Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 51

Blockchain Technology Regulatory Standards in the EU and U.S.: Smooth Sailing, or Iceberg Ahead?

Nikolaos I. Theodorakis

2020

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Nikolaos Theodorakis is Of Counsel in the Brussels office of Wilson Sonsini Goodrich & Rosati, where his practice focuses on privacy and cybersecurity. Nikolaos regularly counsels on matters of EU data protection law, GDPR compliance, cybersecurity preparedness, advertising, and marketing, and offers a full cycle of services that includes both non-contentious matters and investigations with supervisory authorities.
Nikolaos represents multinational companies across a wide range of industries, including technology, financial services, healthcare, hospitality, food and beverage, insurance, pharmaceuticals, chemicals, and automotive. He also works with start-ups and established companies in the EMEA region, and, in particular, Greece and Cyprus.
Having advised on a broad spectrum of corporate matters, Nikolaos has developed an expert insight into the increasing interplay between data protection, financial services (PSD2), competition law, and international trade law. He is at the forefront of advising on emerging privacy challenges on matters of AI, biotech, fintech, and blockchain.
In addition, Nikolaos is an associate professor of law and fellow at the University of Oxford. He holds an LLB from the University of Athens, an MPhil from the University of Cambridge, an LLM from University College London, and a PhD from the University of Cambridge. Previously, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. He also gained professional experience at the U.S. Committee on Capital Markets Regulation, the Kluge Center at the U.S. Library of Congress, and the UK Ministry of Justice.
Nikolaos has received awards from several bodies, including the State Council of the People's Republic of China, Economic and Social Research Council (ESRC), British Academy, and the Greek Parliament. He has been widely published and frequently receives invitations for public engagements, including guest lectures across the world, international symposia, and TEDx conferences.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Nikolaos I. Theodorakis, Blockchain Technology Regulatory Standards in the EU and the U.S.: Smooth Sailing, or Iceberg Ahead?, Stanford-Vienna TTLF Working Paper No. 51, http://ttlf.stanford.edu.

Copyright

Abstract

Blockchain is a distributed ledger technology that comes with several uses that can revolutionize our daily life. For instance, governments can take advantage of blockchain to issue IDs that cannot be replicated, or can monitor taxation reporting in a unique and transparent way. Insurance companies can utilize automatic execution of contracts, financial bodies can secure money and financial asset transfers in a matter of seconds, and the intellectual property sector can distribute and manage IP rights pertinent to music, videos or other protected content.
Despite the multiple benefits of blockchain, and its use in cryptocurrencies, this technology comes with a number of drawbacks. Both EU and US regulators have raised concerns regarding the legal status of blockchain applications in different sectors (e.g. whether cryptocurrencies should be considered a currency or a property asset). This paper will discuss in detail how blockchain works and its main uses. It will then explore how the EU and the US intend to regulate blockchain, using cryptocurrencies as a case study. The paper will conclude with a discussion regarding the future uses of cryptocurrency and whether blockchain applications can co-exist with more traditional legal sectors (e.g. data protection law, IP law, contract law etc).

Keywords

Blockchain technology; cryptocurrencies; bitcoin; connected devices; privacy.

Table Of Contents

1. Introduction

We have recently witnessed a significant rise in the popularity of cryptocurrencies in the digital finance era. Traditional currencies are based on banks and governments to establish their credibility on the stability of the government and said government's financial policy. Bitcoin is probably the most known example of a cryptocurrency- however, a bit less is known about its underlying technology: the blockchain. It is important to clarify from the outset, and to avoid any confusion to the readers, that bitcoin is just an application that resides on top of a technological infrastructure, which is the blockchain. Therefore, Bitcoin and blockchain are not synonymous as there can be many different implementations of blockchain as a trust system and the bitcoin implementation of blockchain is and will be different than others.

This paper will explore the nature of blockchain and its underlying technology. It will then discuss the main uses that this new technology can have in real life, apart from the already known function regarding cryptocurrencies. It will move on to discuss regulatory efforts in the EU and the US, using Bitcoin as the real-life example of blockchain regulation. Be it that the applications of blockchain are numerous, Bitcoin is the most far-reaching and mainstream for the time being. This has, naturally, attracted the attention of regulators in both sides of the Atlantic. Through examining the example of Bitcoin, we will extrapolate on the maturity of blockchain technology, and try to predict what the future will bring.

2. What is blockchain?

A blockchain is a digital concept to store data- a diary that is almost impossible to forge. As its name suggests, blockchain consists of multiple blocks strung together. When a block stores new data it is added to the blockchain.

The data is coming in blocks of digital data- they are chained together, which practically makes the data immutable since it can never be changed again. This technology allows us to keep track records of anything we attribute value to without the risk of someone tampering with these records. For instance, if purchaser A buys a car and adds a photograph of the property rights to a blockchain, he will always be able to prove that he owned the car at that point. Nobody will be able to forge this information and claim that they own the car instead of the purchaser- this transactional consistency and safety, in a world of uncertainty, is truly revolutionary.[1]

Blockchain creates stability and offers almost complete anonymity to its users. Every time a new transaction is to be authorized, every node connected in the network validates said

[1] Tama, B.A., Kweka, B.J., Park, Y., Rhee, K.-H., 2017. A critical review of blockchain and its current applications, in: Electrical Engineering and Computer Science (ICECOS), 2017 International Conference On. IEEE, pp. 109–113. https://doi.org/10.1109/ICECOS.2017.8167115

transaction. A block is then created and added to the chain (ergo "blockchain"), which forms part of the public ledger.[2] The public ledger therefore solves the problem of trust: when we deal with a stranger, we cannot always trust them, whereas a contract is not always an optimal solution due to the hassle it requires and the unmitigated chance of resorting to a trial if a dispute arises. The blockchain offers a third option, apart from trust or contract that may not be optimal, which is secure, quick and cheap.

Blockchain provides significant security since the only way to tamper with a transaction is to hack the majority of the computers connected to this decentralized network.[3] The security and robustness of blockchain's architecture is what makes it attractive to financial institutions that try to benefit from its sophisticated nature.[4] Many other sectors have also expressed an interest in blockchain technology (e.g. academic institutions to validate degrees and educational certificates, hospitals to validate medical record, individuals who want to enter into smart contracts, governments to validate property records or passports etc.).

3. How does the blockchain work?

Blockchain is therefore a type of diary or spreadsheet that contains information about transactions. Each transaction generates a hash, which is a string of numbers and letters. Transactions are then entered in the order in which they occurred and the hash depends not only on the transaction but the previous transaction's hash. The majority of the nodes need to approve the transaction in order to write it into a block, and each block is chained to all the previous ones, creating an immutable chain. Blockchain is spread over several computers in the network, each of which have a copy of the blockchain- the computers are called nodes and

[2] Blockchain has also been defined as "*An incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value*.", in Don and Alex Tapscott, Blockchain Revolution (2016).
[3] Also known as "51% attack"
[4] Raval, S., 2016. Decentralized applications: harnessing Bitcoin's blockchain technology, p.15, O'Reilly, Beijing.

the blockchain registry updates itself every 10 minutes, which makes it very efficient and timely.[5]

But how does blockchain work in practice?

Blockchain is an amalgamation of several different existing technologies. While these technologies are not new, it is the way they are combined and applied that brought about blockchain. The component technologies are:

- Private key cryptography
- A distributed network that includes a shared ledger
- Means of accounting for the transactions and records related to the network

But how do cryptographic keys work? Let's take the example of A and B, wanting to conduct a transaction online. Each of them holds two keys: one is private, and one is public. By combining the public and private keys, cryptography allows individuals to generate a secure digital identity reference point. This secure identity is a major component of blockchain technology. Together they generate a digital signature, which is used to certify and control ownership.[6]

The digital signature element is then combined with the distributed network technology component. Blockchain technology acts as a large network of individuals who are validators to reach a consensus about various transactions. A mathematical verification is then used to secure the network, and blockchain allows for new types of digital interactions.

[5] Wang, H., Chen, K., Xu, D., 2016. A maturity model for blockchain adoption. Financial Innovation 2, 1–5. https://doi.org/10.1186/s40854-016-0031-z

[6] Yuan, Y., Wang, F.-Y., 2018. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. Systems, Man, and Cybernetics: Systems, IEEE Transactions on 48, 1421–1428. https://doi.org/10.1109/TSMC.2018.2854904

An important aspect of blockchain technology is how it confirms and validates transactions.[7] For example, when two individuals wish to conduct a transaction online, each with a private and a public key, the blockchain allows A to use their private key to attach information regarding the transaction to the public key of B. Together, this information forms a block which contains a digital signature as well as a timestamp and other relevant information about the transaction, but not the identities of the individuals involved in that transaction, since this information is pseudonymized. That block is then transmitted across the blockchain network to all of the nodes, or other component parts of the network, which will then act as validators for the transaction.[8]

In order for a block to be added to the blockchain, therefore, four things must happen:

1. A transaction must occur (e.g. an individual makes an online purchase);

2. That transaction must be verified (the network of computers connected to blockchain checks that the transaction is valid, confirms the details and time of purchase, amount due and delivery details);

3. That transaction must be stored in a block (once the agreement is validated, the transaction's dollar amount, the digital signature and the vendor's digital signature are all stored in a block). The transaction then joins thousands of others that are also validated;

4. That block must be given a hash (a unique identifying code). Once hashed, the block can be added to the blockchain. When that new block is added to the blockchain, it becomes publicly available for anyone to view.

[7] Nowiński, W., Kozma, M., 2017. How Can Blockchain Technology Disrupt Existing Business Models? Entrepreneurial Business and Economics Review 5, 173–188. https://doi.org/10.15678/EBER.2017.050309

[8] Underwood, S., 2016. Blockchain beyond bitcoin. Communications of the ACM 59, 15–17. https://doi.org/10.1145/2994581

For the above to materialize, it takes huge amounts of computing power since several computers are required to dedicate their computing power towards this endeavor and "mine" the block. The process of mining, and the reward associated with it, solves the problem of computational power. Mining is related to the economic issue of the "tragedy of the commons" which dictates that an incentive is required in cases where users are driven only by self-interest. Put simply, mining incentivizes individuals to dedicate their computational power (which is the labor) in order to earn a small amount of cryptocurrency (which is the reward).

Validation of each transaction is crucial to avoid double-spending. Blockchain networks need to ensure that cryptocurrencies are uniquely owned and imbued with value. The way validation works is that the nodes within the blockchain network act as components of the ledger system, maintaining a history of transactions for each coin in that network by working to solve complicated mathematical problems (riddles). The nodes confirm or reject blocks that contain information about transaction. The majority of node operator needs to arrive at the same solution to the problem in order for a block to be confirmed and added to the chain of blocks.[9]

The majority of computers connected to the network would need to be hacked for a transaction to be forged, which is why we posit that blockchain is unlikely to forge. Let's consider the following example: a corrupt miner has altered a block of transactions and is trying to recalibrate signatures for the subsequent blocks in order to have the rest of the network accept his change. However, at the same time the rest of the network is also calculating new signatures for the new blocks, which means that the corrupt miner will also have to calculate new signatures for these blocks that are being added to the end of the chain. He therefore needs to keep all of the blocks linked, which means that unless the miner has more computational power than the rest of the network combined, he will never catch up with the rest of the network

[9] Prusty, N., 2018. Blockchain for Enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features, pp. 25-40. Packt Publishing, Birmingham.

finding signatures. The reasonable assumption that a single bad actor will never have more computational power than the rest of the network combined is what makes the blockchain immutable.[10]

In theory, a 51% attack (i.e. an attack of a bad actor with more computational power than the rest of the network combined) is plausible, and in fact it has happened on various blockchains in the past. In major blockchain platforms however, like the Bitcoin, such an attack would be far more costly to execute than it would yield in return.[11] This is why the more users participate in the mining process, the more secure a blockchain becomes.

The overall structure of blockchain follows a governance of democracy and therefore updates its record of transactions according to what the majority of its users support. The blockchain protocol does this by always following the record of the longest blockchain because it assumes that this chain is represented by the majority.

4. The applications of blockchain

The use of blockchain technology has remarkable benefits since users have complete control of the value they own and there is no third party that holds their value or can limit their access to it.[12] Further, the cost of using blockchain is quite low, which allows for micropayments whereas value can be transferred in a few minutes and the transaction can be considered secure

[10] Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera Joancomartí, J., SpringerLink, DPM (Workshop), CBT (Workshop), European Symposium on Research in Computer Security, 2017. Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings. Lecture notes in computer science ; 279-282. Springer International Publishing, Cham.

[11] It would not just require an immense amount of hardware, cooling equipment and storage space for computational power, but also involves the risk of prosecution and would irrevocably harm the ecosystem rendering the potential returns in Bitcoin to drop significantly in value.

[12] Chen, G., Xu, B., Lu, M., Chen, N.-S., 2018. Exploring blockchain technology and its potential applications for education. Smart Learning Environments 5, 1–10. https://doi.org/10.1186/s40561-017-0050-x

after a few hours. Finally, and as explained above, any user can verify a transaction, which results in full transparency.[13]

All these properties make blockchain a very attractive option to build decentralized applications that would be able to manage information and transfer value. This led to smart contracts, an innovation presented by the cryptocurrency of Ethereum. Developers can create private cryptocurrencies and contract-based applications through a Turing-complete language, allowing the businesses to use this language to set their own rules and policies.

The distributed ledger technology that blockchain uses offers multiple benefits to businesses that make a difference when implementing a solution requiring a high degree of trust for business transactions. We will review some representative uses of this technology below.

1. *Payment processing and money transfers*

The most widespread use for blockchain is to expedite the transfers of funds from one party to another. It backs the technology behind cryptocurrencies and is used in order to transfer money in a secure and fast way.[14] Several of the world's largest financial institutions have started to embrace the blockchain technology and experimented into incorporating it in their global payment systems. However, cryptocurrencies have often been associated with illicit activities, including money laundering, and there is generally concern over their legitimate uses and limits.

2. *Supply chains and insurance*

Blockchain can be used to monitor supply chains by removing paper records and assisting companies tracing any inefficiencies within their supply chains, as well as locate items in real time. For instance, we can use blockchain to trace food from its origin to a consumer's plate, or

[13] Tasatanattakool, P., Techapanupreeda, C., 2018. Blockchain: Challenges and applications, in: International Conference on Information Networking. IEEE Computer Society, pp. 473–475. https://doi.org/10.1109/ICOIN.2018.8343163

[14] Adams, R., Parry, G., Godsiff, P., Ward, P., 2017. The future of money and further applications of the blockchain. Strategic Change 26, 417–422. https://doi.org/10.1002/jsc.2141

to trace a weapon's origin and path, in an effort to enforce gun control and weapons accountability measures. Finally, blockchain could be a means of transparently tracking prescription medicines, ensure that a product is real and not counterfeit, and offer drug makers the ability to track their products based on serial numbers.[15] Blockchain would also allow businesses, and possibly consumers, to view how products perform in terms of quality when they travel from their origin to their destination.

An interconnected issue is insurance. Blockchain is ideal for smart contracts that define the rules and penalties surrounding an agreement.[16] They operate like a traditional contract, however the main difference is that they automatically enforce the obligations enshrined. These contracts provide the same level of safety as a traditional contract, and are even more reliable since they automatically enact their provisions, without the need for interpretation or dispute resolution proceedings. In this case, smart contracts can be used to implement smart contracts that will automatically check whether all the obligations are met. If yes, the payout will be automatic and will require minimum human input. This can be extended to the more traditional insurance regimes: under blockchain a user could submit a claim online and receive an automatic payout. Insurance companies are already experimenting with this technology that is more client-friendly, fast and easier to use. For instance, a French insurance company is using smart contracts to track flight-delay related insurance products and automatically store and process payouts.[17]

In a similar issue compared to insurance, blockchain can assist individuals in drafting their will on a blockchain network, making said will the ultimate authority of an individual's last wishes.

[15] Nichol, Peter (2017), The Power of Blockchain for Healthcare: How Blockchain Will Ignite the Future of Blockchain, Blockchain applications for healthcare - University of Oxford, pp 69-81
[16] Macrinici, D., Cartofeanu, C., Gao, S., 2018a. Smart contract applications within blockchain technology: A systematic mapping study. Telematics And Informatics 35, pp2337–2354. https://doi.org/doi:10.1016/j.tele.2018.10.004
[17] Feig, E. (2018), A Framework for Blockchain-Based Applications, pp. 2-5.

In combination with smart contracts, inheritances could automatically payout third parties when certain criteria are met (e.g. when grandchildren reach a certain age). Such a development would ensure that a will is crystal clear and truly legally binding, therefore leaving no room for misinterpretation.

3. Finance and investment

Smart contracts can further be used in a range of financial products.[18] For instance, they can be used in trading stocks and shares in a streamlined fashion that reduces the costs of derivatives trading altogether. Settlements could be performed in a matter of seconds rather than days – which is currently the case-, an investor could almost immediately sell a stock and access his funds for reinvestment or withdrawal.[19] Peer-to-peer trading can revolutionize the way stock markets work since it will largely remove the need for middlemen who buy and sell shares on commission. Similarly, smart contracts can be used to help energy companies settle futures trading considerably faster than they currently do. Blockchain can have a significant impact on energy companies altogether in terms of logging their resources and maintaining regulatory compliance.

In terms of broader investment, blockchain can ensure that any transaction regarding land, a house, or a car is safely recorded in an undisputed manner. Blockchain can store ownership titles on its network, allowing for a transparent view of this transfer, as well as having a crystal-clear picture of legal ownership.

4. Identity verification

[18] Mattern, M., 2018. Exploring Blockchain Applications to Agricultural Finance, CGAP Brief, p.2, World Bank, Washington, DC.
[19] Cai, W., Wang, Z., Ernst, J.B., Hong, Z., Feng, C., Leung, V.C.M., 2018. Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access 6, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Blockchain can use its decentralization function to verify an individual's online identity, much quicker. It will help create decentralized databases where identification data is stored, instead of a centralized point of vulnerability to attack. Data storage is tamper-proof and incorruptible altogether when backed by Blockchain, leading innovation on verification of identity.[20]

The need for a single centralized source on identities is essential for a range of applications, including crime prevention. A decentralized digital identity system, as a source of truth, is included in the system only by distributed consensus. The decentralized feature is already explored by a number of enterprises, including Microsoft and IBM, which provides the advantage that no single centralized entity can tamper with user identities or data. Such a system benefits users since it enhances their privacy and control over their personal data, whereas it reduces management costs for enterprises and improved overall efficiency.

A similar utility of unique identification can be used in elections and polls, where blockchain can assist to eliminate fraud, while providing complete transparency to the results and keeping the votes anonymous. Digital voting can provide security while upkeeping the transparency that any regulators would be able to see if something changed on their network. It therefore combines the ease of digital coding with the immutability of blockchain.[21]

Finally, it is expected that in the near future governments will be issuing passports through the blockchain technology, therefore making it impossible to tamper with them, and individuals will have total control over their digital identities.

5. *Internet of Things*

[20] For instance, the city of Zug in Switzerland uses a decentralized application (DAPP) for verify its citizens' electronic identities. Another similar solution is used in Estonia to solve the KYC problem, which is of major importance in identity verification.

[21] White, G.R.T., 2017. Future applications of blockchain in business and management: A Delphi study1. Strategic Change 26, pp439–451. https://doi.org/doi:10.1002/jsc.2144

Blockchain can enable the Internet of Things (IoT) and help unfold its potential. IoT is the network of physical devices, vehicles and other items that are connected to the Internet and they interact.[22] An example of the near future can be the following: you wake up and you don't feel well. You take your temperature and the thermometer shows that you have fever. It is connected to the Internet so it automatically sends an order to your pharmacy for aspirin supplies, books an appointment with your general practitioner online, sends an automated email to your employer that you won't be coming to work today, and checks the supplies of your fridge to see what you are missing to prepare a soup, which it also orders online. In this example a number of devices and services are connected to the Internet (thermometer, online pharmacy, online medical appointment, email, fridge, online supermarket) and they interact through a secure network to deliver the most efficient result.[23]

Blockchain can assist this through securing the network in which the devices interact, prevent hacker attacks, and facilitate the unique interconnectivity between devices. Smart contracts can also be deployed in IoT since, for example, as a consumer you can grant access to your house for service technicians, or allow your mechanic to access your car and perform repairs. Major IT companies predict that by 2020 at least 20 billion connected devices will facilitate functions like the above. Given the sensitivity of the operations and the scale of potential growth, blockchain's strong protection against data tampering will help prevent a rogue device from disrupting a home, factory or transportation system by relaying misleading information.

6. Archiving and file storage

Applications like Google Drive, Dropbox etc. have thoroughly developed the electronic archiving of documents with the use of centralized methods. Centralized sites and their

[22] Huckle, S., Bhattacharya, R., White, M., Beloff, N., 2016. Internet of Things, Blockchain and Shared Economy Applications. Procedia Computer Science 98, 461–466. https://doi.org/10.1016/j.procs.2016.09.074
[23] Yu, B., Wright, J., Nepal, S., Zhu, L., Liu, J., Ranjan, R., 2018. TrustChain: Establishing Trust in the IoT-based Applications Ecosystem Using Blockchain. Ieee Cloud Computing 5, 12–23.

blockchain technology through smart contracts can offer ways to reduce any relevant threat substantially. There are several ongoing blockchain projects that try to facilitate the decentralized process and ensure that the content is hosted on various anonymous users' computers.

Blockchain can also be an ideal way to back up data. Cloud storage systems are designed for data safe-keeping, however they are not immune to hackers, or even infrastructure problems. Blockchain can therefore be used as a backup source for cloud data centers, or for any data.

Safe recordkeeping is a relevant matter since particularly in sensitive industries (e.g. healthcare), blockchain can offer more safety and convenience compared to paper records.[24] In addition to storing patient records, the patient controls his records and would be able to determine who gains access to his data.

7. *Intellectual Property*

Blockchain can further assist in providing greater protection for intellectual property than before. In a world of growing interconnectivity and perplexed laws, internet access, copyright and ownership on music is a stumbling block. There are often disputes originating from copyright laws that may vary from one country to the other, or that might be subject to interpretation. Blockchain can assist these digital content downloads and ensure that the artist or creator is being compensated for his creation at a fair share.[25]

Blockchain can also provide real-time and transparent royalty distribution data to musicians and content creators.

8. *Crime prevention*

[24] Angraal, S., Krumholz, H.M., Schulz, W.L., 2017a. Blockchain Technology: Applications in Health Care. Circulation. Cardiovascular Quality & Outcomes. 10, Circulation. Cardiovascular quality & outcomes. Volume 10:Issue 9 (2017), p.1. https://doi.org/doi:10.1161/CIRCOUTCOMES.117.003800

[25] Mahdi H. Miraz, Maaruf Ali, 2018. Applications of Blockchain Technology beyond Cryptocurrency. Annals of Emerging Technologies in Computing 2, 1–6.

Criminals across the globe tend to hide and camouflage the money gained from their exploits. This is currently done with fake bank accounts, gambling, and offshore companies. As a result of this, there are a lot of concerns regarding the transparency of cryptocurrency transactions. However several regulatory elements, such as identifying parties and information, records of transactions and even enforcement can exist in the cryptocurrency system.

Blockchain, and its smart contracts, have the potential to render most money laundering tactics ineffective and particularly traceable. For example, a criminal that will attempt to launder money through cryptocurrencies can be traced because of the blockchain due to its secure and impenetrable network.

9. Workers' rights

A perhaps unorthodox use for blockchain as a means to bolster the rights of workers around the globe is that, according to the International Labor Organization, around 25 million people worldwide work in forced-labor conditions. In an effort to enforce and harmonize workers' rights, Coca-Cola, along with the US State Department, is working on a blockchain registry complete with smart contracts- protocols that verify, facilitate, or enforce a contract- to improve labor policies and coerce employers to honor digital contracts with their workers.[26]

5. Limitations and Vulnerability

Blockchain's applications are so diverse and pioneering, that it is difficult to navigate through them, even more so come with an effective regulatory roadmap. Blockchain's creation has often been associated, perhaps in a hyperbolic fashion, with revolutionizing inventions including the internet and electricity, in that it is a promising new technology for the future. The rapid growth of blockchain, particularly following the success of Bitcoin, has gained a massive attention in

[26] Miraz, C.M.H., 2018. Applications of Blockchain Technology beyond Cryptocurrency, p.3.

the past years. Even though blockchain's applications can prove significant, they are still far from being materialized, at least in mass adoption.

As with any new technology, it is still unclear how to make the most of the powerful capabilities of blockchain. The more we experiment with its uses, the more likely it is we will unveil new ways of utilizing blockchain for several purposes, as well as new methods that make it effective, efficient, secure and powerful. The growth of blockchain networks like bitcoin is only the beginning of the overall potential growth.[27]

At the end of the day, blockchain will continue to be important the more active users are within it. Its decentralized structure means that in order to operate to its full potential, a network needs to be robust with numerous nodes. There is still lots of distance that needs to be covered, inter alia since there is no blockchain network in existence at the moment that can sustain the same number of transactions like major card issuers.

As described above, there is always the theoretical possibility of a large-scale capture (51% attack) of any given blockchain network. This unlikely, but not impossible, scenario creates a certain level of uncertainty as to whether decentralized networks can sustain infinite growth. Rather, and once they become of critical importance for issues like global supply chain management, banking and finance, and property management, they will be more luring targets for a rogue group.

Overall, the blockchain technology has the potential to revolutionize several industries, from music to finance. Its main power lies in its decentralized nature and ability to ensure trust and privacy, however it comes with certain Achilles' heels that the legislator needs to bear in mind when considering its regulation.

As is commonly the case with any new technology, it takes time for a regulation to adapt and complete, particularly in fintech where regulators are charged with coordinating and

[27] Witherspoon, Z., 20170512. Advancing Consumer Adoption of Blockchain Applications, p.6.

guaranteeing industry stability. Blockchain is in its birth, and despite the exponential growth of Bitcoin, the rise of cryptocurrencies have led to more than 1,000 cryptocurrencies being traded at the moment. This signals that US and EU regulators must develop an understanding for blockchain's potential impact and try to develop an impactful and meaningful regulation.

Let's try, however, to untangle things: in doing so, we will examine the regulatory efforts on blockchain's most (in)famous application, cryptocurrencies. By drawing useful examples on how the EU and the US have made steps to regulate cryptocurrencies, we can also see what the future brings in terms of further regulation, or lack thereof.

6. US Blockchain Regulation

From a US standpoint, the blockchain regulatory efforts mainly revolve around cryptocurrencies, blockchain's most known application. No explicit legislative initiative in the US deals with cryptocurrencies, however its notion and use has largely developed through case law.

The US government overall shows support towards blockchain regulation- for instance, the US congress has created the Congressional Blockchain Caucus, a dedicated caucus to handle relevant legislation and cryptocurrencies. The caucus has introduced certain bills that mostly relate to digital currencies and monitoring blockchain initiatives. The introduction of "The Virtual Currency Consumer Protection Act of 2018" and the "US Virtual Currency Market and Regulatory Competitiveness Act of 2018" have provided further insight to the US Commodity Futures Trading Commission. These bills focused on cryptocurrencies, indicating that these are the main US regulatory priorities. To that effect, the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) delineates virtual currency as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real

currency".[28] Further, the US Internal Revenue Service (IRS) requires that cryptocurrencies traders must disclose their identity and cryptocurrency transactions should be taxed like property transactions.

On the other hand, the US Commodity Futures Trading Commission considers cryptocurrencies to be commodities under their jurisdiction, noting the lack of industry standards that will become highly problematic when blockchain further emerges. The US Securities Exchange Commission (SEC) also explored potential applications of blockchains for financial services transactions in the public securities market under the premise that cryptocurrencies are under their jurisdiction.

Overall, in the US the government does not have preemptive power to regulate blockchain over the US states, meaning that states are free to independently introduce rules and regulations. To that effect, some US states have worked on bills relevant to blockchain technology: for instance Arizona has introduced bills on smart contracts, Vermont on the use of blockchain as evidence, Chicago on real estate records, and Delaware on company shares' registration.

Also, efforts to apply laws on an extraterritorial basis have revolved around initiatives like the Foreign Corrupt Practices Act (FCPA). In May 2013 the US Department of Homeland Security issued a seizure warrant to the American-based firm undertaking transfers for the Tokyo-based cryptocurrency exchange, which complied and received a money business service license months before filing for bankruptcy protection. However, extra-territorial jurisdiction has not otherwise been widely implemented in cryptocurrencies to date.

Some recent cases can help illustrate the regulatory vortex that surrounds cryptocurrencies and, by extension, blockchain.

[28] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, p.1, available at https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

U.S. v. Ulbricht

Among the several cases where Bitcoins were used for money laundering, *United States v. Ulbricht* is the most notorious; Mr. Ulbricht was the creator of Silk Road, *a "billion-dollar online market that facilitated the illegal purchase of drugs, firearms and more"*. Mr. Ulbricht tried to argue that since Bitcoins are treated as "property" and not as "currency",[29] he could not have engaged in money laundering at all since the transactions were not "*financial transactions*".[30] The Court however held that "*the money laundering statute is broad enough to encompass the use of Bitcoins in financial transactions and that any other reading would be nonsensical*".[31] The district court judgment allowed the FBI to uncover almost one million Silk Road users, whereas the judgment was reaffirmed by the Court of Appeal in May 2017. It conveyed a simple yet clear message- if Bitcoins are laundered and used to fuel criminal activities, the law enforcement authorities will need to act.

The US government has since been pursuing similar cases, including the IRS summons against John Doe in November 2016, seeking information on all Coinbase users with a US address, telephone number or e-mail domain.[32]

U.S. v. Faiella

The case of *US v. Faiella* (2014) served to answer the substantive question of what is a Bitcoin (i.e. currency v. property). The Southern District of New York prosecuted Mr. Faiella for a violation of 18 USC para. 1960, alleging that he facilitated money laundering operation though the use of Bitcoins on the Silk Road marketplace.

[29] According to the IRS on March 21st 2014, notice 2014-14 defines virtual currency as property not money.
[30] Denial of Defense Motion: Opinion & Order, United States of America v. Ulbricht, Forrest, Doc. 14-cr-68 (S.D.N.T., July 9, 2014) at 48.
[31] United States v. Ulbricht, 2014 US Dist. LEXIS 93093 (S.D.N.T.) [Silk Road].
[32] See also Rob Wile, ''CEO of Bitcoin Exchange Arrested" Business Insider (January 27, 2014), online: <http://www.businessinsider.com/report-ceo-of-major-bitcoin-exchange-arrested-2014-1>; Cadie Thompson, ''CEO of Bitcoin exchange arrested" CNBC (January 27, 2014), online: <https://www.cnbc.com/2014/01/27/ceo-of-bitcoinexchange- arrested.html>.

In his defense, Faiella invoked three main grounds: (i) Bitcoins are not money; (ii) operating a Bitcoin exchange does not facilitate transmitting money as per 18 USC par. 1960; and consequently he was not a money transmitter. However, Judge J. Rakoff ruled that Bitcoin qualifies as money since it can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions.[33] This ruling gave the first definition of Bitcoin in Federal Case Law.

Faiella was convicted of operating an unlicensed money service business (exchanging business in the dark web). He was offered a plea to the charge and the additional charge of conspiracy to commit money laundering was dropped. Faiella was convicted to four years of imprisonment and he was ordered to pay a fine of $950,000 for his offences.

U.S. v. Murgio.

In September 2016, an Order was filed in the US District Court of New York in the case of *US v. Murgio*. The charges related to 18 USC par. 1960 and 18 USC par. 1956, in addition to other charges for operating a Bitcoin money laundering operation. The charges against Murgio alleged the opening of an unlicensed Bitcoin exchange under the name Coin.mx and thereafter facilitating money exchanges related to known criminals and money laundering activities. Murgio was also allegedly exchanging Bitcoins into cash for known cyber criminals.

Murgio disputed the charges through the argument that Bitcoins are not funds as prescribed in the statute and the charges are non-material. Judge Allison Nathan denied the motion based on three main premises. The first pertained to language within 18 USC defining money transmitting *"…to include transferring funds on behalf of the public by any way and all*

[33] *U.S. v. Faiella*, 2015, p.2, para. 2.

means…".[34] The key terms are funds in the agreement, practically referring to "*available pecuniary resources*".[35]

The Judge further defined pecuniary as "*taking the form or consisting of money*".[36] Judge Nathan also stated that money is defined as "…*something generally accepted as a medium of exchange…*".[37] Judge Nathan also reiterated the argument in the *US v. Faiella* case, that Bitcoins qualify as money under federal law.

The last argument addressed was about prior guidance and rulings regarding FinCEN, IRS, and the CFTC. Each of these agencies gave different perspectives regarding Bitcoins and digital currency; however, the court rejected the context of prior rulings. The final ruling stated Bitcoins fit the definition of funds, the definition of money, and 18 USC 1960 applied to Bitcoin cases. Finally, the court rejected the argument that funds should be more narrowly defined as currency.

Notwithstanding the rulings in *US v. Faiella* and *US v. Murgio*, Bitcoin has not been formally identified as money or currency by US legislators or regulators, nor has blockchain been further examined in a law or regulation. Blockchain needs a specific legal classification for regulation and enforcement purposes and at the same time specific mandates are needed to eliminate future confusion concerning the status of Bitcoin (digital currencies) as being a currency, commodity, or security.

7. EU Regulatory Framework

There are different elements of uncertainty surrounding blockchain implementation. For starters, liability is a key issue to resolve since it is often doubted how we can effectively assign

[34] *U.S. v. Murgio*, 2016, p. 4, para. 2
[35] *U.S. v. Murgio*, 2016, p. 5, para. 4
[36] *U.S. v Murgio*, 2016, p. 5, para. 4
[37] *U.S. v. Murgio*, 2016, p. 5, para. 4

liability in this new world of P2P transactions and automated contracts. Further, with regard to smart contracts, the question is to what extent they represent something new in the legal universe, if at all. Another point of inquiry is to what extent does the data stored on a blockchain have legally binding status? Does blockchain allow the creation of new types of digital assets? If not, is there a new categorization of legal and regulatory treatment that better reflects the existing frameworks?

For Europe, there is much at stake in clarifying these questions. A robust legal framework is the prerequisite for a value-producing blockchain industry, and an essential prerequisite for entrepreneurs, developers and the blockchain community to innovate.

Provided that Europe has this framework, it can cement its position as an attractive location for blockchain technology. More effort is needed towards that direction, as well as a firm commitment that any regulation brought forward will not hamper innovation. Otherwise, it is a matter of time that innovation companies will flee to other, more regulatory friendly and understanding, destinations.

The European Union (EU) has drafted a number of legislative initiatives in the past years that relate to financial services and the fight against money laundering, which serve as the main vehicle to regulate cryptocurrencies and blockchain. In this section, we will discuss how the Payment Services Directive (1) and (2), the e-money Directive (1 and 2), and the 4th and 5th Anti-Money Laundering Directives can be used, or not, for the regulation of cryptocurrencies and their illicit uses.

Payment Services Directive (1)

In 2007, the EU adopted a legal framework on payment services, known as the First Payment Services Directive (PSD). The directive restricts access to the market of payment services, but certain provisions are designed to waive or limit certain requirements for small market players.

The First PSD primarily regulated service providers, and not their actual services, and therefore arguably cannot apply to virtual currencies. Moreover, the consensus in literature is that the directive does not leave room to include virtual currencies at large, and cryptocurrencies in particular.[38]

Application to virtual currency service providers would only be possible to the extent virtual currency services can be qualified as payment services under the directive's scope. This is problematic since payment services under the directive are understood to revolve around the notion of funds, defined as *"banknotes and coins, scriptural money and electronic money as defined in Article 1(3)(b) of Directive 2000/46/EC"*. Even if we were to argue that privately issued currencies can fall under the scope of that definition, virtual currencies are typically not denominated in EURO or another currency recognized as legal tender, and therefore the substantive part of the Directive (Titles III and IV) would not apply. This means that even if virtual currency services are considered as payment services under the PSD, only a very limited set of provisions of the Directive would apply.

Perhaps an interesting exception, the French banking supervisor (Autorité de contrôle prudentiel et de resolution (ACPR)) has argued that cryptocurrency exchanges involve receipt of funds, in the strict sense of banknotes, coins, money or e-money, in exchange of cryptocurrency, which in turns leads to a payment service.[39] This approach however does not appear to have gained widespread popularity outside France.[40]

Payment Services Directive 2

[38] Shcherbak, S., 2014. 'How should Bitcoin be regulated?', European Journal of Legal Studies, 41:56–61.
[39] ACPR, '*Position de l'ACPR relative aux opérations sur Bitcoins en France Position' 2014-P-01*. This position was earlier signalled at by the French national bank: Banque de France, '*Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin' [2013]* Focus 1, 5–6.
[40] De Vauplane, H., 2015. '*La fascination autour du Bitcoin et des « monnaies virtuelles » : comment les définir*?' Alternatives Economiques, blogpost available at: https://blogs.alternatives-economiques.fr/vauplane/2015/11/07/la-fascination-autour-du-bitcoin-et-des-monnaies-virtuelles-comment-les-definir

The Second PSD does not substantially change things in that it is ultimately up to the Member States to interpret the relevant provisions of their directive and depending on their local sensitivities decide on the implementation.[41] Interestingly, in its proposal for amendments to the Fourth Anti-Money Laundering Directive, the European Commission explicitly states that it did not want to bring virtual currency exchange platforms under the scope of the Second PSD, as this would *"submit them to broader consumer protection rules, licensing requirements and safeguarding requirements"*.[42]

The fear behind this position was that it would legitimize virtual currencies and "*drive consumers to believe VC are safe and sound products"*.[43] As a result, third party cryptocurrency service providers are not, *ab initio*, covered by the EU legal framework on payment services. This was confirmed in the European Central Banks's 2012 opinion on virtual currencies. Further, the European Banking Authority has noted that the Second PSD is not suitable to address the specific risks posed by virtual currencies at large, and the technical risks posed by cryptocurrencies in particular.[44]

As a final remark, both PSDs include large sets of scope exemptions, meaning there are several cases where services are excluded from their scope, including relevant exemptions for virtual currency service providers. Some authors have suggested that cryptocurrencies could benefit from the limited networks scope exemption, however this is defined in a very narrow way under

[41] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/ 36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35 (hereinafter: Second Payment Services Directive or PSD2).

[42] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73 (hereinafter: Fourth Anti-Money Laundering Directive or AMLD4).

[43] European Commission, '*Impact assessment accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC'* SWD(2016) 223 final, 30–31.

[44] European Banking Authority, '*Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD*)' (EBAOp- 2016-07 2016) 4–5.

the Second PSD, and would practically appear impossible. The money exchange exemption also does not appear to be appropriate since it targets physical exchanges, whereas cryptocurrency exchanges by nature appear online and require the use of an account. The added value exemption would, due to the Second PSD's narrowing down its scope to electronic communications providers, would also not be applicable to these service providers.

E-money Directive (1 and 2)

The last decade of the 20th century saw the rise of multi-purpose stored-value cards.[45] The European Monetary Institute (the ECB's predecessor) was concerned that this technology had the potential to disrupt the traditional finance institutions, which resulted in the adoption of the first E-money directive in 2000[46] that tried to regulate the provision of electronic services and ensure that E-money would not be detrimental to the traditional system.[47]

The EU recently replaced the initial directive with a revised Second E-money Directive.[48] The legal framework is focused solely on issues of E-money, however the second e-money directive also relies on the First PSD for several provisions, including scope exemptions. If certain exemptions could prevent virtual currency service providers from falling under the scope of the PSDs, they would also prevent them from being subject to the Second E-money Directive.

Other restrictions aside, the E-money directive has a limited scope in itself: its primary notion is E-money, which is defined as *"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*

[45] Jacobs, E., 2011. 'Bitcoin: A Bit Too Far?', Journal of Internet Banking and Commerce 1, 3.
[46] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions [2000] OJ L275/39 (hereinafter: First E-money Directive or EMD1).
[47] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009], OJ L267/7 (hereinafter: Second E-money Directive or EMD2).
[48] Houben, R. 2015. 'Bitcoin: there are two sides to every coin' Tijdschrift voor Belgisch Handelsrecht 139, 156

making payment transactions"[49] and which is accepted by a natural or legal person other than the electronic money issuer.[50] This requires E-money to be issued on receipt of funds, essentially establishing it as prepaid goods. While some forms of virtual currencies could be established as prepaid tokens, the ECB's recent opinion created a consensus that cryptocurrencies do not fall into such scope. These forms of virtual currencies are therefore not subject to the E-money directive, and other elements of the definition would also prove problematic, including virtual currency schemes.

The Second E-money Directive was supposed to be reviewed by late 2012, to coincide with the review of the First PSD, however to date this has not happened. The question therefore remains whether the scope of the definition will be more expanded once the update occurs. The initial regulatory intention was connected to multi-purpose stored-value cards; these are now not widely used, meaning that this legal framework needs to either be updated, or otherwise it will become totally obsolete.[51] The addition of network-based E-money in the definition is a progress, however it does not clarify questions including whether account-based transfers do or do not fall under the scope of E-money.[52]

The UK Financial Services Authority (FSA) considers deposits as involving the creation of a debtor-creditor relationship, whereas E-money involves the purchase of a means of payment, albeit the European Commission does not agree with this reasoning.[53] With the development of payment services, and the diminishing differences with electronic payment transactions, it is interesting to see whether these two legal frameworks will merge or whether the E-money

[49] As defined in point 5 of Article 4 of Directive 2007/64/EC.
[50] Kubát, M. 2015. 'Virtual currency bitcoin in the scope of money definition and store of value', Procedia Economics and Finance 409, 411–412.
[51] Vardi, N., 2016. 'Bit by Bit: Assessing the Legal Nature of Virtual Currencies' in Gabriella Gimigliano (ed), Bitcoin and Mobile Payments: Constructing a European Union Framework (Macmillan Publishers 2016) 61.
[52] Guadamuz González, A., 2004. 'PayPal: The legal status of C2C payment systems', Computer Law & Security Review 293, 297.
[53] Financial Services Authority, 'Implementation of the second Electronic Money Directive: supplement to HM Treasury's consultation – Feedback on CP10/25 and part of CP10/24, and final rules' (Policy Statement PS11/2) 73.

directive will expand to include cryptocurrencies in its scope. Several authors contend that the expansion of this framework toward virtual currencies could be the way forward.

On a last note, some virtual currency service providers voluntarily register as payment service providers.[54] There are a number of reasons for service providers to pursue this voluntary registration; by submitting themselves to a current legal framework, they could benefit from a transitional regime if new regulation would be adopted.[55] Another reason service providers use voluntary licensing is to foster user trust through regulatory oversight to which they will be submitted. Finally, this license could also serve as a marketing tool to offer a competitive advantage over unregulated market players.

Anti-money Laundering Directive (4th)

The Fourth Anti-Money Laundering Directive was adopted on 20 May 2015 as one of the initiatives which was has put into effect since the first related Directive in 1990 in order to prevent the misuse of the financial system for the purpose of money laundering. The main focus of the Directive relates to property derived from criminal activity, meaning *"assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets"*. This is a rather broad definition that could, in theory, include virtual currencies as incorporeal assets. The questions then becomes whether the entities providing virtual currencies exchanges, are to be considered credit or financial institutions.[56]

[54] For example in France the Paymium cryptocurrency exchange relies on HiPay, an e-money institution authorized in Belgium. Similar examples are seen in Luxembourg (SnapSwap that operates a mobile messenger payment service via blockchain technology licensed as an e-money institution) and the UK (Circle- a payments application provider that utilizes cryptocurrencies).

[55] Valcke, P., Vandezande, N., Van de Velde, N. 2015. 'The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4' (SWIFT Institute Working Paper 2015-001) 56–59.

[56] Künnapas, K., 2016. 'From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda?' in Tanel Kerikmäe, Addi Rull (eds), The Future of Law and eTechnologies (Springer 2016) 119–120.

However, legal and natural persons, as well as financial institutions, are defined in a way that virtual currencies do not fall into their scope.[57] Interestingly, one of the services under the 4th AML relate to *"issuing and administering other means of payment (e.g. travelers' cheques and bankers' drafts)*" insofar such is not a payment service. The legislative procedure that led up to the Fourth Anti-Money Laundering Directive signals that it was never the intention to explicitly include virtual currencies under the scope of this legal framework.[58] Neither does the final text mention anything about virtual currencies nor can we indirectly infer that anonymous E-money instruments refer to virtual currencies.

Member States could still bring the virtual currencies under the explicit scope of the domestic laws since a Directive is a minimum harmonizing initiative and allows Member States to further specify the scope and introduce stricter requirements and procedures. The UK government was an example that vouched for the inclusion of virtual currencies[59] but exercised caution at the same time not to deter investments in the growing fintech industry, a fear also expressed by the Financial Conduct Authority that stressed the importance of allowing the new technologies to thrive.[60]

Anti-money Laundering Directive (5th)

In February 2016, the European Commission presented its Action Plan to strengthen the fight against terrorism financing. There, it acknowledged that virtual currencies were not regulated at the level of the EU, including the anti-money laundering framework, and expressed its clear intent to bring virtual currency service providers under the scope of that legal framework.

[57] Services included in Annex I to Directive 2013/36/EU.
[58] While the European Commission did acknowledge that virtual currency exchange platforms were not included under the directive, it did propose "to look again into virtual currencies". Payment Systems Market Expert Group, 'Minutes of the meeting of 28 April 2015' (PSMEG/005/15) 3.
[59] HM Treasury, 'Digital currencies: response to the call for information' (HM Treasury 2015) < gov.uk/government/uploads/system/
[60]
uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf>

The European Commission's proposal to amend the Fourth Anti-Money Laundering Directive was consequently published in July 2016. In its proposal, which led to the 5th AML Directive, it recognized the potential benefits of virtual currencies, and in particular the possibilities emanating from the blockchain technology related to cryptocurrencies. Submitting those cryptocurrencies to anti-money laundering rules would arguably impose strict requirements on the virtual currency service providers, however it did not find that the proposal would have negative effects to the benefits and technological advances of these currencies. On the contrary, it felt that the use of virtual currencies for criminal purposes could diminish their credibility, which would turn anonymity more a hindrance than an asset for virtual currencies and their potential benefits spreading. It tried to further limit the anonymity around virtual currency transactions through the use of National Financial Intelligence Units (FIUs) in being able to associate virtual currency addresses to the identity of the owner of virtual currencies.

The European Central Bank objected to the use of the notion of 'currency', when discussing the AML directive, in the fear that the notion would imply a reference to legal tender. The ECB therefore pushed that virtual currencies would be clearly distinguished from legal tender. The ECB further warned that if the discrimination was not clear, this could be perceived as lending legitimacy to virtual currencies, which would be rather unwarranted since not all of the associated risks were addressed, including their volatility and potential to disrupt price stability. Including some of the virtual currencies in the anti-money laundering legal framework, without complementing that with consumer protection or prudential safeguards, may give a false impression of full regulation to consumers. ECB posited that there is a need for an all-encompassing regulation that addresses all the challenges of virtual currencies and that adequately shields consumers.[61]

[61] ECB, *Opinion of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/ 849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/ 101/EC* (ECB 2016) 3.

The 5th Anti-Money Laundering Directive is the latest addition to the European Commission's AML efforts. It provides that obliged entities must apply customer due diligence requirements when entering into a business relationship, for instance identify and verify the identity of clients, monitor transactions and report suspicious transactions. This legislation has been constantly revised to mitigate risks relating to money laundering and terrorist financing.

The 5th Anti-Money Laundering Directive (Amendments to the 4th Anti-Money Laundering Directive) was published in the Official Journal of the European Union on 19 June 2018. The Member States must transpose the Directive by 10 January 2020.

Part of the amendment to the 4th AML relates to the Panama Papers revelations. The 5th AML in brief aims to:

- Increase transparency about the true owners of companies for the purpose of preventing money laundering and terrorist financing through opaque structures;
- Facilitate the work of Financial Intelligence Unites with better access to information through centralized bank account registers;
- Tackle terrorist financing risks linked to anonymous use of virtual currencies and/or prepaid instruments;
- Improve the cooperation and exchange of information between anti-money laundering supervisors with the European Central Bank;
- Broaden the criteria for assessing high-risk third countries and ensure a common, increased, level of safeguards for financial flows from said countries.

The 5th AML marks the first time ever in EU legislation that directly targets the use of virtual currencies. The rules apply to entities which provide services and which are in charge of holding, storing and transferring virtual currencies, to persons who provide similar services to those provided by auditors, external accountants and tax advisors and who are already subject

to the 4th AML directive and to persons trading in works of art. Said actors will need to identify their customers and report any suspicious activity to the Financial Intelligence Units.

Certain provisions explicitly deal with aspects of virtual currencies. Specifically, recital 8 explains the rational of the Directive mentioning that, currently, providers engaged in exchange services between virtual currencies and fiat currencies (i.e. *"coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country"*) are under no Union obligation to identify suspicious activity, which in turn facilitates terrorist groups to transfer money into the Union financial system or within virtual currency networks. This legal gap, the Directive contends, makes it essential to extend its scope to also include virtual currencies,[62] fiat currencies and custodian wallet providers.[63]

Recital 9 also points to the misuse of the virtual currencies' anonymity as a way to pursue criminal goals. The Directive recognizes that including providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity since a large part of the virtual currency environment will remain anonymous because users can also transact without such providers. The Directive actively puts National Financial Intelligence Units (FIUs) in the process, saying that they should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency.

The Directive makes an important distinction regarding the use of virtual currencies (Recital 10) and that they should not be confused with electronic money as defined in point (2) of Article

[62] The Directive defines "virtual currencies" as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

[63] The Directive defines "custodian wallet provider" as an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.

2 of Directive 2009/110/EC of the European Parliament and of the Council, nor with the larger concept of 'funds' as defined in point (25) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council, nor with monetary value stored on instruments exempted under points (k) and (l) of Article 3 of Directive (EU) 2015/2366, nor with in-game currencies that can be used exclusively within a specific game environment. The Directive recognizes that virtual currencies can frequently be used as a means of payment, but they could further be used for other purposes and broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The Directive adopts an all-encompassing approach and attempts to cover all the potential uses of virtual currencies.

Finally, the 5th AML has consequences for the users of virtual currencies- the amendments touch on the core of what users tend to consider a major benefit, which is anonymity. Given how most users acquire cryptocurrencies through exchange platforms, or use the services of custodian wallet providers in their payments, they will now be required to verify their identity toward those service providers. This would arguably limit the risk posed to users by that anonymity.[64] Creating a central database that includes all the users of cryptocurrencies would further inhibit users from using this new technology.

8. Conclusion

Blockchain is in a track to change the way we perceive the global economy, supply chains, and the notion of trust. It is a novel concept and we are still trying to comprehend how it works and how it can be used on a daily basis. The etheric nature of blockchain and its current applications, for instance Bitcoin, makes it even more difficult to effectively regulate them, since in essence we need to regulate something that we do not fully understand, and which is a

[64] ECOLEF, 2013, 'The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy' (European Commission) <www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf>.

work in progress. While their uses can be wide, and blockchain can also be used in a number of sectors, cryptocurrencies can also be misused.

At the same time, regulation needs to be thoughtful and laws need to be carefully crafted, or else they are nothing more than a Pandora's box. Placing blockchain under the aegis of law comes with a great opportunity, which is that we can determine the basic rules of the game. However, this also comes with a non-eliminable risk: citizens will perceive that since blockchain is regulated, for instance via cryptocurrencies, and even though this regulation may be partial and limited in scope, they are now safe to use all such applications. How much regulation is good enough for blockchain is therefore the million dollar question, since regulating something so perplexed may create the misconception of security to consumers.

When all is said and done, the next years will determine whether blockchain's applications will evolve into a mainstream tool, or whether they will end up being associated with illicit or insecure activities.