Exploring Blockchains Cyber Security Techno- Regulatory Gap. An Application to Crypto-Asset Regulation in the EU.

Simona Ramos[1], Lela Melon[2] and Joshua Ellul[3]

10th Graduate Conference in Law and Technology, Sciences Po

18th June 2022

Abstract. Blockchain technology has taken off rapidly in the last decade, as blockchain- based applications have expanded across sectors and acquired substantial global user support. This rise has been accelerated in the domain of cryptocurrencies, as one of blockchains' most famous (or infamous) applications. This relatively novel type of a financial asset class with increasingly large market valuation has sparked the interest of regulators and law makers. As a means of fostering fintech innovation, the EU has stated its support for adoption and development of blockchain and cryptocurrencies in the European Economic Area. Nevertheless, cryptocurrencies lie at the top of a potentially dangerous feedback loop mediated by market valuation. Cyber-attacks targeting cryptocurrencies (and the underlying blockchain technology) have been on the rise, costing users and businesses millions of euros. From a European Union regulatory standpoint, high cyber security resilience is a precondition for sustainable innovation in an increasingly digitalized financial sector, where protecting users and businesses is a priority. In this paper, we discuss aspects of blockchains' technical vulnerabilities and related cyber-attacks in order to develop a deeper understanding of the extent and efficiency of possible regulatory remedies concerning crypto-assets in the EU. We present a regulatory overview of the emerging fields of cyber risk and blockchain in Europe and illustrate a techno- regulatory gap which requires further attention. We underline the difficulty of assigning traditional cyber regulatory measures due to certain technical characteristics related to blockchains. We maintain how the relationship between cyber law and technology may evolve in the near future, as decentralized technologies and the cyber risks that go with them, continue to develop rapidly. By providing an interdisciplinary perspective of cyber security in the blockchain domain, we aim to bridge the gap that exists between legal and technical research, supporting policy makers in their regulatory decisions concerning crypto-assets, decentralized technologies and associated cyber risks.

Keywords: Blockchain, Crypto-Assets, Cyber Security, Regulation

---

[1] Marie Curie Research Fellow, PhD candidate at Universitat Pompeu Fabra (UPF).

[2] Professor at UPF, UNESCO Chair in Lifecycle and Climate Change. Executive Director of Planetary Wellbeing.

[3] Professor at Malta University, Director of Centre for DLT.

Table of Contents

Introduction

A blockchain is a peer-to-peer distributed ledger that records transactions between parties in a verifiable and permanent way by storing them in a sequence of blocks (of transactions). Blocks are linked together into a chain, which is secured using cryptographic primitives and a lottery mechanism exhibiting randomness. Each block contains a hash of the previous block, an unforgeable proof from the lottery, a timestamp, and a list of transactions [1]. Among the most interesting instances of blockchain technology, public blockchains (also known as 'permissionless') demonstrate a concept of distributed and decentralized systems, where users are not required to trust a third party but simply agree to execute and be bound to the outcomes of a computer program implementing a set of rules[4] [2]. Smart contracts are often described as types of contracts whose terms are recorded in computer code and can be automatically executed by a computing system, such as a distributed ledger system. With the growing use of smart contracts and an increasing variety of smart contracts applications, the debate over their legal validity, legal status and implications on law has intensified [3]. Smart contracts provide guarantees to the various stakeholders since the code (actions and terms) encoded within them cannot be changed, as they are immutably stored and executed on a blockchain [4]. However, the immutable nature of smart contract code is a double-edged sword providing user guarantees yet at the cost of inability to fix code deployed that may have software bugs within (of which ramifications are further discussed herein). The most popular instances of public blockchains that provide cryptocurrencies — which have become a novel financial asset class with increasingly large market valuation [5]. The definition of cryptocurrencies varies among jurisdictions. At EU level, as part of the most recent EU regulatory proposals, "*digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology*" are referred as crypto- assets[5]. In this article we use the terms crypto-assets and cryptocurrencies inter changeably.

Today, there are more than 2,000 crypto-assets outstanding [6]. Given the short historical track record of these systems and the relative novelty of the mechanisms that keep them operating, many questions on the risks and reliability of cryptocurrencies as financial assets naturally remain. Along with the rapid

[4] Consisting of the so-called 'consensus rule set' and other rules that may be encoded in any smart contracts used.
[5] See (pg.15) of Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto Assets, and amending Directive (EU) 2019/1937.

uptake of cryptocurrencies, cyber-attacks related to blockchain and cryptocurrencies have also significantly increased. The Carbon Black report uncovered a total of 1.1 billion dollars in cryptocurrency-related thefts during the first half of 2018 [7]. Although cyber risks have been a common topic of discussion among experts and regulators, due to the technical complexity of blockchains, these risks still remain under addressed. Overall, blockchain technology brings along with it application novel types of cyber risks (particularly in the domain of crypto- assets) for which further attention is required [8]. From a general standpoint, cyber-attacks related to blockchains and cryptocurrencies could be analyzed and potentially mitigated from two angles:

1. by improving the technical resilience of technology used or related to the blockchain system and associated smart contracts, which may include developing incentive mechanisms under which blockchains would be more resistant to adversarial behavior.

2. by introducing regulatory measures that mitigate these risks and alleviate the burden of risks of attacks from the affected parties.

In this article we focus on the latter (which include regulatory measures that could result in improved technical resilience as well). While the task of designing resilient and sustainable Distributed Ledger Technologies (DLT) lies mostly in the hands of private entities and decentralized communities, the introduction of regulatory measures could be considered a complimentary remedy and a security reinforcing factor imposed by governments – if certain constrains can be accounted for. A firm grasp of security and intricacies of blockchain systems and understanding how cyber risks can be mitigated could determine the extent of acceptance of blockchain technology within the European community. Whilst, arguments made in this paper are directly centered around Proof-of-Work based blockchains, many of the issues raised are suited for Proof-of-Stake systems as well, yet due to space constraints we could not expand further on this.

The remaining of this paper is structured in the following manner. In the following section, we explore the notion of trust in a decentralized Proof-of-Work setting and present a brief overview of salient technical vulnerabilities and cyber-attacks related to blockchains. Thereafter, a regulatory overview of the emerging fields of cyber risk, blockchains and cryptocurrencies in the European Union is presented. Following, we discuss the existence of a techno-regulatory gap and explore the ways

blockchain technology poses challenges to traditional cyber security measures. We present several viable measures that could mitigate cyber risks and give examples of regulatory remedies that show to be a prosperous lead in this domain. By providing an interdisciplinary perspective of cyber security regulation in the blockchain domain, we aim to merge the gap that exists between legal and technical research, supporting policymakers in their regulatory decisions concerning crypto assets and associated cyber risks.

Blockchains: Base for Trust and Security Overview

After the release of Nakamotos' paper in 2009 the idea of blockchain as known today came about, as a result of the establishment of the Proof-of-Work (PoW) consensus mechanism that permitted for the development of the arguably most essential trait of the system – trust [9]. A consensus mechanism is the protocol over which users taking part in maintaining a blockchain agree to validate new (and old) blocks. The PoW consensus mechanism is still one of the most frequently used in existing blockchains [10]. PoW works as a lottery mechanism where a node (aka and run by a miner) is 'selected' based on a computational power competition where the node that manages to first solve the cryptographic puzzle set by the network gets to create the block [1]. This process is known as mining. Exploitation of the way the protocol works can expose system vulnerabilities, lead to a cyber-attack and cause significant damages. In broad terms a cyber-attack is an attempt by å malicious party to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage [11]. Large-scale cyber-attacks can cause substantial damage, economic loss and disrupt the flow of information and operation of systems [12]. Due to its lucrative nature, in the last years, blockchain based attacks targeting cryptocurrencies have increased in size and scale. Majority (or 51%) and wallet attacks have been some of the most lucrative ones, costing users and businesses millions of euros. By way of example, in May 2018, eighteen million euros of Bitcoin Gold were stolen as part of a double spend that occurred during a majority attack [13], while the majority attack that hit Ethereum Classic in 2019 costed users around half a million euros [14]. 72 million dollars worth of Bitcoin were stolen from Bitfinex exchange in 2016 through a wallet attack [15]. Just in 2019 twelve (known) crypto exchanges were hacked, where 292,665,886 euros worth of cryptocurrency and 510,000 user logins were stolen from crypto exchanges [16]. Besides theft of coins, cyber- attacks on crypto-assets can also cause abnormal economic losses for investors. By a way of example, [17] found that majority and wallet attacks cause a decrease in the affected cryptocurrency price and

generate abnormal economic losses. Wallet attacks can occur via different attack vectors, including breach of the wallet provider core protocol, DNS hijacking, phishing attacks, remote code injection, amongst others [18]. Likewise, certain attacks can be leveraged as a double spend strategies[6]. For example, a consensus delay, BGP attacks, flood attack on mempools, can cause additional latency in the verification and propagation process, hence increasing the chances of a double spend attack. Under a Sybil attack an attacker can cause block propagation delays which can increase the probability of winning the mining race and launching a double spend [8]. Cyber risks are not only associated with attacks that aim to exploit a blockchain's protocol, but also may be induced through software bugs — which may exist within a blockchain platform itself or within smart contracts executing on top of a blockchain [19]. Software bugs can lead to a myriad of unwanted outcomes, such as locking away funds mistakenly forever[7]. Another early infamous case is that of the DAO (Decentralized Autonomous Organization) hack, which enabled for attackers to undertake a reentrancy attack enabling for them to get away with USD 160 million worth of cryptocurrency [20]. Indeed, there other types of bugs that can emerge in smart contracts, some a result of complex logic and some could be due to a typo, an incorrect line of code, or a mistaken order in two (or more) lines of code. In Table 1 below we present an overview of salient vulnerabilities targeting DLT and identify the entities that would be or may be affected. Each of these attack vectors affects different parts of the blockchain eco-system, bringing to the forefront the complexity and relevance of a suitable DLT specific cyber-regulatory approach.

Attack	**Description**	**Blockchain**	**Miners**	**Users**	**Exchanges**	**Smart Contract**
Majority (51%) Attack	Attack on a blockchain by a group of miners who control more than 50% of the network's mining hash rate. If successful attack would allow for an attacker to undertake a double-spend attack.	**X**	**X**	**X**	**X**	
DoS Attack	An attack which aims to overwhelm a resource through extensive use of the resource to disrupt service to its intended users. This may include a machine, a network re-source or even a smart contract (e.g. by forcing a smart contract into a situation that results in out-of-gas exceptions)			**X**	**X**	**X**
Wallet Attack	Theft of private keys, can happen through different ways including a possible breach of a wallet provider's core protocol, DNS hijacking, phishing, etc.			**X**	**X**	**X**
Sybil Attack	Single entity tries to take over the network by creating multiple accounts or running multiple nodes.	**X**	**X**	**X**	**X**	
DNS Hijack	Attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites.			**X**	**X**	

[6] Double spending is a problem that arises when transacting digital currency that involves the same tender being spent multiple times.

[7] As was the case when USD 300 million worth of crypto was lost forever due to a bug in the Parity wallet which allowed for unwanted functionality to be exploited

BGP Attack	Illegitimate takeover of groups of IP addresses by corrupting internet routing tables maintained using the Border Gateway Protocol (BGP).	X	X			
Eclipse Attack	In an eclipse attack, the malicious actor will ensure that all of the target's connections are made to attacker-controlled nodes.	X	X	X	X	
Finney Attack	A type of double-spend attack, where the attacker creates two transactions – one crediting the victim and one crediting themselves.	X	X	X	X	
Contract Code Exploit	A smart contract will do exactly what it was written to do --- including executing a software bug mistakenly encoded. Attackers can exploit such bugs to steal funds, manipulate state to their benefit, or manipulate a smart contract in a malicious or other manner. An example of such a bug is the reentrancy bug which allows for an attacker to cause unintended code paths to execute, which may result in the attacker stealing funds or some other unintended behavior.			X		X
Front-Running	Front-running & Before transactions are accepted into a blockchain they form part of the mempool and are broadcast for all to see. Knowledge of a first transaction and its contents that has not yet been accepted could be used by an attacker to submit a second transaction which exploits knowledge learned from the first not-yet-accepted transaction. The second transaction is submitted with higher gas fees in aim of having it accepted before the first.			X		X

Table 1. Taxonomy of cyber-attacks & technical vulnerabilities related to blockchains, cryptocurrencies and smart contracts.

Crypto-Assets and Cyber Security Regulation within the EU

In the European Union, a number of regulations have been put into place to address cyber-security risks pertaining to the usage of computer technologies. The NIS Directive, adopted on 6th of July 2016, represents the first EU-wide rule book on cyber security.[8] Via the implementation of the EU directive (EU 2016/1148) for network and information security, Member States are required to create and enforce a national security strategy to deal with cyber-security risks. In December 2020, the Commission made a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) which expands the scope by adding new sectors based on their relevance for the European economy and society.[9] The EU Cyber Security Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes.

Yet, blockchain technology and crypto-asset applications bring novel types of security challenges for which other types of regulatory remedies may be needed. The European Securities and Markets Authority (ESMA) identified the most significant risks regarding crypto-assets as fraud, cyber-attacks,

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

[9] See Proposal for a Directive of the European Parliament and the Council on measures for a high common level of cyber security across the Union, repealing Directive (EU) 2016/1148.

money laundering, and market manipulation. In particular, ESMA emphasized that technology-specific risks are still under addressed while certain existing requirements may not be easily applied or may not be entirely relevant in a DLT framework (e.g. GDPR) [6]. Both EBA and ESMA emphasized that beyond EU legislation aimed at combating money laundering and terrorism financing – most crypto-assets fall outside the scope of EU financial services legislation and therefore are not subject to provisions on consumer and investor protection [21]. Recently, the Basel Committee on Banking Supervision demanded for cryptocurrencies to carry the toughest bank capital rules of any asset due to high-risk exposure, including the risk of cyber-attacks [22]. On these grounds, many countries worldwide have issued warning notices for their citizens advising them of the potential dangers of investing in crypto-assets. In general, governmental measures span from those which are restrictive, to permissive and encouraging [23] and indeed given the nascency of the sector many jurisdictions have not taken any measures.

Recently, the EU Commission and Council jointly declared their commitment to establish a legal framework that will harness the potential opportunities that crypto-assets may offer while at the same time mitigate associated risks posed to European users and businesses [21] [24].The Commission's President, Ursula von der Leyen, expressed the need for *"a common approach with Member States on crypto-assets to ensure we understand how to make the most of the opportunities they create and address the new risks they may pose."*[10]In an effort to determine the legal status of crypto-assets as part of the ``Digital Finance Package" initiative[11] as well as to reinforce cyber resilience within the union, the EU recently issued three regulatory proposals. A proposal on Markets in Crypto-Assets (MiCA) [24], a proposal for regulation on a Pilot Regime For Market Infrastructures Based On Distributed Ledger Technology [21] and a Proposal On Digital Operational Resilience For The Financial Sector (DORA) [25].

In November last year, the Council adopted its position on the proposals that are part of the digital finance package. This agreement forms the Council's negotiating mandate for trialogue negotiations with the European Parliament. Last month, the members of the European Parliament (MEPs)

[10] Mission letter of President-elect Von der Leyen to Vice-President Dombrovskis, 10 September 2019.
[11] Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, 23 September 2020, COM (2020)591

reviewed and amended the European Commission's proposal and decided to begin negotiations on the final shape of these rules with EU countries in the Council.

The overall objectives of the above mentioned proposals are to: a) provide legal certainty; b) support innovation and remove regulatory obstacles which may be constraining Fintech development while mitigating risks arising from it; c) to protect European users, investors and business by enabling trust and confidence in the market integrity; and d) to maintain financial stability on European grounds . The proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger (under Article 6) aims in future to introduce new requirements where operators of DLT market infrastructures shall ensure that the overall IT and cyber arrangements related to the use of the DLT in place are proportionate to the nature, scale and complexity of their business. Likewise, DLT market infrastructure operators must inform competent authorities of any evidence of hacking, fraud, or other serious malpractice, as well as technical and operational difficulties which may pose risks to investor and user protection (under Article 9). Recognizing the gap that exist in relevant law, the European Parliament in the recommendations to the Commission on ``emerging risks in crypto-assets'' calls on the Commission to propose legislative changes in the area of ICT and cyber security requirements for the Union financial sector in order to address the inconsistencies, gaps and loopholes [26].

Existence of a Techno- Regulatory Gap and Difficulties of Applying Cyber-Measures in a Blockchain Setting

It can be argued that current and proposed regulatory measures may not fully resolve or mitigate cyber-attack risks pertaining to the usage of DLT and crypto assets. In the following sections we describe the regulatory gap that exists due to the legal, technological and operational specificity related to the use of DLT in the EU. Considering cyber resilience as a precondition to sustainable innovation in the blockchain and crypto-asset domains, we stress the absence of detailed guidance, security remedies, supervisory approaches and harmonization at an EU level. After summarizing some of the main security concerns maintained by the EU, we identify some of the inherit blockchain features that impose difficulties in assigning traditional regulatory measures and put a constrain to the scope of cyber regulation in the crypto-asset domain. We examine some of the opportunities as well as the concerns of assigning certain regulatory remedies and suggest several viable measures that may mitigate such cyber security risks.

Identification of a techno-regulatory gap and constraints to regulation in the blockchain and crypto-asset framework

The overall cyber arrangements of the proposed EU regulations aim to protect user funds from hacking, degradation, illegal access, loss, cyber-attack or theft, however not much further explanation of the required technical measures has been given. Besides security issues such as vulnerabilities in databases, protocols, APIs, etc. for which traditional cyber measures exist, current EU regulations don't include DLT specific cyber measures. For example, distinction among types of blockchain related attacks; threat agents; consensus design vulnerabilities; smart contract code reviews and assurances; defense techniques; liability measures, etc. has not been made. As noted, there are no safety requirements imposed on the protocols and smart contracts underpinning crypto-assets[12]. Likewise, the decentralized governance and open source nature of many public blockchains, poses challenges to traditional liability remedies as well fiduciary duty obligations for which no further recommendation has been noted. [27] argues that on-chain conduct may render issues of tortious liability and non-contractual disputes, for which further regulatory clarity is needed. In other words, certain blockchain-based transactions seem to bypass current regulatory control [28]. It can be argued that the blockchain model challenges in many ways traditional regulatory frameworks pertaining to cyber security whilst at the same time it brings software quality and assurances to the forefront, given the often-immutable nature of code and inability to update code, even if buggy.

The Commission acknowledged that market participants still remain unprotected against some of the most significant risks posed by crypto-assets (e.g. cyber-attacks) and recognizes that: "*regulatory gaps exist due to legal, technological and operational specificities related to the use of DLT*".[13] As noted, with further digitalization and adoption of crypto-assets cyber-attacks are set to grow. New types of cyber-attacks may bring consumer protection and market integrity issues. Moreover, the Commission recognizes (under paragraph 2.2.2) the existence of a regulatory challenge regarding third party service providers: "*crypto-asset trading platforms, exchanges, brokers, dealers and wallet services operate without proper cyber security*

[12] See (pg.11) of Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for Market Infrastructures based on Distributed Ledger Technology.
[13] See paragraph 4, (pg.11) of Proposal for a Regulation Of The European Parliament And Of The Council on a pilot regime for market infrastructures based on distributed ledger technology

arrangements" which imposes a threat to safeguarding users funds[14]. The EU proposal for regulation on digital operational resilience for the financial sector stresses the absence of detailed and comprehensive rules and supervisory approaches to digital operational resilience at EU level [25].

In general, crypto and blockchain regulations within the European Union have not been harmonized yet, thus allowing for national regulation to differ in several domains. As part of the latest regulatory proposal, the EU recognized the lack of legal standardization and harmonization within the union, asking for further actions to be taken into this direction. Nevertheless, the fast-evolving nature of blockchain technology and cyber-attacks and risks related to it poses the dilemma whether regulation can keep up with such technological change. Research shows a growing gap between emerging technologies and the law [29]. All in all, EU member states have been at different levels of regulatory maturity when it comes to regulating blockchains and crypto-assets [30]. Furthermore, while some risks have been mitigated in certain Member States that have introduced bespoke regimes on crypto-assets, market participants in other Member States remain unprotected against some of the most significant cyber risks. As noted in [25]: *"ICT-risk related provisions at Union level shows gaps or overlaps in important areas, such as ICT related incident reporting and digital operational resilience testing, and creates inconsistencies due to emerging divergent national rules or cost-ineffective application of overlapping rules. This is particularly detrimental for an ICT-intensive user like finance since technology risks have no borders and the financial sector deploys its services on a wide cross-border basis within and outside the Union.*"

A Pan-European approach may be essential for an effective cyber-security strategy due to the cross-border nature of public blockchains and crypto-asset applications. Thereby, we have outlined some of the main regulatory security concerns and risks regarding blockchain and crypto-assets in the EU:

a. Blockchain technology poses novel forms of cyber risks (e.g. cyber-attacks) that are not appropriately addressed by existing EU rules.
b. With further digitalization these cyber risks are set to grow is size and scale.
c. There are no safety requirements, detailed and comprehensive security rules imposed on the protocols and smart contracts underpinning crypto-assets.
d. Challenge of applying liability measures.
e. No proper cyber security arrangements for third-party service providers.

[14] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in crypto-assets.

f. Lack of regulatory harmonization among Member States.

Addressing the above-mentioned concerns via regulatory measures in order to mitigate cyber risks (e.g. cyber-attacks) is a challenging task that requires further discussion and analysis. Protecting users while enabling further innovation in the blockchain and crypto-asset domain may require for certain trade-offs between the two EU objectives.[15] In accordance, we have identified some of the main technical blockchain features that impose difficulties in assigning regulatory measures concerning cyber-attacks:

1. the decentralized (governance) nature of the blockchain system.
2. the anonymous/pseudonymous nature of network participants.
3. the cross-border nature of blockchains.
4. the immutable nature of smart contract code.

The decentralized nature of a "permissionless" blockchain system is one of the main appealing features of this technology. The system can often be characterized with decentralized governance structure where not one single and/or dominant entity is in charge of the design, operation and/or execution of the system protocol rules. This has brought in place a regulatory dilemma due to the lack of a distinguishable dominant decision-making authority which can be held accountable in case of a cyber-attack and to which certain cyber security requirements can be imposed. By a way of example, Bitcoin is one of the most noted decentralized blockchain-based application, where anyone can freely contribute resources to the network and the system operates thanks to the contributions of hundreds and thousands of users, collectively in charge of maintaining the network [31]. Also, as part of the rapidly evolving domain of decentralized finance (DeFi), decentralized exchanges (DEXs) allow for direct peer-to-peer cryptocurrency transactions without the need for a trusted intermediary. Although centralized exchanges are still more commonly used, DEXs offer certain features that can be considered as comparative advantages in the future.[16] DEXs transactions are characterized as non-custodial, automated, cross-border and pseudo anonymous [32].

[15] See (pg.1) of Reasons for and objectives of the proposal for a regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology.

[16] Compared to a 'centralized' exchanges, which can only be used for exchange of crypto assets, a DEX can use its chain to issue new crypto assets, trade that crypto asset, and record business transactions related to the crypto asset.

In many instances, the pseudonymous/anonymous nature of the system participants also adds constrains in identifying and enforcing any type of cyber requirements, assurances and penalties. Also, due to the cross-border nature of this system and the lack of regulatory harmonization on a European and global level adds to the difficulty of enforcing security measures. In other words, current cyber regulatory measures are often limited to blockchain based systems that are operated by private entities, organizations or communities where clearly distinguishable governance rules are set in place. All in all, it can be argued that applying cyber security requirements and assurance measures would be a challenging task in a truly decentralized setting.

In the following subsections we dive further into the above mentioned blockchain techno- regulatory constraining features, by exploring the possibilities to regulate blockchains via a) insiders (miners and developers) and b) intermediate points (e.g. exchanges). We continue by suggesting several viable regulatory remedies that may reduce the risk of cyber-attacks and reinforce the overall cyber-resilience of the system. We allude to the importance of technical and jurisdictional interoperability. Although establishing a Pan-European, harmonized cyber resilience approach pertaining to blockchains and crypto-assets may be an unattainable task at the moment, we highlight the example of Malta - a Member State whose current cyber regulation has managed to provide a more detailed, concise and promising approach to combating cyber-attacks and addressing other blockchain related vulnerabilities and risks.

Regulating `Insider' Adversarial Behavior?

Incentive design can be portrayed as a pay-for-performance reward system, which compensates individuals for their `honest' behavior [33]. The incentive design behind a blockchain system is crucial for its proper operation, nevertheless it does not always guarantee trust between unknown parties. Under certain premises of some PoW blockchains, participants can engage in strategic behavior, sometimes affecting the proper operation and security of the system. For example, some non-malicious forms of `collusive behavior', such as miners joining mining pools, may be essential for miners to beneficially participate in the system (e.g. due to the increased difficulty level of generating a block), although under certain premises mining pools can collude and act as a cartel and threaten the trustworthiness of the system [34]. Williamson maintains that trust can often be considered as an

antonym of opportunism, but in its essence `calculated cooperative behavior' is not a trustworthy behavior [35]. Nissembaum approaches trust in ICT as a conglomeration of two main factors, namely composed of insiders (e.g. developers, miners) and outsiders (e.g. hackers), maintaining that very often security issues can appear from an `adversarial insider' [36]. This perspective has been essential when analyzing blockchains, as the system operations are primarily maintained by `insiders', such as miners and developers, whose `dishonest' behavior may put the security of the system at stake. As maintained by Gambetta, trust in a system depends on the agency of others [37] and in the absence of trust in the agency of participants, further security measures are needed [38].

As is often the case for `public' blockchains, eliminating the need for a single decision-making entity replaces the top-down hierarchical organizational model with a system of distributed and bottom-up cooperation where each network participant is at the same time contributor and shareholder [39]. Arguably, regulatory frameworks ought to reflect the way economic incentives are propagated along with the structural roles of the agents involved [28].In this regard, certain studies have explored the possibility for regulating DLT via the agents who form part of the de facto governance structures of public blockchains, e.g., by exploring whether the imposition of certain fiduciary duties should be assigned to core developers and dominant miners [40] [41].

Nevertheless, certain challenges arise from this approach. Although protocol developers may exercise an influential role in the creation and implementation of certain software applications, [28] argues that protocol developers do not function as corporate fiduciaries, and labeling them as such would render negative effect in a blockchain framework. Also, treating core developers and miners as fiduciaries could discourage them from participating in what may be considered a socially beneficial project, due to a fear of potential liability---and without them contributing code and processing power (under PoW) the system risks disappearing [40]. Nevertheless, under certain conditions it may be favorable that developers working on smart contracts to be held legally responsible if they were able to ``reasonably foresee'' that their smart contracts will be used illegally.[17] Moreover, core developers and miners are usually not compensated enough to bare the accountability standard of a fiduciary, and in a different case of elevated compensation fees there could be a significant increase in the cost associated with using this technology. Increasing the `cost of participation' in a PoW system could

[17] Remarks of Commissioner Brian Quintenz at the 38th Annual GITEX Technology Week Conference, CTFC (Oct. 16, 2018)}

further motivate rational miners to group and form mining pools - which can act as a colluding power with propensity to increase in size until it becomes a majority, thus having the possibility to perform organized majority attacks [42]. [43] argues that blockchains are a more complex ecosystems where different liability rules may apply depending on a careful distinction of the operation level and use case (e.g. blockchain level, smart contract level, transaction level).[18]

Moreover, the anonymous/pseudonymous nature of network participants increases the challenges of assigning and enforcing regulatory measures [43]. In a narrow use of the concept, deterrence based on punishment in a decentralized setting may not be highly effective due to the anonymous/pseudonymous nature of the system. According to [44], punishment measures are less likely to be effective in the cyber sphere where the identity of the attacker is uncertain and there are many unknown adversaries. Another blockchain feature that presents challenges with enforceability, is the cross-border nature of the system and its participants. In other words, as in most cases of public blockchains, the operation of nodes is located in a vast amount of countries, hence associating and locating attackers (both insiders and outsiders) may increase the detection cost [43]. All in all, it can be argued that enforcing necessary measures such as penalties (as defined under Article 9 of 2013/40/EU) can be challenging when it comes to DLT. Furthermore, beyond adversarial risks, software bugs in smart contracts which may be due to negligence or oversight on behalf of a/the developer/s could lead to catastrophic events (of which many such events have taken place over the past decade). Detail in regard to measures to counteract such bugs are missing from that which has been proposed in present regulatory proposals.

Regulating third parties: 'central points' in a decentralized world

Although public blockchains are mostly decentralized, in the crypto-asset ecosystem the existence of service providers, including wallet providers, financial platforms and exchanges is still relatively centralized. These are the central points that often enable transactions between agents in the `crypto-world' and have grown to become an essential part of the system. However, their economic significance has made them a significant vulnerability point, whose exploitation can compromise a

[18] Recently, the European Union rejected a proposed amendment to MiCA that could have banned PoW cryptocurrencies such as Bitcoin and Ethereum across the European bloc. A last-minute addition to the bill aimed to limit the use of cryptocurrencies that are powered by the energy-intensive processes like proof-of-work (PoW) - as a way of the negative climate change consequence of the usage of this processes.

large part of the ecosystem. By way of example, wallets are essential for any crypto user – as in order to transact with a cryptocurrency, users need to control a cryptocurrency wallet (whether directly or indirectly). A wallet is often managed by a hardware device, a software program, or an online service which stores the private and public keys corresponding to the addresses associated with the user [45]. A wallet attack is an attack on wallet software or wallet service providers and its users, which could result in massive thefts and lead to an overall decrease of trust in the system [18]. In the last years, exchange platforms and wallet service providers have often been a target of `large-scale' cyber-attacks amounting to millions of euros. For example, Coincheck exchange was hacked in January 2018 resulting in losses of around 500 million U.S. dollars [46]. Also, although beyond the scope of this paper, it is worth mentioning that recent concerns over money laundering and terrorism funding activities due to the anonymity feature of crypto exchanges' users, has sparked another regulatory urge over establishing a regulatory frame.[19]

DORA acknowledges that despite the high cyber risk associated with the operation of third-party service providers, this has been barely addressed in Union legislation. As noted, the lack of proper measures at Union level is compounded by the absence of specific mandates and tools allowing for national supervision and monitoring.[20] With the increased adoption and usage of crypto-assets, the DORA acknowledged the existence of regulatory gap and alluded to the need of harmonized oversight and monitoring framework, in order to tackle risks stemming from ICT third-party service providers, including concentration and contagion risks for the EU financial sector.[21] Moreover, the proposal underlines that there is a need of regulatory measures that will establish a suitable ICT risk management framework, including ICT-related incident reporting, testing and oversight of critical ICT third-party service providers. In order to avoid significant losses, crypto exchanges may need to implement comprehensive security standards, where vulnerability points are identified and properly addressed. In the case of wallet attacks on crypto exchanges or wallet service providers, some

[19] In 2020 a new Anti-Money Laundering Directive (6AMLD) came into force. The Directive has important implications for crypto currencies and further toughens rules around information on the beneficial ownership of companies and trusts.

[20] See paragraph 28. (pg. 18) of Regulation of the Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014}.

[21] See (pg.3) of Regulation of The European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014}.

regulatory remedies to mitigate cyber risks and reduce the burden from affected parties can be done through:

- imposition of capital requirements as well as a guarantee to return of certain percentage of stolen funds to users in case of a cyber-attack;
- requirement for an exchange to block transacting operations for a certain amount of time if certain types of attacks are noticed.
- ability to issue cyber-insurance

Under Annex III of MiCA, crypto-asset service providers could become subject to capital requirements, governance standards, and the obligation to segregate their clients' assets from their own assets and will be subject to IT requirements to avoid the risks of cyber thefts and hacks. In other words, MiCA proposes that crypto-asset service providers are held liable for damages resulting from an ICT-related incident, including an incident resulting from a cyber-attack, theft or any malfunctions.[22] This may however imply higher monitoring costs for the exchanges and increase the overall cost of operating and transacting with cryptocurrencies. In the case of theft of coins via a deep chain reorganization, an exchange may act by blocking transacting operations for a certain amount of time. For example, in January 2019 Coinbase detected a deep chain reorganization of the Ethereum Classic blockchain, and immediately paused interactions with the ETC blockchain to protect customer funds. The cost of the attack (in double spends) amounted to around 1.1 million dollars. In this event, the early detection and pause of transactions of Coinbase protected users' funds, while another popular exchange Gate.io, lost around 200,000 dollars to the attacker [47]. An alternative way to protect users' funds could be implemented in the form of a `crypto insurance' option issued by exchange platforms [48]. Imposing a cyber-security insurance may help differentiate between users who are more risk averse. This could reduce compliance burden by minimizing regulatory intervention where the risks are relatively low and maximizing efficiency through the implementing insurance fee to areas where cyber-attack risks are the highest.

[22] See Paragraph 2.2.2 (pg.17) of Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets

Deterrence by Prevention: Viable Risk-Mitigating Measures

Several EU directives[23], including the new regulation proposals on crypto assets and DLT infrastructure, allude to the need for reinforcing `soft measures' that can act as possible risk-mitigating measures, preventing or diminishing the negative consequence of a given cyber-attack [12] [17]. Soft security can refer to immediate security measures which do not require costly investment. In this regard, as possible viable measures we note the following:

a. Monitoring
b. Increasing Awareness of users
c. Early Detection
d. Timely Reporting
e. Technology and security audits
f. Employee compliance standards (where applicable)

Monitoring a public blockchain to detect potential attacks can be considered a viable measure, although certain technical expertise and monitoring cost is required [49]. By way of example, the BTG majority attack in 2020 was discovered by a researcher at MIT's Digital Currency Initiative. Monitoring increases the probability of early detection which can reduce negative consequences [13]. As noted, attack monitoring helped Coinbase safeguard users' funds [50]. Investing in cyber-detection techniques may be one of the possible ways of protecting users. For example, a deep learning approach for detecting security attacks on blockchain has been suggested as plausible solution to monitor the security of blockchain transactions and detect potential 51\% attacks. Another study by [51] explored the possibility for early detection of crypto ransomware using pre-encryption detection algorithms. Timely reporting of attacks may also reduce the negative consequences. As seen in [17] markets react to information regarding cyber-attacks and timely notification may make a difference in safeguarding users funds. The EU Parliament has suggested the creation of centralized data hubs for incident reporting which would help identify weaknesses to be addressed within European financial markets.[24]

[23] See Directive 2013/40/EU and Directive (EU) 2016/1148

[24] Establishing a single EU Hub for major ICT-related incident reporting by financial entities. See (pg. 10) of Proposal for a Regulation of The European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC).

Moreover, as noted in previous studies, user awareness policies were found to significantly increase cybersecurity action skills [52]. All BitThumb, NiceHash, and YouBit exchanges attacks involved a compromised access to exchanges' employee login details. In accordance, regulatory remedies may need to ensure certain compliance standards among employees as well as technology and security audits. Security screenings and audits may likely decrease vulnerability points and increase cyber resilience.

The Case of Malta: An in-depth cyber approach to blockchain regulation

In order to provide legal certainty to operators, instill market integrity, protect investors and stakeholders and encourage the use and adoption of blockchain technology, the Maltese parliament enacted three laws enabling blockchain based businesses: the Malta Digital Innovation Authority Act, the Innovative Technology Arrangements and Services Act and the Virtual Financial Assets Act. It was acknowledged that the new technological challenges that blockchain brought forth would not only impinge on the financial cryptocurrency related sector, but in any other sector where the technology will be used. Within its regulatory regime empowered through the Innovative Technology Arrangements and Services Act, the MDIA developed a Blockchain, DLT and Smart Contract certification framework [23] which includes a system audit - a rigorous process requiring an independent system auditor and subject matter experts to amongst other diligence checks to verify that the system is implemented as per a blueprint or specification. System Auditors are required to ensure a laid out set of control objectives are met [53], which includes amongst other aspects:

a. functionality and code review
b. vulnerability, incident and security management
c. disaster recovery
d. risk management
e. cyber security

The system audit process is a precautionary measure in attempt to mitigate risks by reducing the likelihood of negative events from occurring. The certification framework also stipulates features to ensure that if a negative event occurs that remedial action is taken through: (i) a `Forensic node', an independent system which must log all relevant information for the respective system undergoing

certification to enable for post-mortem investigation and also to facilitate any post-event actions as required; and (ii) a `Technical Administrator' must be available to act to their best capacity to undertake any remedial actions which may include stopping systems and alerting stakeholders (amongst any other action which may resolve any issues that arise).

One challenge to implementing such a regulatory framework is that of appropriate human resources. Having the regulator undertake system audits itself raises two issues: (i) it would be a challenge to ensure the availability of the varied required expertise, and given that limited expertise is often available in general, such an approach where the authority would resource itself would further eat into the limited expertise available on the market; and (ii) if the authority itself would conduct audits then whilst it would be independent of the software operation, it would not be independent of the audit itself. An alternative (and the adopted) solution is to have system audits undertaken by third party service providers. A similar issue may arise with system auditors requiring to recruit subject matter experts for specific system audit engagements and therefore a similar approach was also taken to allow for system auditors to make use of third-party subject matter experts (subject to having sufficient agreements in place). To put sufficient assurances in place to ensure the quality of system auditors and their subject matter experts, the authority would then vet and scrutinize each involved party (both on technically and on other aspects of due diligence).

Rather than pose mandatory technology focused regulation, e.g. regulation for all blockchain systems, such technology-based regulation is mandated through specific laws or by other national competent authorities - alternatively, the technology regulatory framework established by the MDIA is voluntary. This is the regulatory balance that Malta found to both allow for blockchain innovation to flourish whilst mandate required technology focused assurances where required. For cryptocurrency-based activities, classified as Virtual Financial Assets (VFA) in the Virtual Financial Assets Act, the Malta Financial Services Authority mandates a systems audit and certification where required. More specifically then, the Malta Financial Services Authority, on top of the required system audit further defines cybersecurity principles established in a guidance document which focuses on technical aspects of VFAs, postulating cyber security practices in a more flexible yet detailed manner [54]. The document views each cyber regulatory proposal from three different yet equally important aspects: (i) People, (ii) Processes and (iii) Technology. As a first step into a more concise and effective regulatory

measure, the document gives the establishment of an Information Security Policy (ISP) covering among others:

a. Threat Agents (e.g. script kiddies, hackers, insiders, etc.);
b. Malware, phishing, DDoS attacks;
c. Hacking of a website/ web application;
d. Protocol design errors
e. Disruption of critical infrastructure of other parties;
f. Other cyber-attacks on the ICT infrastructure (software and/or hardware, insider-threats, etc.)

The document goes even further, alluding to the establishment of a comprehensive and in-depth inquiry regarding cyber incidents, where an analysis pertaining to the detection, target and method of attacks are made. Investigations relating to cyber security incidents are designed to assess the following: (i) the origin of the attack; (ii) the attackers' possible scope; (iii) the attack's blast radius; and (iv) whether the attack had any significant impact on the system.

Security awareness, training, compliance and auditing are also part of the suggested regulatory measures. Proactive measures such as: leading and coordinating cyber defense management processes; overseeing implementation and monitoring cyber risks; initiating and executing cyber exercises; undertaking cyber defense control assessment; etc. are considered as part of the cyber defense strategy. With regard to service providers such as exchanges, brokers, wallet service providers, etc. the regulations set out four license classes with a different set of considerations among which review of cryptographic algorithms and crypto-key configurations through rigorous testing on all cryptographic operations (encryption, decryption, hashing, signing); key management procedures (generation, distribution, installation, renewal, revocation and expiry), as well as testing in line with industry-standard statistical tests for randomness.

Fiduciary duties in the blockchain setting have also been discussed under the Innovative Technology Arrangements and Services Act. The term `Innovative Technology Arrangements' (ITAs) is used to refer to software artefacts and architectures including an aspect of distributed ledger technology (DLT), blockchain or smart contracts. For an ITA to be certified, it must undergo an in-depth systems audit [55]. On that basis, core developers will normally have to demonstrate that they have observed

and meet the duty of care standards thus limiting liability exposure. However, if found to be acting negligently, in bad faith or dishonestly and their actions caused damages, then they will be held personally liable. Miners can be treated under certain circumstances as administrators, contractors, agents and/or negotiorum gestor. In certain situations, under Maltese law, this can be considered a quasi-contract which can trigger fiduciary obligations [55].

Conclusion

The technological change and pace thereof being witnessed in the cryptocurrency and blockchain sector poses an ever moving `regulation defying' target - for which a regulatory balance must be found to both promote innovation whilst also protecting stakeholders' interests. Jurisdictions around the world have and are investigating different approaches to regulating the sector. In this paper, we delved into efforts being made by the EU to provide cyber security assurances (in the domain of blockchains and crypto-assets) through its proposed regulatory framework. However we maintain that this bring to light a techno- regulatory gap emerging from the proposed frameworks by delving into risks for which sufficient measures have not been provided. We suggest viable regulatory measures and highlight jurisdictions that have already provided solutions to some of the issues raised. We argue that regulatory frameworks may need to adjust to reflect, both the way economic incentives are propagated and also the structural roles of the agents involved in blockchain systems. We maintain that having a clear understanding of blockchain systems and how cyber risks can be mitigated could determine the extent of acceptance of blockchain technology and crypto-assets within the European community.

Bibliography

[1] D. Vujicic, D. Jagodic and S. Randjic, "Blockchain technology, bitcoin, and ethereum: A brief overview.," *INFOTEH 2018-Proceedings ,* 2018. https://ieeexplore.ieee.org/document/8345547

[2] S. Zhang and J. Lee, "Analysis of the main consensus protocols of blockchain," no. https://www.sciencedirect.com/science/article/pii/ S240595951930164X, 2019.

[3] A. Ferreira, " Regulating smart contracts: Legal revolution or simply evolution?," *Telecommunications Policy 45, 102081 ,* 2021.

[4] M. Alharby, A. Aldweesh and A. Moorsel, "Blockchain-based smart contracts: A systematic mapping study of academic research (2018). . https://doi.org/10.1," *International Conference on Cloud Computing, Big Data and Blockchain (ICCBB).,* p. pp. 1–6, 2018.

[5] A. Hayes, "Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin.," *Telematics and Informatics,* vol. 34, no. https://doi.org/10.1016/j.tele.2016.05.005, 2017.

[6] European Securities and Market Authority:, " Advice - initial coin offerings and crypto-assets," Vols. https://www.esma.europa.eu/sites/default/files/ library/esma50-157-1391_crypto_advice.pdf, 2019.

[7] Carbon Black, "Cryptocurrency gold rush on the dark web," 2018. https://www.vmware.com/resources/security/cryptocurrency-gold-rush-on-the-dark-web.html

[8] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua and S. Shetty, "Exploring the attack surface of blockchain: A systematic overview.," *ArXiv abs/1904.03487,* 2019. https://arxiv.org/abs/1904.03487

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009.

[10] R. Zhang and B. Preneel, "Lay down the common metrics: Evaluating proof-of-work consensus protocols' security.," *IEEE Symposium on Security and Privacy (SP),* p. pp. 175–192, 2019. https://ieeexplore.ieee.org/document/8835227

[11] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments.," *Energy Reports ,* p. https://www. sciencedirect.com/science/article/p, 2021.

[12] A. Abhishta, R. Joosten, S. Dragomiretskiy and L. Nieuwenhuis, "Impact of successful ddos attacks on a major crypto-currency exchange," 2019.

[13] B. Bambrough, " Bitcoin rival suffers devastating attack," January 2020. [Online]. Available: https://www.forbes.com/sites/billybambrough/2020/01/28/ bitcoin-rival-suffers-devastating-attack/#7a462dafcb73.

[14] CoinDesk , "Crypto investors have ignored three straight 51% attacks on ETC," 2019. [Online]. Available: https://www.coindesk.com/markets/2020/09/08/ crypto-investors-have-ignored-three-straight-51-attacks-on-etc/.

[15] Reuters, "Bitcoin worth 72 million stolen from bitfinex exchange in hong kong," 2016. [Online]. Available: https://www.reuters.com/article/ us-bitfinex-hacked-hongkong-idUSKCN10E0KP.

[16] Self Key, "list-of-cryptocurrency-exchange-hacks," url{https://selfkey.org/ list-of-cryptocurrency-exchange-hacks/}, 2019.

[17] S. Ramos, F. Pianese, E. Oliveras and T. Leach, "A great disturbance in the crypto: Understanding cryptocurrency returns under attacks.," *Blockhain Applications,* 2021.

[18] M. Guri, "Beatcoin: Leaking private keys from air-gapped cryptocurrency wallets.," *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing ,* 2018.

[19] Yahoo, "Bug affecting ethereum network leads to fork„" [Online]. Available: https://finance.yahoo.com/news/ bug-affecting-ethereum-network-leads-170500387.html.

[20] I. Mehar, C. Shier , E. Gong and A. Giambattista , "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack," 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3014782

[21] European Commision, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology COM/2020/594 final," *eur-lex.*

[22] Fortune, "Basel Committee puts bank holdings in Bitcoin and crypto in its highest risk category," https://fortune.com/2021/06/10/basel-bitcoin-crypto-capital-requirements-risk-category/, 2021.

[23] J. Ellul, M. Ganado, J. Galea, S. Mccarthy and G. Pace, "Regulating blockchain, dlt and smart contracts: a technology regulator's perspective.," 2020.

[24] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937," *eur-lex,* 2020.

[25] E. Commision, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014," *Eur-lex,* 2020.

[26] European Parliament, "Digital finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets," https://oeil.secure.europarl.europa.eu/oeil/ popups/ficheprocedure.do?lang=en\, 2020.

[27] Blockchain Observatory Report, "Legal and regulatory framework of blockchains and smart contracts," https://www.eublockchainforum.eu/sites/default/files/reports/report_ legal_v1.0.pdf, 2019.

[28] R. Haque, R. Seira, B. Plummer and N. Rosario, "Blockchain development and fiduciary duty," 2019.

[29] G. Marchant, "The growing gap between emerging technologies and the law.," *Springer,* p. pp. 19–33., 2011.

[30] Blockchain observatory forum, "Eu blockchain ecosystem developments. a thematic report prepared by the european union blockchain observatory & forum (2020)„," 2020.

[31] P. De Filipi, "Blockchain technology and decentralized governance: The pitfalls of a trustless dream.," *Cyberspace Law eJournal ,* 2019.

[32] M. Yano, C. Dai, K. Masuda and Y. Kishimoto, Blockchain and Crypto Currency., Springer, 2020.

[33] J. Chiu and T. Koeppl, " Incentive compatibility on the blockchain.," *Springer,* p. pp. 323–335. , 2019.

[34] T. Schrepel, "Collusion by blockchain and smart contracts.," *Harvard Journal of Law and Technology ,* 2019.

[35] O. Williamson, "Opportunism and its critics.," *Managerial and decision economics,* p. pp. 97–107, 1993.

[36] H. Nissenbaum, " Securing trust online: Wisdom or oxymoron.," 2001.

[37] D. Gambetta, "Can we trust trust?," 2000.

[38] B. Schneier, " Liars and outliers: enabling the trust that society needs to thrive.," 2012.

[39] A. Pazaitis, P. De Filippi and V. Kostakis, "Blockchain and value systems in the sharing economy: The illustrative case of backfeed.," *Technological Forecasting and Social Change ,* p. 105–115 , 2017.

[40] A. Walch, "Call blockchain developers what they are: Fiduciaries.," *American Banker,* 2016.

[41] M. Ganado, J. Ellul, G. Pace, S. Tendon and B. Wilson, "Mapping the future of legal personality," 2020.

[42] I. Eyal and G. Sirer, " Majority is not enough: Bitcoin mining is vulnerable.," 2018. https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

[43] E. Frommelt, " Liability challenges in the blockchain ecosystem.," *Business Law Journal ,* 2021.

[44] J. Nye, "Deterrence and dissuasion in cyberspace.," *International security,* 2016.

[45] M. Aydar, S. Cetin, S. Ayvaz and B. Aygun, " Private key encryption and recovery in blockchain," 2019.

[46] BBC, "Coincheck: World's biggest ever digital currency 'theft," https://www.bbc.com/news/world-asia-42845505, 2018.

[47] M. Orcutt, "Once hailed as unhackable, blockchains are now getting hacked," 2019. [Online]. Available: https://www.technologyreview.com/2019/02/19/239592/ once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

[48] R. Sharma, "Cryptocurrency insurance could be a big industry in the future „" 2021. [Online]. Available: https://www.investopedia.com/news/ cryptocurrency-insurance-could-be-big-industry-future/.

[49] "Report on the cost of third-party cybersecurity risk management," https://cdn2.hubspot.net/hubfs/2378677/Content-Assets/CyberGRX\ %20Ponemon\%20Report.pdf}, 2019.

[50] M. Nesbitt, " Ethereum classic (etc) is currently being 51% attacked," url{https://blog.coinbase.com/ ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de}, 2019.

[51] S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Prevention of cryptoransomware using a pre-encryption detection algorithm.," 2019. https://www.mdpi.com/2073-431X/8/4/79

[52] M. Choi, Y. Levy and A. Hovav, "The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse.," 2013. https://aisel.aisnet.org/wisp2012/29/

[53] Malta Innovation Authority, "Systems auditors guidelines," https://mdia.gov.mt/sa-guidelines/, 2019.

[54] Malta Financial Service Authority, "Guidance Notes on Cybersecurity," 2019. https://www.mfsa.mt/wp-content/uploads/2019/06/Cybersecurity-Guidance-Notes.pdf

[55] M. Ganado, " Blockchain versus the law," 2019. https://ganado.com/wp-content/uploads/2019/11/Ganado.pdf