Chile[315]
Banned	Pakistan, Iraq, Morocco, Egypt etc[316].
Implicit ban	China, Indonesia, Saudi Arabia, Dominican Republic etc[317].
Application of tax law	Argentina, Austria, Bulgaria, Finland, Iceland, Israel, Italy, Norway etc[318].
Anti-Money Laundering & Anti-Terrorism Financing Laws.	the Isle of Man, Estonia, Hong Kong, Latvia, Singapore, Lichtenstein, Luxembourg, etc[319].
Tax & Anti-money laundering & Anti-Terrorism Financing laws	Australia, Canada, Denmark, Switzerland, Japan[320]
Restrictions on investments in cryptocurrencies[321]	Marshall Islands, Venezuela, the Eastern Caribbean Central Bank (ECCB) member states, and Lithuania.

[314] *Regulation of cryptocurrency around the world,* (Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018): 8, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

[315] Ibid, 12.

[316] Ibid, 4,

[317] Ibíd.

[318] Ibíd, 5.

[319] Ibíd.

[320] Ibíd.

[321] Ibid, 2.

Table 3: *definition of cryptocurrencies in different countries in general*

What is cryptocurrency in general	Country
digital monetary units	Lichtenstein[322]
financial asset	Slovakia[323]
financial instrument	Germany[324]
other (intangible) commodities	Austria[325], Czech Republic[326], Australia[327], China[328], Hong Kong (but may be securities)[329], the US (regulation varies by state[330])
virtual asset	Mexico[331]
non-security tokens	Anguilla[332]
means of payment	Swiss Cantons of Zug and a municipality within Ticino, Isle of Man and Mexico[333], Canada[334], under EU Anti-Money Laundering Directive[335], Estonia [336]
contractual means of payment	Latvia[337]

[322] Ibid, 71.
[323] Ibid, 54.
[324] Ibid, 40.
[325] Ibid,30.
[326] Ibid,33.
[327] Ibid, 103-104.
[328] Ibid, 107.
[329] Ibid, 108-109.
[330] "Cryptocurrency Regulations Around The World," ComplyAdvantage, Accessed 24 February 2020, https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/
[331] *Regulation of cryptocurrency around the world,* (Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018): 16, https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf
[332] Ibid, 20.
[333] Ibid, 3.
[334] Ibid, 10.
[335] Ibid, 28.
[336] Ibid, 36.
[337] Ibid, 45.

Table 4: *definition of cryptocurrencies in different countries for tax purposes*

Classification of cryptocurrency for tax purposes[338]	Country
asset	Israel, Australia[339]
financial asset	Bolgaria[340]
foreign currency	Switzerland
capital property	Norway[341]
property	Russia[342], Japan[343], the US[344]
income (subject to income tax)	Argentina & Spain
income (subject to income tax and losses are deductible)	Denmark
Depending of the tax payer: • ***company income***: corporations (corporate tax); • ***income***: unincorporated businesses (income tax) • ***profit from the sale of an asset***: individuals (capital gains tax)	United Kingdom

[338] Ibid, 3.

[339] Ibid, 104.

[340] Ibid, 3.

[341] Ibid, 74.

[342] Ibid, 76.

[343] Ibid, 111.

[344] Scott D. Hughes, "Cryptocurrency Regulation and Enforcement in the U.S.," *Western State University Law Review* 45, 1 (2017): 10, http://www.scotthugheslaw.com/documents/CRYPTOCURRENCY-REGULATIONS-AND-ENFORCEMENT-IN-THE-US-2.pdf

Annex 4: Participants of cryptocurrency private legal relationships

Table 5: *Private actors of the cryptocurrency market*

Currency creators and other developers	Creator of a particular cryptocurrency may remain anonymous and may not participate in the further development of their creation (e.g. in Bitcoin case) or not hide their identity and continue on the cryptocurrency advancement (e.g. Ripple). The main arising problems in terms of liability are: • most of the cryptocurrencies have *an open-source code* and anyone can make a suggestion on the improvement of the software and make a contribution by writing a particular piece of code that will be adopted. Participants may remain unknown, hence, it is hard to hold someone liable for a program malfunction which may cause damage to the third parties. It is also hard to determine a persons' intention in the moment of a changes' suggestion and implementation of a new idea. • a *voting procedure* that determines which suggestion will be implemented and who will be working on it and an *evaluation procedure* of a particular suggestion. It means that the idea itself may be beneficial but implementation was poorly written or the already implemented idea was harmful from the beginning adoption of which is a result of an unthorough evaluation.
Miner	A separate special node (computer with appropriate software) in the network that contributes its computational to verify a transaction (create the next block). In the context of cloud mining, this term means an investor in a cloud mining contract.
Cryptocurrency owners (users)	"A natural person or legal entity who obtains coins to use them (i) to purchase real or virtual goods or services (from a set of specific merchants), (ii) to make P2P payments, or (iii) to hold them for investment purposes (i.e. in a speculative manner)"[345].
Cryptocurrency exchanges (centralized platforms)	Platforms designed for cryptocurrency transactions and they may provide other related services. In exchange, they charge users a trading fee (commission). They offer fiat-crypto and/or crypto-crypto transactions. The main difference from the P2P trading platform is that a centralized platform is run and controlled by an organization or other third party (e.g. Binance, Bittrex, Bitfinex, Kraken).
P2P (decentralized) trading platforms	These are marketplaces that bring together buyers and sellers: the buyer and seller place orders specifying proper price on cryptocurrency and the platform is supposed to match buyer and seller. There is no entity overlooking or controlling the platform (e.g. LocalBitcoins)[346].
Wallet providers	Private, public keys and address storage is called a ***cryptocurrency (digital) wallet***. "It performs various functions such as receiving and sending" cryptocurrency[347]. Some digital wallets can also generate key pairs. Wallet providers offer storage services.
Offerors of ICO	Companies (mainly startups) in order to raise funding launch an ICO. Investors in ICO receive a cryptocurrency token which is used to gain access to services or products that an ICO launcher offers or this token could be a representation of a stake in the company or project[348].
Investors in ICO	Persons who bought into the ICO

[345] Robby Houben and Alexander Snyers, "Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion," (Brussels: European Parliament, 2018): 25, https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

[346] Ibid, 27.

[347] Imran Bashir, *Mastering Blockchain* (Birmingham: Packt Publishing , 2017), 145.

[348] Jake Frankenfield, "Initial Coin Offering (ICO)," Investopedia. Accessed 4 March 2020, https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

LIST OF BIBLIOGRAPHY

Books

1. Ainsworth, Thomas. "Form vs. Matter." *Stanford Encyclopedia of Philosophy* (Spring 2016 Edition). Stanford: Metaphysics Research Lab, Stanford University, 2016. https://plato.stanford.edu/archives/spr2016/entries/form-matter/
2. Arslanian, Henri and Fabrice Fischer. *The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services*. Cham: Palgrave Macmillan, 2019.
3. Bar, Christian von, Ulrich Drobnig, and Guido Alpa, *The Interaction of Contract Law and Tort and Property Law in Europe: A Comparative Study*. Munich: Sellier European Law Publishers, 2004.
4. Barnes, Jeremy, Martin Beyersdorff, Mike Bonham, Linzi Carr, Rob Carrington, Victor Chan, Wei Li Chan, Larissa Connor, Pieter Dekker, Tim Denton, Dennis Deysel, Dennis Esterhuizen, Diego Fernandez, Alan Garry, Archie Groenewald, Prahalad Halgeri, Jane Hurworth, Ted Jones, Bernd Kremp, Sanjeev Kumar, Max Lienhard, Dean Lockhart, Sharon MacIntyre, Takahiro Makino, Amanda Marrion, Emily Moll, Richard Moore, Tina Patel, Michael Pratt, Tim Rogerson, Vadim Shelaginov, Anna Sirocka, David Stolker, Claire Taylor, Michael Varila, Tracey Waring, and Jane Watson, *International GAAP 2019* (Hoboken, NJ: John Wiley & Sons, Inc., 2019.
5. Bashir, Imran. *Mastering Blockchain*. Birmingham: Packt Publishing , 2017.
6. Burdick, William Livesey. *The Principles of Roman Law and Their Relation to Modern Law*. Clark, New Jersey: The Lawbook Exchange, Ltd., 2012.
7. Cartwright, John. *Misrepresentation, Mistake and Non-disclosure*. London: Sweet & Maxwell, 2012.
8. Chen-Wishart, Mindy, Alexander Loke, and Burton Ong. *Remedies for breach of contract*. Oxford, New York: Oxford University Press, 2016.
9. Chen-Wishart, Mindy. *Contract law*. Oxford: Oxford University Press, 2018.
10. Coeckelbergh, Mark. *Money Machines: Electronic Financial Technologies, Distancing, and Responsibility in Global Finance*. New York: Routledge, 2016.
11. Evans, Charles. *The Forensic Economist's Guide to Cryptocurrency*. Fort Lauderdale, FL: Pecuniology Press, 2019.
12. Feria, Rita de la, Stefan Vogenauer. *Prohibition of Abuse of Law: A New General Principle of EU Law?* Oxford : Hart Publishing, 2011.
13. Furneaux, Nick. *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence*. Indianapolis: Wiley Publishing, Inc., 2018.

14. Gans, Joshua, Stephen King, Jan Libich, Martin Byford, Gregory Mankiw, and Robin Stonecash. *Principles of Economics*. South Melbourne: Cengage Learning Australia, 2014.
15. Gwartney, James, Richard Stroup, Russell Sobel, and David Macpherson. *Economics: Private and Public Choice*. Mason: Cengage Learning, 2008.
16. Joshi, James, Surya Nepal, Qi Zhang, Liang-Jie, and Zhang Cham, *Blockchain – ICBC 2019: Second International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings*. Cham: Springer, 2019.
17. Lee, Wei-Meng. *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*. New York: Apress, 2019.
18. Madir, Jelena, ed. *FinTech Law and Regulation*. Cheltenham: Edward Elgar Publishing Limited, 2019.
19. Markesinis, Basil S., Hannes Unberath, and Angus Johnston. *The German Law of Contract: A Comparative Treatise*. Oxford: Hart Publishing, 2006.
20. McBride, Nicholas J, Roderick Bagshaw, "Breach of Statutory Duty." *Tort Law*. Harlow: Pearson Education Limited, 2018. https://books.google.com.ua/books?id=l71dDwAAQBAJ
21. Quiniou, Matthieu. *Blockchain: The Advent of Disintermediation*. London: UK ISTE, Hoboken, NJ: John Wiley & Sons, 2019.
22. *Regulation of cryptocurrency around the world.* Washington, DC: The Law Library of Congress, Global Legal Research Center, 2018. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf
23. Schlichter, Detlev S. Paper Money Collapse: *The Folly of Elastic Money*. Hoboken, NJ: John Wiley & Sons, 2014.
24. Schueffel, Patrick, Nikolaj Groeneweg, and Rico Baldegger. *The Crypto Encyclopedia: Coins, Tokens and Digital Assets from A to Z.* Bern: Growth Publisher, 2019. https://www.heg-fr.ch/media/lbdfnyd1/schueffelgroenewegbaldegger2019_crypto-encyclopedia_eng.pdf
25. Schuster, Ernest Joseph. *The Principles of German Civil Law*. Oxford: Clarendon Press, 1907. https://books.google.com.ua/books?id=wD8RAwAAQBAJ&hl=uk
26. Song, Jimmy. *Programming Bitcoin: Learn how to program Bitcoin from scratch*. Sebastopol, CA: O'Reilly, 2019.
27. Steele, Jenny. *Tort Law: Text, Cases, and Materials. Oxford*: Oxford University Press, 2017.

Journal articles

1. Angelo, Monica di, Alfred Soare, and Gernot Salzer. "Smart Contracts in View of the Civil Code." *SAC* '19 (2019). https://publik.tuwien.ac.at/files/publik_278278.pdf

2. Cong, Lin William and Zhiguo He. “Blockchain Disruption and Smart Contracts.” The Review of Financial Studies 35, 5 (2019): 1754–1797. https://doi.org/10.1093/rfs/hhz007
3. Cvetkova, Iryna. “Cryptocurrencies legal regulation.” *BRICS Law Journal* 5, 2 (2018): 63-81. https://www.researchgate.net/publication/326195399_Cryptocurrencies_legal_regulation
4. Dourado, Eli, and Jerry Brito. “Cryptocurrency.” *The New Palgrave Dictionary of Economics, Online Edition* (2014): 1-10. https://www.researchgate.net/publication/298792075_Cryptocurrency
5. Ershova, Inna, and Elena Trofimova. “Майнинг и предпринимательская деятельность: в поисках соотношения.” *Актуальные проблемы российского права* 103, 6 (July 2019): 73-82. https://cyberleninka.ru/article/n/mayning-i-predprinimatelskaya-deyatelnost-v-poiskah-sootnosheniya
6. Gordon, James D., “Defining a Common Enterprise in Investment Contracts” *Ohio State Law Journal* 72, 1 (2011): 59-94, https://kb.osu.edu/bitstream/handle/1811/71438/OSLJ_V72N1_0059.pdf
7. Hughes, Scott D. “Cryptocurrency Regulation and Enforcement in the U.S.” *Western State University Law Review* 45, 1 (2017): 1-28. http://www.scotthugheslaw.com/documents/CRYPTOCURRENCY-REGULATIONS-AND-ENFORCEMENT-IN-THE-US-2.pdf
8. Király, Miklós, “The Vienna Convention on International Sales of Goods and the Bitcoin,” *US-Chine Law Review* 16, 5 (2019): 179-188, https://www.davidpublisher.org/Public/uploads/Contribute/5d81db8d2160e.pdf
9. Krishnan R., Hari, Sai Saketh Y., and Venkata Tej Vaibhav M. “Cryptocurrency Mining – Transition to Cloud.” *International Journal of Advanced Computer Science and Applications* 6, 9 (2015): 115-124, https://www.researchgate.net/publication/283810104_Cryptocurrency_Mining_-_Transition_to_Cloud
10. Krishnan, Hari, Sai Saketh Y. Venkata Tej Vaibhav M. “Cryptocurrency Mining – Transition to Cloud” *International Journal of Advanced Computer Science and Applications* 6, 9 (2015): 115-124, https://thesai.org/Downloads/Volume6No9/Paper_15-Cryptocurrency_Mining_Transition_to_Cloud.pdf
11. Loi, Hio. “The Liquidity of Bitcoin.” *International Journal of Economics and Finance* 10, 1 (2018): 13-22 . https://www.researchgate.net/publication/321628021_The_Liquidity_of_Bitcoin
12. Lucas, Nicholas F. “Logic and Law” *Marquette Law Review* 3, 4 (1919): 203-210, https://pdfs.semanticscholar.org/f5dd/674b7aadffbfc05b18fafc89a1373df4cc0c.pdf

13. Martin, David A. “The Medium is not Money.” *Journal of Economic Issues (Association for Evolutionary Economics)* 6, 2/3 (1972): 67-74. http://web.a.ebscohost.com.skaitykla.mruni.eu/ehost/detail/detail?vid=13&sid=88792afb-84fd-4628-8423-86b4748a2c43%40sdc-v-sessmgr01&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=4725151&db=bth
14. Melnyk V. “Відшкодування шкоди, завданої правомірною поведінкою.” *Актуальні проблеми приватного права: матеріали наук.-практ. конф., присвяч. 94-й річниці з дня народж. В. П. Маслова*. Kharkiv: Право, 2016: 299–301. http://dspace.nlu.edu.ua/bitstream/123456789/12670/1/Melnyk.pdf
15. Mik, Eliza. “Smart contracts: Terminology, technical limitations and real world complexity” *Law, Innovation and Technology* 9, 2 (2017): 269-300. https://core.ac.uk/download/pdf/132698353.pdf
16. Rose, Chris, “The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution”. *International Business & Economics Research Journal (IBER)* 14, 4 (2015): 617-22. https://www.researchgate.net/publication/297750676_The_Evolution_Of_Digital_Currencies_Bitcoin_A_Cryptocurrency_Causing_A_Monetary_Revolution
17. Sandler, Darren J. “Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?” *Santa Clara High Technology Law Journal* 34, 3 (2018): 250-289, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1628&context=chtlj
18. Savelyev, Alexandr. “Contract law 2.0: “Smart”. Contracts as the beginning of the end of classic contract law.” *Information & Communications Technology Law* 26, 2 (2017): 116-134. https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1301036
19. Srokosz, Witold and Tomasz Kopyscianski. “Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability.” *Journal of Teaching and Education* 4, 2 (2015): 612-627, http://www.universitypublications.net/jte/0402/pdf/F5N180.pdf
20. Tjong Tjing Tai, Eric. “Force Majeure and Excuses in Smart Contracts” *European Review of Private Law* 6, 26 (2018): 787-804. https://pure.uvt.nl/ws/portalfiles/portal/28903834/Smart_contracts_excuses_ERPL_1_postprint.pdf
21. Wang, Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, Dong In Kim. "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks." *IEEE Access* 7 (2019): 22328-22370. https://arxiv.org/pdf/1805.02707.pdf

22. Zhang, Rui, Rui Xue, and Ling Liu. “Security and Privacy on Blockchain.” *ACM Computing Surveys* 52, 3, article 51 (July 2019): 1-34. https://arxiv.org/pdf/1903.07602.pdf

Dissertations and Theses

Shovkovyi, Vladyslav. “What Investment Opportunities Do Cryptocurrencies Provide?” Master thesis, Kyiv School of Economics, 2018. https://kse.ua/wp-content/uploads/2019/03/Vladyslav-Shovkovyi6.pdf.pdf

Conference papers

Pernice, Ingolf, Sebastian A. Henningsen, Roman Proskalovich, Martin Florian, Hermann W. Elendner, and Bjorn Scheuermann. “Monetary Stabilization in Cryptocurrencies – Design Approaches and Open Questions.” Paper presented at Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland, June 2019: 47-59. https://www.researchgate.net/publication/334995475_Monetary_Stabilization_in_Cryptocurrencies_-_Design_Approaches_and_Open_Questions

Szczerbowski, Jakub J. “Place of smart contracts in civil law. A few comments on form and interpretation.” Proceedings of the 12th Annual International Scientific Conference NEW TRENDS 2017 (Znojmo: Private College of Economic Studies Znojmo, 2017). https://ssrn.com/abstract=3095933

Working Papers, White Papers, and other Unpublished or Informally Published Works

1. Akgiray, Vedat, Blockchain Technology and Corporate Governance. Paris: OECD Publishing, 2019, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/CA/CG/RD(2018)1/REV1&docLanguage=En
2. Aydar, Mehmet, Salih Cemil CetinSerkan, Serkan Ayvaz, Betul Aygun. “Private Key Encryption and Recovery in Blockchain” (2019). https://www.researchgate.net/publication/334361184_Private_key_encryption_and_recovery_in_blockchain
3. Barakat, Mohamed, Christian Eder, and Timo Hanke. An Introduction to Cryptography. September 2018. https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf
4. Blumenfeld, Matthew, Michael Horn, Keaghan Ames, Nikhil Raina, Cesar Munoz, and Margaret Paulsen. “Regulatory Brief. Carving up crypto: Regulators begin to find their

footing." New York: PwC (2018). https://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/cryptocurrency.pdf

5. Boehm, Franziska and Paulina Pesch. "Bitcoin: A First Legal Analysis - With Reference to German and US-American Law." Financial Cryptography Workshops (2014). https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf
6. Bucha, David, Charlie Errington. Commodities demystified: A Guide to Trading and Global Supply Chain. Singapore: Trafigura Group, 2019. https://www.commoditiesdemystified.info/pdf/CommoditiesDemystified-en.pdf
7. Buterin, Vitalik. "Ethereum White Paper: A Next Generation Smart Contract & Decentralizes Application Platform" (2013). https://static1.squarespace.com/static/5793509acd0f6810d1242921/t/5abfb9cd575d1f2de635e7a5/1522514382746/Ethereum-ETH-whitepaper.pdf
8. Cryptocurrencies and blockchain. Europe and Central Asia Economic Update (May). Washington, D.C.: World Bank, 2018. http://documents.worldbank.org/curated/en/293821525702130886/pdf/Cryptocurrencies-and-blockchain.pdf
9. David Andolfatto. "A Model of Fiat Money." October 2008. http://www.sfu.ca/~dandolfa/olg2008.pdf
10. Digital currencies. Basel: Bank for International Settlements, November 2015. https://www.bis.org/cpmi/publ/d137.pdf
11. EBA Opinion on 'virtual currencies'. Paris: European Banking Authority, July 2014. https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1
12. FAFT Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks. Paris: Financial Action Task Force, June 2014. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
13. Goldberg, Dror. "Legal Tender." Working Papers. Ramat Gan: Bar-Ilan University, Department of Economics (2009). https://www.biu.ac.il/soc/ec/wp/2009-04.pdf
14. Goodell, Brandon, Sarang Noether, and Arthur Blue. "Compact linkable ring signatures and applications." Cryptology ePrint Archive. Report 2019/654 (2019). https://web.getmonero.org/resources/research-lab/pubs/MRL-0011.pdf
15. Goodrich, Mark, Hirra Tung. "Force Majeure: substantial damages even if you cannot perform. New York: White & Case LLP, July 2019.

https://www.whitecase.com/sites/default/files/2019-07/force-majeure-substantial-damages-even-if-you-cannot-perform.pdf

16. He, Dong, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes. IMF Staff Discussion Note. Virtual Currencies and Beyond: Initial Considerations. Washington, DC: International Monetary Fund, January 2016. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
17. Houben, Robby and Alexander Snyers. "Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion." Brussels: European Parliament, 2018. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
18. Institutionalization of cryptoassets. Amstelveen: KPMG, November 2018. https://assets.kpmg/content/dam/kpmg/us/pdf/2018/11/institutionalization-cryptoassets.pdf
19. Kcehowski, Rebekah B. "Consumer contracts Q&A: United States." Toronto: Thomson Reuters, 2017. https://www.jonesday.com/-/media/files/publications/2017/08/consumer-contracts-qa-united-states-thomas-reuters/files/consumer-contracts-qanda-united-states/fileattachment/consumer-contracts-qanda-united-states.pdf
20. Kultti, Klaus. A model for money as a store of value. Helsinki: Faculty of Social Sciences, Dep. of Economics, 2010. https://helda.helsinki.fi/bitstream/handle/10138/18007/amodelfo.pdf?sequence=1
21. Ledoit, Olivier, and Sébastien Lotz. The Coexistence of Commodity Money and Fiat Money. Zürich: University of Zurich, Department of Economics, 2011. http://www.econ.uzh.ch/static/wp/econwp024.pdf
22. Mana, Mehdi Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. Frankfurt am Main: European Central Bank, May 2019. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf
23. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. https://bitcoin.org/bitcoin.pdf
24. Natarajan, Harish, Solvej Karla Krause, and Helen Luskin Gradstein. Distributed Ledger Technology (DLT) and blockchain. Washington, D.C.: World Bank Group, 2017. http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
25. National Bank of Belgium. "A Stable Currency." Brussels: National Bank of Belgium, 2013. http://www.nbbmuseum.be/doc/chap5e.pdf

26. Okupski, Krzysztof. "Bitcoin Developer Reference" (2016). https://www.lopp.net/pdf/Bitcoin_Developer_Reference.pdf
27. Ripple. "Solution Overview." https://static1.squarespace.com/static/5793509acd0f6810d1242921/t/5abfba102b6a28a926f9250c/1522514455093/Ripple-XRP-whitepaper.pdf
28. Shirakawa, Rico, Jacinta Bernadette, and Upalat Korwatanasakul. "Cryptocurrency Regulations: Institutions and Financial Openness." ADBI Working Paper 978. Tokyo: Asian Development Bank Institute, 2019. https://www.adb.org/publications/cryptocurrency-regulations-institutions-financial-openness
29. Solli, Jami, Arthur Goujon, and Michael Gaweseb, "A guide to developing consumer protection law." London: Consumers International, 2011. http://www.fao.org/3/a-at346e.pdf
30. Szabo, Nick, "Smart Contracts," 1994, Accessed 15 March 2020 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
31. Trimborn, Simon, Mingyang Li, and Wolfgang K. Härdle. "Investing with cryptocurrencies - A liquidity constrained investment approach." Journal of Financial Econometrics, 2017. http://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2017-014.pdf
32. Virtual Currency Schemes – a further analysis. Frankfurt am Main: European Central Bank, February 2015. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
33. Virtual Currency Schemes. Frankfurt am Main: European Central Bank, 2012. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
34. "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective." New York: International Swaps and Derivatives Association, 2017. https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

Legal Documents and Case Law

1. Anns v. Merton London Borough Council [1978] AC 728. http://www.e-lawresources.co.uk/cases/Anns-v-Merton-London-Borough-Council.php
2. Bürgerliches Gesetzbuch (Vom 18. August 1896), Prof. Dr. Gerhard Köbler (Person Publikationen Projekte), Accessed 14 March 2020, http://www.koeblergerhard.de/Fontes/BGB/BGB1896_RGBl_S.195.htm
3. California Commercial Code. FindLaw. Accessed 16 February 2020 https://codes.findlaw.com/ca/commercial-code/com-sect-1201.html

4. Consumer Rights Act 2015, legislation.gov.uk, Accessed 9 March 2020, http://www.legislation.gov.uk/ukpga/2015/15/contents/enacted
5. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, EUR-Lex. Accessed 9 March 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0013
6. 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 (Text with EEA relevance). EUR- Lex. Accessed 4 February 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0110
7. Donoghue v. Stevenson [1932] UKHL 100 (26 May 1932). https://www.uni-trier.de/fileadmin/fb5/FFA/KURSUNTERLAGEN/Anglo-Amerikanisches_Recht/Law_of_Torts/Siry-SS-2012/Donoghue_v_Stevenson__1932__UKHL_100__26_May_1932_.pdf
8. Fabian v. LeMahieu [2019], CASE NO. 19-cv-00054-YGR. Order Granting in Part and Denying in Part Motion to Dismiss. https://casetext.com/case/fabian-v-lemahieu
9. German Civil Code. Bundesministerium der Justiz und für Verbraucherschutz. Accessed 14 March 2020. https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html
10. Gevorkyan v. Bitmain Inc. et al., Case 5:18-cv-07004, https://ru.scribd.com/document/393870365/Bitmain-Class-Action
11. Long v. Provide Commerce Inc. FindLaw. Accessed 9 March 2020. https://caselaw.findlaw.com/ca-court-of-appeal/1729412.html
12. 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). Intersoft Consulting. Accessed 6 April 2020. https://gdpr-info.eu
13. Singapore International Commercial Court of the Republic of Singapore. B2C2 Ltd v. Quoine Pte Ltd. SGHC(I) 03 (2019). https://www.sicc.gov.sg/docs/default-source/modules-document/judgments/b2c2-ltd-v-quoine-pte-ltd_a1cd5e6e-288e-44ce-b91d-7b273541b86a_8de9f2e2-478e-46aa-b48f-de469e5390e7.pdf
14. Terpin v. AT&T Mobility, LLC [2019]. Order Granting, in Part, and Denying in Part, Defendant's Motion to Dismiss[14]; And Denying Defendant's Motion to Strike [15]. https://www.leagle.com/decision/infdco20190722561
15. The Currency Act. Singapore Statutes Online. Accessed 16 February 2020. https://sso.agc.gov.sg/Act/CA1967

16. The Unfair Terms in Consumer Contracts Regulations 1999, legislation.gov.uk, Accessed 9 March 2020, http://www.legislation.gov.uk/uksi/1999/2083/contents/made
17. UNIDROIT International Institute for the Unification of Private Law. Rome: International Institute for the Unification of Private Law, 2016. https://www.unidroit.org/english/principles/contracts/principles2016/principles2016-e.pdf
18. United Nations Convention on Contracts for the International Sale of Goods. New York: United Nations, 2010. https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf
19. Zakinov Et al v. Ripple Labs [2020]. Motion to Appoint Lead Plaintiff and Lead Counsel. 1, Accessed 5 April 2020, https://www.docketbird.com/court-documents/Zakinov-Et-al-v-Ripple-Labs-Inc-et-al/OPPOSITION-RESPONSE-re-36-MOTION-to-Appoint-Lead-Plaintiff-and-Lead-Counsel-filed-by-Bradley-Sostack/cand-4:2018-cv-06753-00050
20. Zakinov Et al v. Ripple Labs [2020]. Case 4:18-cv-06753-PJH. http://securities.stanford.edu/filings-documents/1066/RLI00_01/2020226_r01x_18CV06753.pdf
21. Цивільний кодекс України, в редакції від 13.02.2020, Законодавство України, Accessed 14 March 2020 https://zakon.rada.gov.ua/laws/show/435-15

Websites

1. Ascienzo, David. “Cryptocurrency CFPB Complaints Rise as Prices Fall.” ValuePenguin. Accessed 6 April 2020. https://www.valuepenguin.com/cfpb-complaints-about-cryptocurrencies
2. Berger, Klaus Peter. “The Lex Mercatoria (Old and New) and the TransLex-Principles.” Trans-Lex. Accessed 14 March 2020, https://www.trans-lex.org/400200
3. Biggs, Jack. “Introduction to Digital Currency.” bookdown.org. 2018. Accessed 11 February 2020. https://bookdown.org/Jack_Biggs/Cryptocurrency/what-is-digital-currency.html
4. Canellis, David. “Cryptocurrency-related lawsuits are mooning, up 300% from last year.” TNW. Accessed 4 April 2020. https://thenextweb.com/hardfork/2018/11/20/cryptocurrency-lawsuits-moon/
5. Cavicchioli, Marco. “Ripple: Who owns the most XRP?” Accessed 20 February 2020. https://en.cryptonomist.ch/2020/01/25/ripple-who-owns-the-most-xrp/
6. Chan, Jason. “S. Korean cryptocurrency exchanges take responsibility for losses from hacks.” Asia Crypto Today. Accessed 9 March 2020. https://www.asiacryptotoday.com/s-korean-cryptocurrency-exchanges-take-responsibility-for-losses-from-hacks

7. Chen, James. "Algorithmic Trading." Investopedia. Accessed 10 March 2020. https://www.investopedia.com/terms/a/algorithmictrading.asp

8. Chen, James. "Commodity." Investopedia. Accessed 19 February 2020. https://www.investopedia.com/terms/c/commodity.asp

9. Chen, James. "Consumer Price Index – CPI." Investopedia. Accessed 10 February 2020. https://www.investopedia.com/terms/c/consumerpriceindex.asp

10. Drbyos. "Simultaneous class action lawsuits filed against 11 bitcoin companies." World Today News. Accessed 5 April 2020. https://world-today-news.com/simultaneous-class-action-lawsuits-filed-against-11-bitcoin-companies/

11. Fawkes, Jeff. "Lawsuits Filed against Binance, Block.one, BitMEX and Other Crypto-Related Companies." Coinspeaker. Accessed 5 April 2020. https://www.coinspeaker.com/lawsuits-filed-binance-bitmex-block/

12. Frankenfield, Jake, "Initial Coin Offering (ICO)," Investopedia. Accessed 4 March 2020, https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

13. Hayes, Adam. "Purchasing Power." Investopedia. Accessed 10 February 2020. https://www.investopedia.com/terms/p/purchasingpower.asp

14. Helms, Kevin. "US Lawmaker Introduces Crypto-Currency Act of 2020 While Under Coronavirus Quarantine." Bitcoin.com. Accessed 6 April 2020. https://news.bitcoin.com/cryptocurrency-act-of-2020/

15. Herold, Thomas. "What is Commodity Money?" Herold Financial Dictionary. Accessed 10 February 2020. https://www.financial-dictionary.info/terms/commodity-money/

16. Huillet, Marie. "Binance Launches P2P Trading for Chinese Yuan." Cointelegraph. Accessed 3 February 2020. https://cointelegraph.com/news/binance-launches-p2p-trading-for-chinese-yuan

17. Idjeri, Anaëlle, "Reform of French contract law – Ratification Law published on April 21, 2018: Main changes impacting business law," Soulier Avocats, Accessed 14 March 2020, https://www.soulier-avocats.com/en/reform-of-french-contract-law-ratification-law-published-on-april-21-2018-main-changes-impacting-business-law/

18. Jamie, Elizabeth, "No Worries: Bithumb will Reimburse Lost Money of Users," BTCNN.com, Accessed 9 March 2020, https://www.btcnn.com/no-worries-bithumb-will-reimburse-lost-money-of-users/

19. Kluchenek, Matthew F. "The Status of Environmental Commodities Under the Commodity Exchange Act." Harvard Business Law Review. Accessed 19 February 2020. https://www.hblr.org/2015/01/the-status-of-environmental-commodities-under-the-commodity-exchange-act/

20. Legal Commentary on the article 1166 of the Civil Code of Ukraine. ННП Юрисконсульт. Accessed 3 April 2020. https://legalexpert.in.ua/komkodeks/gk/79-gk/1533-1166.html

21. Lim Pui Sze, Amanda. "Functions and Characteristics of Money." UK Essays. Accessed 13 February 2020. https://www.ukessays.com/essays/economics/functions-characteristics-money-6335.php?vref=1

22. Litecoin Project." GitHub. Accessed 20 February 2020. https://github.com/litecoin-project

23. Main. Antpool. Accessed 8 March 2020. https://v3.antpool.com/home

24. Main. BTC.com. Accessed 8 March 2020. https://pool.btc.com/?_ga=2.106616384.279728806.1583883976-291678957.1583883976

25. Main. GitHub. Accessed 1 April 2020. https://github.com

26. McCormick, Jamie. "Eligius Bitcoin Mining Pool Review." Bitcoins In Ireland. Accessed 7 March 2020. https://bitcoinsinireland.com/eligius-bitcoin-mining-pool-review/

27. Monero Forum. Monero. Accessed 22 February 2020. https://forum.getmonero.org/6/ideas

28. Nicolosi, Phil, "When Is A Website Disclaimer Effective?" Phil Nicolosi Law, P.C. (Blog). Accessed 9 March 2020. https://www.internetlegalattorney.com/when-is-website-disclaimer-effective/

29. Price, Rob, "Fiat currency doesn't store value: Investor shares advice on where we can store our value." IOL. Accessed 10 February 2020. https://www.iol.co.za/business-report/opinion/fiat-currency-doesnt-store-value-investor-shares-advice-on-where-we-can-store-our-value-32713407

30. Pui Sze, Amanda Lim. "Functions and Characteristics of Money." UK Essays. Accessed 13 February 2020. https://www.ukessays.com/essays/economics/functions-characteristics-money-6335.php?vref=1

31. Redman, Jamie, "New York Judge Classifies Bitcoin As Money." Bitcoin.com. Accessed 24 February 2020. https://news.bitcoin.com/judge-classifies-bitcoin-money/

32. Reed, Eric. "Equity Tokens vs. Security Tokens: What's the Difference?" Bitcoin Market Journal. Accessed 28 February 2020. https://www.bitcoinmarketjournal.com/equity-token/

33. Rodriguez, Jesus, "The Middleman of Trust: The Oracle Paradox and Five Protocols that can Bring External Data into the…" Hackernoon, , Accessed 18 March 2020, https://hackernoon.com/the-middleman-of-trust-the-oracle-paradox-and-five-protocols-that-can-bring-external-data-into-the-df39b63e92ae

34. Rogers, Craig, Wendy Boucrot, Michael Bahar, "Is a cyber-attack "Force Majeure"? Je ne crois pas!" Lexology. Accessed 8 March 2020. https://www.lexology.com/library/detail.aspx?g=9f8784de-aa99-4eed-ab92-79a3353582bf

35. Rosenstein, Philip. "Investors Allege Ripple CEO Dumped XRP While Touting It." Law360. Accessed 5 April 2020. https://www.law360.com/articles/1257526

36. Sanitt, Adam, "Smart Contracts," Norton Rose Fulbright, Accessed 18 March 2020 https://www.nortonrosefulbright.com/en/knowledge/publications/1bcdc200/smart-contracts

37. Schwartz, Davis. "The Inherently Decentralized Nature of XRP Ledger." Ripple. Accessed 20 February 2020. https://ripple.com/insights/the-inherently-decentralized-nature-of-xrp-ledger/

38. Sedgwick, Kai. "Bitcoin History Part 10: The 184 Billion BTC Bug." Bitcoin.com. Accessed 14 March 2020. https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/

39. Shultz, Suzette. "Three Countries in Hyperinflation." The Borgen Project. Accessed 13 February 2020. https://borgenproject.org/three-countries-in-hyperinflation/

40. Sizov Anton, Igor Losev, Vitaliy Voronov, Dmitriy Makarov, Elena Karpina. "Лучшие пулы для майнинга криптовалюты на 2020 год." Майниг Криптовалюты. Accessed 8 March 2020, https://mining-cryptocurrency.ru/luchshie-puly-dlya-majninga/

41. Sotelo, Nicole, "German Civil Code (Bürgerliches Gesetzbuch, BGB) (1900)." Towards Emancipation? Accessed 14 March 2020. http://hist259.web.unc.edu/german-civil-code-burgerliches-gesetzbuch-bgb-1900/

42. Szabo, Nick. "Formalizing and Securing Relationships on Public Networks." Satoshi Nakamoto Institute. Accessed 18 March 2020. https://nakamotoinstitute.org/formalizing-securing-relationships/

43. Szkudlarek, Anna. "Cryptocurrency taxes – CRS/FATA: Do you need to disclose your cryptocurrencies?" KENDRIS. Accessed 4 April 2020. https://www.kendris.com/en/blog/crs-fatca-do-you-need-disclose-your-cryptocurrencies

44. Tassev, Lubomir. "In the Daily: Liberstad Coin, Mining Contracts, Luxembourg Law." Bitcoin.com. Accessed 9 March 2020. https://news.bitcoin.com/in-the-daily-liberstad-coin-mining-contracts-luxembourg-law/

45. Taylor, Allen. "David Chaum: Godfather of Digital Currency." Blockchain Times. Accessed 4 February 2020. https://blockchaintimes.news/2018/10/19/david-chaum-godfather-of-digital-currency/

46. Yovel, Jonathan. "Comparison between provisions of the CISG (Seller's Right to Remedy Failure to Perform: Article 48) and the counterpart provisions of the PECL (Articles 8:104 and 9:303)" (March 2005), Accessed 15 March 2020 http://cisgw3.law.pace.edu/cisg/text/peclcomp48.html

47. Zmudzinski, Adrian. "Lawsuit Alleging Ripple's XRP Is Unregistered Security Moves Forward." Cointelegraph. Accessed 5 April 2020. https://cointelegraph.com/news/lawsuit-alleging-ripples-xrp-is-unregistered-security-moves-forward
48. "An Employer's Liability for Employee's Acts." FindLaw. Accessed 1 April 2020. https://smallbusiness.findlaw.com/liability-and-insurance/an-employer-s-liability-for-employee-s-acts.html
49. "Antpool User Service Agreement," Antpool, Accessed 8 March 2020. https://v3.antpool.com/copyRight1
50. "Binance Adds Peer-to-Peer (P2P) Trading for Vietnamese Dong (VND)." Binance. Accessed 3 February 2020. https://www.binance.com/en/blog/421499824684900366/Binance-Adds-PeertoPeer-P2P-Trading-for-Vietnamese-Dong-VND-
51. "Bitpenny Closes Indefinitely." Bitcoin Miner. Accessed 7 March 2020. http://www.bitcoinminer.com/bitpenny-closes-indefinitely/
52. "crypto-." Online Etymology Dictionary. Accessed 7 February 2020. https://www.etymonline.com/word/crypto-
53. "Cryptocurrency and Bitcoin Liquidity". Kraken. Accessed 16 February 2020. https://www.kraken.com/features/liquidity
54. "Cryptocurrency exchanges change their terms of service: FTC." Yonhap News Agency. Accessed 9 March 2020. https://en.yna.co.kr/view/AEN20190617005300320?section=search
55. "Cryptocurrency Regulations Around The World." ComplyAdvantage. Accessed 24 February 2020. https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/
56. "Cypherpunk definition." SearchSecurity.com. Accessed 12 February 2020. https://searchsecurity.techtarget.com/definition/cypherpunk
57. "Duty of Care Lecture." LawTeacher.net. Accessed 1 April 2020. https://www.lawteacher.net/modules/tort-law/negligence/duty-of-care/lecture.php
58. "Electronic Money." European Central Bank. Accessed 4 February 2020. https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html
59. "FAQ." Monero. Accessed 22 February 2020. https://web.getmonero.org/get-started/faq/
60. "Frequently Asked Questions," Bitcoin, Accessed 12 February 2020 https://bitcoin.org/en/faq
61. "Frequently Asked Questions." Ripple. Accessed 20 February 2020, https://ripple.com/faq
62. "General Terms and Conditions." Slush Pool. Accessed 8 March 2020. https://slushpool.com/about/tos/

63. "Hashrate Distribution: An estimation of hashrate distribution amongst the largest mining pools." BLOCKCHAIN. Accessed 8 March 2020. https://www.blockchain.com/en/pools

64. "How do I pay with Bitcoin?" Overstock. Accessed 17 February 2020. https://help.overstock.com/help/s/article/Bitcoin

65. "How to use Bitcoin to add money to your Microsoft account". Microsoft. Accessed 17 February 2020. https://support.microsoft.com/en-us/help/13942/microsoft-account-how-to-use-bitcoin-to-add-money-to-your-account

66. "KFC Canada Is Accepting Bitcoin for Fried Chicken." Coindesk. Accessed 17 February 2020. https://www.coindesk.com/kfc-canada-is-accepting-bitcoin-for-fried-chicken

67. "Main Page: Everything about Litecoin." Litecoin.info. Accessed 22 February 2020. https://litecoin.info/index.php/Main_Page

68. "Main." Tether. Accessed 29 February 2020. http://tether.to/

69. "Majority of Cryptocurrencies Can Be Classified as Centralized, Securities." NewsBTC. Accessed 3 February 2020. https://www.newsbtc.com/2018/10/17/centralized-cryptocurrencies-dominate-market-but-what-about-bitcoin/

70. "MiFID II, Crypto Assets and the Cryptocurrency Market." eflow. Accessed 4 April 2020. https://eflowglobal.com/2019/06/17/mifid-ii-crypto-assets-and-the-cryptocurrency-market/

71. "Proof of Stake (PoS)." EthHub. Accessed 20 February 2020. https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/

72. "Riot Games® Terms of Service". Riot Games. Accessed 11 February 2020. https://www.riotgames.com/en/terms-of-service

73. "System." Meriam Webster dictionary. Accessed 11 February 2020. https://www.merriam-webster.com/dictionary/system

74. "Technical Specs." Monero. Accessed 22 February 2020. https://web.getmonero.org/technical-specs/https://forum.getmonero.org/6/ideas

75. "The Complete Guide to Monero Cryptocurrency." BitDegree. Accessed 22 February 2020. https://www.bitdegree.org/tutorials/monero/#The_Advantages_and_Disadvantages_of_Monero

76. "Tidal Wave of Lawsuits Accuse Bitcoin (BTC) and Crypto Companies of Selling Unregistered Securities." The Dayly Hodl. Accessed 5 April 2020. https://dailyhodl.com/2020/04/05/tidal-wave-of-lawsuits-accuse-bitcoin-btc-and-crypto-companies-of-selling-unregistered-securities/

77. "Top 100 Cryptocurrencies by Market Capitalization." CoinMarketCap. Accessed 20 February 2020. https://coinmarketcap.com/

78. “What is API: Definition, Types, Specifications, Documentation.” AltexSoft. Accessed 1 April 2020. https://www.altexsoft.com/blog/engineering/what-is-api-definition-types-specifications-documentation/

79. “What is Ether?” EthHub. Accessed 20 February 2020. https://docs.ethhub.io/ethereum-basics/what-is-ether/

80. “What is Ethereum?” EthHub. Accessed 20 February 2020. https://docs.ethhub.io/ethereum-basics/what-is-ethereum/

81. “What is Litecoin?” Litecoin, Accessed 20 February 2020, https://litecoin.org/

82. “XRP.” XRP Ledger. Accessed 20 February 2020. https://xrpl.org/xrp.html

83. “Пулы для майнинга — самые прибыльные пулы в 2020.” Coinpost. Accessed 7 March 2020. https://coinpost.ru/p/pul-dlya-majninga-samye-pribylnye-puly-v-2019-godu#loc-20

84. “Условия использования.” 2Miners. Accessed 8 March 2020. https://2miners.com/ru/terms

ABSTRACT

Cryptocurrencies and distributed ledger technology became a revolutionary and insightful phenomenon that provide benefits of decentralized payment system, quasi- or complete anonymity, and lower transaction fees for cryptocurrency users. Despite all the advantages, the crypto domain also imposes challenges on the market participants. The long-lasting status quo of governments and their refusal to quickly clarify the rights and obligations of cryptocurrency service providers and offerors of crypto-related contracts has given rise to uncertainty on civil liability issues in the crypto sphere. Thus, many private actors – companies and users – are suffering from financial losses.

The thesis intends to outline the main pitfalls in contractual cryptocurrency relations and provide clarification of possible liability issues that may occur. The research refers to findings in the relevant case law as well as gives an overview of legal provisions found in national legislation, regional and international frameworks that might help to eliminate the uncertainty of contractual liability.

The question of the tortious liability has been raised in the thesis. In particular, cryptocurrency platforms and programmers' duty of care, as well as its breach, may lead to civil claims regarding the tort of negligence. The possible breach of statutory by crypto companies and developers has been also explored in the work. The purpose of all information provided by the thesis is to safeguard private actors' interests, prevent damages in the future, and propose solutions that will alleviate existing risks in the cryptocurrency domain.

Keywords: blockchain, civil liability, contractual liability, cryptocurrency, tortious liability.

SUMMARY

The Thesis is dedicated to the 'Theoretical and Legal Perspective of Civil Liability in Cryptocurrency Relations.' The research aims to analyze in isolation contractual and non-contractual (tortious) liability issues arising in the cryptocurrency sphere. The common law system, as well as the continental law system, approaches towards civil liability are explored in the work. The Thesis includes some thoughts on possible solutions that might prevent unfair business practices that abnormally flourish in the cryptocurrency domain.

The Thesis consists of general and special parts. The first chapter aims to explore the nature of cryptocurrencies, to discover specifics of its machinery, and to give a final and unambiguous definition of the term 'cryptocurrency.' This chapter answers the important and significant question the answer on which may distort some business models: is cryptocurrency money or commodity? Additionally, this chapter provides clarification of the terms needed to understand the specifics of cryptocurrency relations. The next part's purpose is to familiarize the reader with different states' approaches towards cryptocurrency regulation. The graphical result of data analysis is three tables provided in the Annexes' section.

The second chapter opens the special part and is dedicated to contractual liability in the crypto sphere. In particular, it gives an evaluation of various service agreements offered by crypto companies to their users and outlines the main danger clauses that shift the balance of interests towards the business actors. The chapter also explores crypto mining contracts, including cloud mining contracts, and lays out contracts' main features. The second part of the chapters describes the phenomenon of smart contracts.

The last chapter contextualizes tortious liability in the cryptocurrency domain from the common and the continental law perspective. As a benchmark for comparative analysis, the case law of the US, and the UK as common law counties and Ukrainian legislation as a state of civil law tradition are used. The tort of negligence and the breach of statutory duty in the cryptocurrency relations are explored.

At the end of the Thesis, some thoughts and recommendations on safeguarding private interests of cryptocurrency actors, the possible future, and the better application of existing provisions on civil liability are provided.

HONESTY DECALARATION

25/04/2020
Vilnius

I, _Iryna Arkhypchenko,____, student of
(name, surname)

Mykolas Romeris University (hereinafter referred to University),
Mykolas Romeris Law School, the Institute of Private Law, Private Law
(Faculty /Institute, Programme title)

confirm that the Master thesis titled

"THEORETICAL AND LEGAL PERSPECTIVE OF CIVIL LIABILITY IN CRYPTOCURRENCY RELATIONS":

1. Is carried out independently and honestly;
2. Was not presented and defended in another educational institution in Lithuania or abroad;
3. Was written in respect of the academic integrity and after becoming acquainted with methodological guidelines for thesis preparation.

I am informed of the fact that student can be expelled from the University for the breach of the fair competition principle, plagiarism, corresponding to the breach of the academic ethics.

_______________ Iryna Arkhypchenko
(signature) *(name, surname)*