Blockchains in the Real World: An Interdisciplinary Perspective on Enhancing Security and Adoption

Simona Ramos

TESI DOCTORAL UPF / Year 2023

THESIS SUPERVISOR
Dr. Fabio Pianese and Dr. Ester Oliveras Sobrevias
Department of Information and Communication Technologies
Engineering (ETIC)

Thanks

Embarking on a Ph.D. journey is akin to setting sail on an uncharted sea, where the pursuit of discovery intertwines with the daunting challenges that lie ahead. For me, these four years have been a soul-stirring journey, a profound transformation that goes beyond the realms of academia. For this, my gratitude extends to all those who have stood by my side throughout this journey.

To my dearest mother, whose support breathed life into the pursuit of this Ph.D., a venture I might have overlooked. To my father, a symphony of hard work and ambition, a perpetual melody echoing inspiration through my every endeavor. To my sister, my cherished confidante, my best friend and the sorceress of laughter. To Arthur, my volley and life partner, an unwavering pillar of support over these transformative years. Your encouragement, understanding, and shared joys have been the cornerstone of this journey. To my friends scattered across borders and those nestled in Barcelona. To my volleyball family, here's to the thousands of games we've conquered and those we've gracefully surrendered. This sport has been a profound teacher, imparting lessons in team spirit, discipline, and the essence of pure fun.

To my esteemed advisors, Fabio, Vanesa, and Ester, a heartfelt gratitude for your support. Fabio, your critical insights and generous assistance have made you both my most vocal critic and my greatest ally, guiding me through the intricate labyrinth of academic research. Likewise, thank you for making Paris feel less 'gray' during the confusing beginnings of my Ph.D. journey and the Covid times. Vanesa, though our interactions during the research were limited, your presence was a beacon during my stay at UPF, always supportive and welcoming. Your positive energy and readiness to help left a lasting impression.

To my colleagues - Abhi, Philemon, Arathxa, Massood, Mohamed, and Sina - your vibrant spirits have infused joy into the tapestry of my Ph.D. life. Thank you for turning the journey into a cheerful symphony.

To Dr. Joshua Ellul, your invaluable contributions have made me feel a true sense of belonging within the complex realm of interdisciplinary research. Thank for your collaboration and meaningful insights.

To the dynamic duo, B and J, colossal thanks for steering me into the exhilarating realm of blockchains, revealing a whole new universe with unprecedented possibilities!

Abstract

This thesis investigates the complex nature of the blockchain ecosystem, where technology, law, and economics intersect across layers and applications. By offering an interdisciplinary perspective on blockchains, we seek to understand both their potential as well as their vulnerabilities. With a specific emphasis on blockchain cybersecurity, this thesis sheds a light to the diverse attack vectors targeting cryptocurrencies, blockchains, and associated entities, aiming to evaluate their economic impact using publicly available data. Furthermore, the study delves into the legal and regulatory frameworks pertinent to blockchains and crypto-assets, recognizing and addressing the technical limitations that impede regulatory intervention. We explore the economic and cybersecurity challenges associated with MEV, including practices like front-running and sandwich attacks, which are deemed illegal in traditional financial markets. The thesis also analyses smart contracts, examining their complex relationships with users and the resulting 'information gap'. Finally, we explore the blockchain's potential as a normative tool, facilitating disintermediation and transparency in multifaceted use cases, such as AI applications and renewable energy communities.

Resumen

Aquesta tesi investiga la naturalesa complexa de l'ecosistema blockchain, on la tecnologia, el dret i l'economia es creuen entre capes i aplicacions. En oferir una perspectiva interdisciplinària sobre les cadenes de blocs, busquem entendre tant el seu potencial com les seves vulnerabilitats. Amb un èmfasi específic en la ciberseguretat de blockchain, aquesta tesi il·lumina diversos vectors d'atac dirigits a criptomonedes, blockchains i entitats associades, amb l'objectiu d'avaluar el seu impacte econòmic mitjançant dades disponibles públicament. A més, l'estudi aprofundeix en els marcs legals i reglamentaris pertinents a les cadenes de blocs i els criptoactius, reconeixent i abordant les limitacions tècniques que impedeixen la intervenció reguladora. L'estudi explora els contractes intel·ligents, examinant les seves complexes relacions amb els usuaris i el 'buit d'informació' resultant. Finalment, examinem el potencial de la cadena de blocs com a eina normativa, que facilita l'arbitratge, la desintermediació i la millora de la ciberseguretat en casos d'ús multifacètics, com ara les aplicacions d'IA i els mercats d'energies renovables.

Contents

List of Figures

List of Tables

Chapter 1

INTRODUCTION

> Breakthrough innovation occurs when we bring down boundaries and encourage disciplines to learn from each other.
>
> *Gyan Nagpal*

1.1 On Blockchains

The origin of ledgers dates back thousands of years. Their usage has been significant across industries [4]. In the inception of the conventional banking system, institutions authenticated data records manually for centuries until the introduction of computers led to the digitization of ledgers, transforming the banking system although still mirroring the practices originally conducted on paper. The early computer networks brought the concept of distributed computing in the 1960s, when scientists began to explore new ways to connect multiple computers to share resources and work collaboratively [5]. Over the years, this field developed in different directions, popularizing the concept of peer-to-peer (P2P) networks in the 1990s-2000s [6]. In a P2P network, participants could directly interact and share resources (e.g., file sharing applications such as Gnutella or BitTorrent) without relying on a central server [6].

In 2009, Satoshi Nakamoto (a pseudonymous figure) introduced Bitcoin, a cryptocurrency based on a public blockchain that sparked a transformative revolution in the world of finance and digital technology [7]. A public blockchain is a peer-to-peer distributed ledger technology (DLT) that records transactions between two or more parties in a verifiable and permanent way by storing them as a sequence of blocks. In such a system, anyone can trade a digital cryptocurrency

without the need for a trusted central authority (e.g., a bank).

In computer science, decentralization is a concept that refers to the distribution or dispersion of control, power, resources, or decision-making across multiple entities or nodes within a network or system [8]. In a fully decentralized system, there is no single central node or authority that holds complete control over any aspect of the system. Instead, decision-making and control are distributed among various participants or nodes, often aiming to achieve a more democratic, transparent, and resilient infrastructure. In contrast to public (permissionless) blockchains, private blockchains differ in the way their membership is restricted (or permissioned), as only parties that are granted access by a controlling authority are able to use the ledger [9]. In private blockchains, access control is usually centralized and parties are verified using similar techniques as found in centralized systems (PKI, certificate chains, etc.). The novelty of public blockchains as a trust-less and fully decentralized system greatly motivates our interest in these unusual artifacts.

In a public blockchain, the interconnected chain of blocks is typically safeguarded by cryptographic techniques and a randomized lottery mechanism. Each block includes a secure digest or hash (a unique digital fingerprint) of the preceding block, an verifiable proof from the lottery process, a timestamp, and a list of unique transactions. Therefore, once a transaction is recorded and stored within a block, it cannot be tampered without modifications to the entire series of following blocks [10]. Hashes enable anyone to verify the integrity of the data. Hence, any alteration in the original data would result in a completely different hash, making it nearly impossible to tamper with the data without detection.

One of the most important parts of Nakamoto's work is the development of the **Proof of Work (PoW)** consensus mechanism which Nakamoto borrowed from the HashCash scheme introduced in 1997 by Adam Back [7]. PoW aims to solve the Byzantine Generals Problem with an unknown number of participant nodes by inducing an unforgeable computational effort, thus preventing quorum attacks where an adversary simply controls a large number of nodes. **Byzantine Generals Problem** is a key problem in distributed computing. It describes a situation in which the system's actors must agree on a consistent outcome, even though some of these individuals are unreliable or downright malicious [11].

PoW works as a lottery mechanism where a node that solves a computationally-intensive random search operation is allowed to create a new block. The node that first solves a cryptographic puzzle set by the rules of the network is the one that gets to create the next block in a process called mining [12]. In general, the higher the relative computational power available to a miner, the greater the likelihood of finding a valid solution before a less-endowed competing miner. Then, other participants in the network validate the proof of work by independently verifying that the hash of the new block meets the required criteria, thus establishing a consensus. PoW belongs to the probabilistic-finality consensus mechanism category,

as the finality of a block is not absolute but probabilistic. Under PoW, once a block is added to the blockchain, it is considered final, but this finality comes with a certain probability depending on the number of blocks added on top of a particular block. The higher number of blocks mined after a certain block the higher the probability of its finality [13].

With PoW, Nakamoto introduced a groundbreaking concept by incorporating economic incentives in the form of cryptocurrency rewards [7]. Miners, who actively contribute computing power (and equipment), are motivated by the prospect of receiving tokens of economic value, such as Bitcoin. This innovation is considered a crucial element in the realm of distributed systems, aiming to establish a truly decentralized transaction ledger. Here, the system positions miners as rational agents which try to maximize their gains by adhering to the rules of the network. The design ensures that no specific party, including miners, requires trust for the system to function as intended and for consensus to be reached among participants. The incentives built into the system are rooted in game theory, providing a framework to understand the circumstances under which rational players, like miners, may choose to collaborate or collude, potentially challenging the established rules of the system [14, 15]. Tokenomics, a relatively recent concept, emerges from the synergy between tokens (typically generated on a blockchain) and economic incentives, often rooted in the principles of game theory [16]. A digital token is a broad term referring to a digital representation of value that can serve various purposes. Today, many digital tokens are known as cryptocurrencies or crypto-assets, such as the Bitcoin (BTC). The definition of crypto-assets varies amongst jurisdictions. At a EU level, *"digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology"* are referred as crypto-assets [17]. The European Union's regulation distinguishes between different crypto-asset categories (e.g., asset-referenced tokens, electronic money tokens and other crypto-assets not covered by existing EU law such as utility tokens) [17]. Nevertheless, in this thesis we use the terms crypto-assets and cryptocurrencies interchangeably, making category specific distinctions only when relevant to the discussion.

Today, cryptocurrencies are built upon different consensus mechanisms among which, Proof-of-Work (PoW) and Proof-of-Stake (PoS) are the most prevalent. The Proof-of-Stake (PoS) consensus mitigates one of the most criticized aspects of PoW - the high power consumption needed for its operations. In PoS, rather than relying on computing power to mine a block, nodes known as validators, are required to lock up a form of 'security deposit' in a given cryptocurrency (e.g., ETH) in order to participate in the consensus. Using the security deposit incentivizes nodes to act honestly, keeping the network secured [18, 19]. Under PoS, the more coins a node holds, the higher probability they have to validate a blockchain transaction and be rewarded.

1.2 Blockchains and Cyber Security

Even though public blockchains introduce groundbreaking concepts, they come with their own set of constraints and vulnerabilities. The blockchain ecosystem possesses a complexity that extends well beyond the simplified portrayals it typically receives [20, 21]. Its security landscape is multifaceted, encompassing intricate set of cyber vulnerabilities across use cases and applications. The rapid adoption of cryptocurrencies and the lucrative nature of their trading have positioned them as an important and dynamic asset class within the broader financial landscape, drawing significant attention from users, investors, businesses, and regulatory bodies worldwide. Nevertheless, this has also increased the number and sofistication of attacks targeting cryptocurrencies and the underlying blockchain technology, costing users millions of euros [22, 23].

Attacks that target incentive design in blockchains are of paramount importance due to their potential to undermine the fundamental principles of security, decentralization, and trust that blockchain technology seeks to establish [20]. Incentive mechanisms are integral to motivating participants, such as miners or validators, to behave in ways that contribute to the overall health and security of the network. By exploiting or manipulating these incentives, malicious actors can disrupt the intended operation of the blockchain system, leading to a range of undesirable outcomes, including double-spending, transaction censorship, and a breakdown in consensus [21]. As noted by [22], majority (or 51% attacks) have been common in the last years. 51% attacks occur when a miner (or group of miners) controls 51% or more of the computational power in the network. Such a scenario empowers the attacker to manipulate transactions, potentially leading to the double spending of the same cryptocurrency [21]. The increased propensity of joining mining pools (e.g., due increased difficulty level of finding a block) have affected the ability of the incentive mechanism to ensure decentralization and security resistance over the possibility of majority attacks.

Managing incentives to strengthen the security is not an easy task. Often, increasing the security means a trade-off with the decentralization and scalability. For example 'sharding' mitigates a problem of network congestion attributed to a significant volume of transactions demanding substantial computational resources, but it makes blockchains more easily corruptible, especially through 51% attacks. This example brings to the forefront the Buterin Trilemma [2]. Vitalik Buterin, the founder of Ethereum argued that achieving high levels of scalability, security, and decentralization simultaneously is a challenging trilemma, as improving one aspect often comes at the expense of the other two. The tendency for centralization brings to the forefront the issue of a single (central) point of failure - which decentralized technologies promise to avoid. There are different instances of centralization in the blockchain ecosystems, such as mining central-

ization (under PoW), wealth concentration (under PoS), wallet ownership concentration (e.g., in centralized exchanges), etc.

From a computer science perspective, blockchain systems can manifest **centralization** in both logical and practical forms, each presenting distinct challenges to the overall security. We define logical centralization as centralization that arises when factors such as reduced randomness in selecting miners, or on-chain incentives favoring those with dominant computing power, introduce a concentration of influence. This scenario can compromise the decentralization principle, potentially leading to the dominance of a few powerful entities in the network. On the other hand, practical centralization occurs when users predominantly transact through major centralized exchanges (or other service providers) consolidating control within a limited number of platforms. These forms of centralization have varying impacts on security. Logical centralization poses risks to the fundamental tenets of decentralization and cybersecurity. On the other hand, practical centralization introduces vulnerabilities related to data privacy and potential points of failure such as leak of wallet IDs, but can also have a diminishing effect on user's confidence in the blockchain ecosystem and its services.

Real-world blockchains form intricate ecosystems, typically involving numerous stakeholders, users, applications, and service providers. This complexity expands the potential vectors for attacks and introduces *a broader spectrum of vulnerabilities, extending beyond the confines of the consensus mechanism* [20]. For example, the ability for miners (or validators) to order transactions within a block can create an important challenge in the blockchain ecosystem which can consequently impact users and the overall security. Miner (or maximum) extractable value (MEV) is a measure of the profit a miner (or validator, sequencer, etc.) can make through the ability to arbitrarily include, exclude, or reorder transactions within the blocks they produce - driven by the economic incentives tied to transaction fees [24]. When transacting, users attach fees to their transactions to encourage miners to prioritize the inclusion of their transactions within a block. Paired with the presence of a decentralized market exchange where cryptocurrencies are traded by smart contracts depending on consensus outcomes, targeted exploitation of MEV can lead to front-running, back-running, and sandwich attacks [23]. These types of attacks which occur when a entity such as a miner (or validator) manages to attach their own transactions before and/or after the user's transaction, performing a financial arbitrage and extracting profits - an action illegal in traditional financial markets (e.g., stock exchange and broker). Statistics show that MEV is worrisome as one out of 30 transactions might have been added to the blockchain for this purpose, while MEV related sandwich attacks are estimated to have cost users about 90 million dollars in 2022 [25, 26, 27].

The presence of **smart contracts** introduces a vulnerability that extends the potential impact of attacks in the blockchain ecosystem. In 2013, Ethereum intro-

duced a virtual machine that enabled the decentralized execution of blockchain-resident programs, known as smart contracts, without the need for third-party intervention [28]. Within this framework, participants can autonomously coordinate complex sets of contractual relationships in a peer-to-peer fashion, adhering to protocols and rules embedded within executable code [29, 30]. Smart contracts provide transparency to the various stakeholders since their code (actions and terms) is public and cannot be changed, as they are immutably stored and executed on a blockchain [31]. Decentralized applications (DApps) function autonomously on a blockchain through the execution of smart contracts, while a decentralized autonomous organization (DAO) is a collective decision-making body run by its members through a set of smart contracts, rather than being controlled by a centralized authority [32].

The widespread integration of smart contracts across various use cases has elevated both their significance and susceptibility to potential attackers. The issue of bugs emerges in smart contracts, some a result of complex logic and some due to a typo, an incorrect line of code, or a mistaken order in two (or more) lines of code [33]. Bugs can lead to a myriad of unwanted outcomes, as was the case when 300 million dollars worth of crypto-assets were lost forever due to a bug in the Parity wallet which allowed for unwanted functionality to be exploited [34]. A missing line in a smart contract led to a hack of 10 million euros [35]. The DAO hack enabled attackers to undertake a re-entrancy attack enabling them to steal 150 million dollars worth of cryptocurrency [36]. The inability to fix code deployed that is found to have software bugs have been one of the main challenges for both businesses and regulators. The inability of non-tech users to fully understand the smart contract code has been noted as another of the main challenges associated with smart contracts and their adoption [37].

Centralized exchanges (CEXs) are external entities to the main blockchain infrastructure, however they are also an important part of the blockchain ecosystem enabling millions of users around the world to transact with cryptocurrencies. Due their importance, they are also a vulnerability point that often gets exploited, costing users millions of euros. CEX can be regarded as a marketplace where users typically need to entrust the custody of their funds to the exchange before engaging in trading activities. Users usually need to create an accounts on the CEX platform and deposit their funds into wallets controlled by the exchange in order to make a transaction. An attack on the software of a CEX, can yield significant consequences for user's funds, leading to substantial losses. As seen in [22], wallet attacks on crypto exchanges and wallet service providers have been increasing over the last years. Besides theft of coins, cyber attacks on centralized exchanges can also cause abnormal economic losses for users and investors. Compared to CEX, Decentralized Exchanges (DEX) operate on a distinct mechanism, where users wanting to transact are matched in a peer-to-peer way, without a centralized

intermediary, and they retain control of their private keys and funds. DEXs also present their own set of security vulnerabilities [38].

Moreover, smart contracts face a constraint in their inability to access external data necessary for governing logic execution. Oracles serve the purpose of supplying this external data to smart contracts [39]. They can take the form of traditionally centralized entities or decentralized applications [40]. Oracles are entities crucial to the blockchain ecosystem, yet they also introduce a cybersecurity risks associated with data inaccuracies or fraudulent activities [41]. Some of the risks include the incorrect execution or non-execution of smart contracts, along with the manipulation of market prices.

1.3 Motivation

As we stand on the threshold of a new technological paradigm, the need to fortify this transformative technology against cyber threats has never been more pronounced. While ensuring absolute security in any computer-based system is an unattainable objective [42], standards, strategies, and regulations exist as a way to bolster security and mitigate cyber risks. Cybersecurity involves the protection of digital systems, networks, and data from unauthorized access, attacks, damage, or theft [43]. Cybersecurity is an inherently interdisciplinary domain as it encompasses a wide range of fields, disciplines and expertise. While technological advances focus on creating secure software, hardware, and network infrastructure to prevent and detect potential cyber threats, legal and policy frameworks define the boundaries and responsibilities related to cybersecurity. Laws and regulations dictate how organizations handle data, respond to security incidents, and protect individuals' privacy. Moreover, international standards guide global cybersecurity efforts, fostering collaboration and a united front against cyber threats.

Cybersecurity risks related to blockchain technology and its applications (e.g., cryptocurrencies) could be analyzed and potentially mitigated from two angles (one does not exclude the other):

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.

Enhancing the technical resilience of blockchain infrastructure, guaranteeing the reliability of smart contracts, engineering and implementing a robust incentive design to counter potential attacks are tasks mostly within the purview of

technical experts. Token-based systems, for instance, can deter certain 'dishonest' or malicious behavior through measures like token deductions or temporary restrictions, discouraging actions that could jeopardize the system. However, these efforts may not be entirely sufficient in shielding users from the adverse consequences of cyber attacks and associated vulnerabilities within blockchain systems and applications, such as crypto-assets [44].

Crypto-assets have emerged as the most prominent application of blockchain technology, yielding significant financial and innovative implications. Nevertheless, the European Securities and Markets Authority (ESMA) identified substantial risks linked to crypto-assets, including concerns about cyber-attacks, money laundering, and market manipulation. ESMA has emphasized that certain risks specific to technology are inadequately addressed, and existing requirements may not seamlessly apply or may lack relevance within a Distributed Ledger Technology (DLT) framework [45]. Acknowledging the existing gaps in pertinent legislation, the European Parliament, in its recommendations to the Commission on 'emerging risks in crypto-assets,' called on the Commission to propose legislative changes in the realm of Information and Communication Technology (ICT) and cybersecurity requirements for the European Union financial sector. This call aims to address inconsistencies, gaps, and loopholes [46].

Nevertheless, crypto-assets and the underlying DLT constitute intricate ecosystems, where furnishing pertinent insights requires an interdisciplinary examination that bridges the divide between legal, economic, and technical research. Cyber attacks on blockchain applications extend beyond their immediate impact, influencing financial markets and posing a potential threat to financial stability. Decentralized technologies also deviate from the conventional regulatory norms prevalent in centralized systems [47, 48], leaving users and businesses unprotected. In line with two of the main objectives (to protect users and foster innovation) of the EU Digital Package, we highlighting the necessity for a specialized approach in addressing a research gap that demands an interdisciplinary perspective. An interdisciplinary research is crucial not only for addressing the complexities of the blockchain but also for supporting policy and regulatory decisions related to crypto-assets, decentralized technologies, and associated cyber risks. A thorough comprehension of the security intricacies inherent in blockchain systems and their applications is indispensable for the formulation and implementation of effective regulatory measures.

1.4 Interdisciplinary perspectives on DLT Security

Blockchain systems are interdisciplinary in nature, not just by the diversity of their applications but also by the way the blockchain operates. Besides tokenomics

as described above, governance also represents a critical interdisciplinary facet within blockchain systems, especially when related to cybersecurity. Within the blockchain network, **on-chain governance** encompasses the structural framework for incentivizing participation, decision-making processes, allocation of voting rights, etc [8]. This mechanism operates directly within the blockchain protocol, enabling stakeholders to collectively influence system upgrades, modifications, or policy changes. The decentralized nature of on-chain governance seeks to ensure a fair and inclusive decision-making process, aligning the interests of network participants and enhancing the system's security and resilience. In the context of cybersecurity, effective governance is paramount for several reasons. First, it directly influences security-related decisions and responses to potential threats or attacks. The ability to promptly and efficiently implement security upgrades is vital in mitigating vulnerabilities and safeguarding the network against evolving cyber threats. Additionally, the governance model impacts the economic and financial stability of the blockchain ecosystem. Decisions regarding monetary policies, inflation rates (e.g., a cap on minting coins can have a deflationary effect on their economic value), and protocol changes can influence the value of cryptocurrencies and the economic incentives for network participants. A hard forks which happen when the blockchain splits into two separate branches following a change in the rules of the system, are often seen as governance divisions that can threaten the stability of a cryptocurrency, impact its economic returns and reduce the presumed level of security in the blockchain [22].

On the other side, **off-chain governance** represents a different dimension that encompasses elements such as regulations, policies, external management practices, third-party services, etc [8]. Unlike on-chain governance, which directly interacts with the blockchain protocol, off-chain governance involves mechanisms and external influences to the blockchain system. Despite this external positioning, off-chain governance can affect the on-chain behavior and outcomes within the blockchain ecosystem [23]. Regulatory frameworks as part of the off-chain governance, for instance, play a substantial role in shaping how blockchain technologies are utilized, adopted, as well as how cryptocurrencies are traded, taxed, or legally recognized. Government policies regarding data privacy, security standards, and compliance requirements can influence the overall behavior and operations of blockchain networks, impacting the way transactions are conducted and data is managed on the blockchain. Likewise, third-party services, including cryptocurrency exchanges and wallets service providers, play a vital role in facilitating and securing blockchain transactions. Their security measures and operational practices can directly impact users, affecting both the adoption and security of the system. As noted in [49], third-party service providers can play a pivotal role in bridging the gap between intricate technological advancements and the end-users, making blockchain technology and smart contracts more accessible

and user-friendly. However they can also become important vulnerability points which could require adequate security standards and regulatory measures [44].

Furthermore, when considering the interdisciplinary nature of blockchain based applications - cryptocurrencies exhibit a particularly strong connection to the realm of finance. Financial factors, such as the potential for significant gains in cryptocurrency value, can influence the propensity for cyber attacks, as highlighted in [22]. Overall, the potential for significant gains in cryptocurrency value can be seen as a double-edged sword. On one hand, it attracts investors and traders seeking substantial profits. On the other, it can entice cyber criminals to devise sophisticated cyber attacks, including phishing, ransomware, and hacking attempts, to exploit vulnerabilities and steal valuable assets. Therefore, designing effective cyber security measures can be seen as prerogative to the widespread adoption of blockchains and crypto assets.

1.5 DLT Opportunities beyond Vulnerabilities

Mitigating cyber vulnerabilities in blockchain systems is not merely a defensive strategy but a catalyst for unlocking a myriad of new use cases and fostering innovation. As blockchain technology becomes more resilient against cyber threats, it will instill confidence in its broader application across diverse industries. In an era defined by rapid digitization and an expanding digital frontier, blockchain technology has emerged as a revolutionary force with transformative potential across domains. Attributes of decentralization, disintermediation and transparency have propelled the utilization of blockchain technology into diverse sectors, including finance, energy markets, supply chain, gaming, and beyond.

Blockchains address crucial missing elements in renewable energy markets, where traditional centralized systems have faced challenges in transparency, efficiency, and resistance to fraud [50, 51, 52]. Blockchains can enhance coordination, privacy, and alignment of incentives within renewable energy use cases establishing a trustworthy reputation in the eyes of relevant external stakeholders. In particular, tokens build on top of a blockchain can be used as incentives to guide participants in performing socially desirable (e.g., green) actions, thus avoiding free-riding and other relevant problems in Commons based communities [53]. Likewise, blockchains seem to align with the socio-economic fabric of Renewable Energy Communities (RECs), enabling stakeholders to replicate their governance processes on-chain [54, 55].

The rapid growth and adoption of another groundbreaking technology - Artificial Intelligence (AI), has introduced various challenges, amongst which the ones in data compliance and cybersecurity [56, 57, 58]. In accordance with regulatory standards, the need to address how data is managed and secured has been

at the forefront of AI systems research needs [59]. Arguably, the incorporation of blockchain technology can enable specific AI-based systems to align with regulatory provisions in particular to aspects such as data, data governance, record-keeping, transparency assurance, and access control enforcement.

1.6 Contributions

On one hand, blockchain technology promises to revolutionize traditional systems, decentralize control, and provide a secure foundation for various applications. On the other hand, lurking in the shadows, are the multifaceted vulnerabilities and threats that could undermine its very essence, causing a domino effect across use cases. This thesis stands at the intersection of these contrasting forces, aiming to navigate this digital frontier and unravel the complex tapestry of the blockchain eco-system.

Conducting a comprehensive examination of the intricate relationship between blockchain and cybersecurity, this thesis aims to identify cyber vulnerabilities in real-world applications, assess their implications, and propose measures to strengthen the security infrastructure of blockchain ecosystems and their applications. Mitigating these vulnerabilities requires an interdisciplinary and multifaceted strategy, encompassing efforts to a) analyze the economic impact of cyber attacks on users and markets in real world blockchain applications b) enhance the technical resilience of the blockchain eco-system and c) implement regulatory measures that alleviate risks and reduce the impact of attacks on affected parties.

With this research work we aim to pave the way for a more secure digital future, where technological innovation harmoniously coexists with legal and economic imperatives. With the intent of promoting the creation of more robust, secure and widely adopted blockchain systems, this thesis will provide the following contributions:

- We offer a comprehensive taxonomy of cyber attacks and security vulnerabilities inherent to public blockchain technology, offering a structured understanding of potential threats.
- Using data from open blockchain APIs, we delve into the economic effects of cyber attacks on both users and investors, shedding light on the financial implications and risks associated with public blockchain-based systems and cryptocurrencies.
- We highlight specific facets of public blockchain technology that might require regulatory intervention for long-term sustainability and secure operation.

- We delve into the technical aspects of public blockchains which constrain regulatory intervention. Understanding its limitations we propose alternative approaches that have the potential to mitigate certain cyber risks.

- We consider certain challenges of smart contracts, which are both software artifacts and legal agreements, placing particular emphasis on the concept of an 'information gap' and its potential implications.

- We consider DLT as a normative tool that can be used to arbitrate and disintermediate interactions in complex societal contexts, such as AI applications, energy markets, and commons based communities.

1.7 Thesis Organization

This thesis is divided in two parts. The first (Chapters 2, 3, 4, 5) focuses on different cyber vulnerabilities, challenges and attack vectors in blockchain based systems, analysing their economic and regulatory implications. The latter part (Chapters 6 and 7), showcase how a blockchain, leveraging its technological capabilities, can be utilized as a security enhancement, coordination and incentive alignment tool across different systems. The subject matter of individual chapters can be summarized in the following way:

- *Chapter 2: Understanding Cryptocurrency Returns under Cyber Attacks.* In this chapter we examine cryptocurrencies, arguably the most well known blockchain application. We argue that although cryptocurrencies bring a number of advantages, the blockchain infrastructure on which they are built is susceptible to several types of security vulnerabilities and cyber-attacks, affecting negatively users and businesses. Besides the technical challenges, cryptocurrencies constitute a fairly recent and contentious asset category. Their distinction from traditional fiat currencies lies in the absence of national central bank management. Furthermore, they deviate from conventional stock properties, presenting a challenge in assessing risk exposure for investors and policy experts. Due to their intricate nature, merely confining risk analysis within an economic framework proves inadequate in fully understanding the potential disruptions they might undergo. Hence in this chapter we present a taxonomy of some of the possible attacks in a blockchain system and estimate the impact that different attacks may have on the economic returns of cryptocurrencies. Overall, we aim to develop a deeper understanding of these systems that are objects of great research interest in separate disciplines, supporting policymakers in their regulatory

decisions concerning cryptocurrencies and associated cyber-related financial risks. This chapter is published as part of the joint work at the Journal *Blockchain: Research and Applications* cited as [22]. Relevant research was carried at Nokia Bell Labs Paris and LINCS (Laboratory for Information, Networking and Communication Sciences) under the MSCA ITN "BAnDIT" project funded by the EU Commission.

- *Chapter 3: Navigating the Gap: Cybersecurity Challenges in Blockchain and Crypto Regulation*. This chapter is a logical continuation of the Chapter 2. Cyber-attacks targeting cryptocurrencies (and the underlying blockchain technology) have been on the rise, costing users and businesses millions of euros. As a mean 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. 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. We present a regulatory overview of the emerging fields of cyber risk, blockchain and cryptocurrencies in the EU and illustrate a techno-regulatory gap which requires further attention. We highlight specific facets of blockchain technology that might require regulatory intervention for long-term sustainability and secure operations. We delve into the technical boundaries of blockchain which constrain regulatory intervention in certain cases. Understanding its limitations, and propose alternative approaches that have the potential to mitigate certain cyber security risks. This chapter is based on an article published at *10th Graduate Conference in Law and Technology at Sciences Po Paris* cited as [44]. The chapter includes slight adjustments compared to the published article to accommodate changes in regulatory and industry developments. Relevant research was carried forward at Nokia Bell Labs Paris and LINCS (Laboratory for Information, Networking and Communication Sciences) under the MSCA ITN "BAnDIT" project funded by the EU Commission.

- *Chapter 4: MEV Dynamics: Cybersecurity Challenges and Policy Perspectives.* In this chapter we dive deeper into the blockchain architecture, particularly focusing at the incentive design behind block formation in PoW and PoS blockchains. We investigate the phenomena behind MEV (maximun extractable value) which is a common centralizing force in blockchains, causing security challenges in several well known blockchains. We discuss the economic and cyber security issues related by MEV such as front-

running practices and sandwich attacks, which are considered illegal in traditional financial markets. This chapter continues by proposing possible regulatory and technical measures as policy suggestions with an aim of mitigating the negative effects of MEV and protecting users and investors. This chapter is based on an article published at the *35th International Conference on Advanced Information Systems Engineering, under the Advanced Information Systems Engineering Workshop* [23]. Relevant research was carried forward at University Pompeu Fabra under the MSCA ITN "BAnDIT" project funded by the EU Commission.

- *Chapter 5: Closing the Information Gap*. Smart contract is a self-executing program that automates certain actions in agreement on a blockchain. Smart contract adoption has increased over the last decade, also increasing some of the challenges and risks users face when interacting with it. In this chapter we dive into specific challenges related to smart-contracts. Guided by notions from contract law and consumer protection we highlight the 'information gap' that exists between users (including judges/legal bodies) and the source code in smart contracts. We present a spectrum of low-code to no-code initiatives that aim at bridging this gap, promising the potential of higher regulatory acceptance. We argue that this highlights the phenomena of 'The Pitfall of the Trustless Dream', as arguably solutions to the information gap tend to make the system more centralized and vulnerable to a single point of failure. In this article, we aim to make a practical contribution of relevance to the wide-spread adoption of smart contracts and their legal acceptance. This chapter is based on an article published at *IEEE 24th Conference on Business Informatics (CBI), under the International Workshop towards Decentralized Governance Design* [49]. Relevant research was carried forward at University Pompeu Fabra under the MSCA ITN "BAnDIT" project funded by the EU Commission.

- *Chapter 6: Blockchain for AI: EU AI Act Compliance from a Cybersecurity Viewpoint* This chapter aims to investigate the potential of blockchain technology in mitigating certain cyber risks associated with artificial intelligence (AI) systems. Aligned with ongoing regulatory deliberations within the EU, and the escalating demand for more resilient cybersecurity measures within the realm of AI, our analysis focuses on specific mandates outlined in the proposed AI Act. We argue that by leveraging blockchain technology, AI systems can align with some of the requirements mandated in the AI Act, specifically in terms of data, data governance, record-keeping, transparency and access control. The study shows how blockchain can successfully address certain attack vectors related to AI systems, such as data

poisoning in trained AI models and data sets. Likewise, the chapter explores how specific parameters can be incorporated to restrict access to critical AI systems, with private keys enforcing these conditions through tamper-proof infrastructure. Additionally, the article analyses how blockchain can facilitate independent audits and verification of AI system behaviour. This chapter is published at the *International Cybersecurity Law Review Journal* [59]. Relevant research was carried forward at University Pompeu Fabra under the Protocol Labs Fellowship.

- *Chapter 7: Blockchain for RECs: Enhancing Privacy and Incentives in Energy Trading.* In this chapter we present blockchain as a tool that can enhance coordination, privacy, and incentive alignment within Renewable Energy Communities (RECs), while empowering them to establish a trustworthy reputation in the eyes of relevant external stakeholders. We develop a privacy-preserving energy trading protocol which enables secure communication of energy supply and demand. We show how, with a help of tokenized incentives, users are encouraged to publish usage profiles and trade energy in a community-based public forum. This allows all users in the community to benefit from typically cheaper locally-produced renewable energy, while also allowing the community as a whole to more effectively balance energy supply and demand, without compromising sensitive data confidentiality. With this solution we aim to show how blockchain-based protocols can contribute to the further adoption of sustainable energy, and act as a privacy preserving security enhanced tool. This chapter is based on a published article at the *8th International Conference on Renewable Energy and Conservation* [49]. Relevant research was carried forward at University Pompeu Fabra under the Protocol Labs Fellowship with the assistance of the Interplanetary Wellbeing Center.

1.8 Limitations

This thesis acknowledges the extensive diversity of vulnerabilities and cyber-attacks prevalent in blockchain systems and their applications. Nevertheless, given the expansive and ever-evolving nature of these challenges, our objective is not to offer an exaustive inventory of all potential threats within the confines of this research, as such an endeavor would require volumes of literature. Instead, we focus on a specific set of vulnerabilities and challenges present in blockchain systems. As a computer science thesis, this work does not aim to establish novel legal foundations or offer a comprehensive analysis of current laws and regulations. Instead, its primary focus lies in addressing questions situated at the cross-road of

technology and policy within the blockchain landscape. By specifically exploring questions that navigate the complexities between technological advancements and policy considerations, we aim to contribute insights that can facilitate a nuanced understanding of the subject matter in both disciplines, and support policymakers in regulatory decisions concerning blockchains, crypto-assets and associated cyber risks and application opportunities.

Chapter 2

UNDERSTANDING CRYPTOCURRENCY RETURNS UNDER CYBER ATTACKS

This chapter is based on the article: Ramos, S., Pianese, F., Leach, T., & Oliveras, E. (2021). "A great disturbance in the crypto: Understanding cryptocurrency returns under attacks." *Journal of Blockchain: Research and Applications*.

2.1 Introduction

A public blockchain is a peer to peer distributed ledger technology (DLT) that records transactions between two or more parties in a verifiable and permanent way by storing them as a sequence of blocks. The blocks are linked together into a chain, which (in the most popular blockchains based on proof-of-work techniques) is secured using cryptographic primitives and a randomized lottery mechanism. Each block contains a secure digest (or hash) of the previous block, an unforgeable proof from the lottery, a timestamp, and a list of transactions. One of the main advances that blockchain technology brings is the idea that, once recorded, a transaction stored in a block cannot be altered without modifying the entire sequence of subsequent blocks [10]. Blockchain technology originated with the development of Bitcoin, a cryptocurrency developed in 2009 by Satoshi Nakamoto, a pseudonym of its creator [7]. The definition of cryptocurrencies varies amongst jurisdictions. At a EU level, *"digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology"*[17] are referred as crypto-assets. While the EU differentiates between different crypto-asset categories, in this thesis we use the terms crypto-assets and cryptocurrencies interchangeably, making category distinctions only when rele-

vant to the discussion. Soon after the emergence of Bitcoin, the so-called crypto market saw a rapid take-off with the introduction of a vast number of new cryptocurrencies. There are more than 2,000 crypto-assets outstanding[45].

Despite of their operational transparency, decentralization, and ease of support for further applications, cryptocurrencies are still characterized as a highly risky asset class [60]. On these grounds, many countries worldwide issued warning notices for their citizens, advising them of the potential dangers of investing in cryptocurrencies [45]. In particular, the European Securities and Markets Authority (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). We go into more details over this issue in Chapter 3.

It can be argued that, although cryptocurrencies bring a number of advantages [61], the blockchain infrastructure on which they are built is susceptible to several types of security vulnerabilities and cyber-attacks [20], [62], which ultimately affect the overall risk level associated with crypto assets. Apart from the technical issues, they make up a relatively new and controversial asset class: they differ from fiat currencies in that they are not managed by a national central bank, but they also lack fundamental properties typical of stocks, making the analysis of their risk exposure difficult for investors, researchers, and policy makers. Because of their complex nature, constraining an analysis of the risks associated with cryptocurrencies within a purely economic framework is not sufficient to capture the possible disruptions to which they are susceptible [63].

In this chapter we adopt a multidisciplinary perspective by exploring the properties of cryptocurrencies at the intersection of computer science and economics. In particular, our objective is to analyze the various technical vulnerabilities (cyber-attacks & coordinated user-miner behavior) that apply to cryptocurrencies and to understand the economic (financial) impacts caused by them. After surveying the most common types of attacks for PoW cryptocurrencies, we focus in more detail on instances of 51% attacks, hard forks, and wallet attacks. Utilizing the intrinsic features of blockchain technology, we adapt existing event study methodologies to specific crypto-related event scenarios so that we can understand the impact caused by them in terms of generated abnormal returns/losses. Our metric of choice is the **Cumulative Abnormal Return (CAR)**, which we define in Section 2.4.1.

2.2 Cyber-attacks in cryptocurrencies

In this section, we introduce some technical background on how cryptocurrencies operate as a distributed systems on a computer network and characterize the

blockchain replica agreement mechanisms, also known as 'consensus'. We focus our analysis on blockchains based on Proof-of-Work (PoW), presently the most common implementation of major cryptocurrencies [64]. We then concisely explore the main security threats by presenting a taxonomy of the types of attacks associated with blockchain and cryptocurrencies, drawing from existing literature [62][65][66][67][20][68][69]. We give an explanation of the types of attack, their likely surface and scope, as well as hints that make them detectable and the benefits that the perpetrator may draw from them. We will later study in more detail three types of attacks from collected traces: 51% or majority attacks, hard forks, and wallet attacks. Our purpose is to estimate the impact on the attacked cryptocurrencies in terms of generated cumulative abnormal returns/losses.

2.2.1 Consensus and Security

The proof of work (PoW) consensus mechanism is the most widely deployed consensus mechanism in existing public blockchains [21]. This consensus mechanism became popular with the development of Bitcoin, although Nakamoto acknowledges its derivation from the HashCash scheme introduced in 1997 by Adam Back [7]. PoW belongs to the probabilistic-finality consensus mechanism category as it guarantees eventual consistency in nominal conditions [13]. In other words, PoW works as a lottery mechanism where a node that solves a computationally-intensive random search operation is allowed to create a new block. The node that first solves a cryptographic puzzle set by the rules of the network is the one that gets to create the next block [12]. This process is known as mining. In general, the higher the computational power available to a miner, the greater the likelihood of finding a valid solution before a less-endowed competing miner. Understanding how a PoW lottery works is important because it determines the main security properties of a blockchain [64].

2.2.2 Taxonomy of attacks

In Table 2.1 we present a taxonomy of the most relevant cyber-attacks targeting cryptocurrencies, along with their impact, indicators, and affected system participants. We add another classification (specific, non-specific), with **specific** being an attack that solely targets one cryptocurrency at a time, and **non-specific** an attack that at the same time affects multiple cryptocurrencies. We indicate as **theoretical** a type of attack that has only been discussed as possible with no evidence of its actual occurrence. Smart contract vulnerabilities and attacks are beyond the scope of this chapter, hence they are not included in the table below.

Table 2.1: Taxonomy of attacks on cryptocurrencies

Attacks	Description	Purpose	Type	Possible Indicator
51% attack	Attack on a blockchain by a group of miners who control more than 50 percent of the network's mining hash rate.	Double spending; Getting block reward	Specific; Attack; Data Available	Selfish-mining; Stale Orphaned Blocks; Consensus and Block Delay
Goldfinger attack	Specific type of a majority attack; attackerâs motivation is based on some incentive outside the cryptocurrency economy	Overthrowing the system as a whole	Specific; Data unavailable; Theoretical	Dominance over total network hash rate, can be noted by demand for rental (Nice Hash); buying mining equipment etc.
Hard Fork	Blockchain splits into two separate branches following a change in the rules of the system	Creating new protocol rules leading to new currency	Specific; Data Available	Attack or controversial situation (community conflict) may lead to forking of a cryptocurrency
Sybil Attack	Single entity tries to take over the network by creating multiple accounts or running multiple nodes	Allowing attackers to infiltrated the routing of messages on the blokchain overlay	Specific; Data unavailable	None
DNS Hijack	Attack in which DNS queries are incorrectly resolved in order to unexpectedly redirect users to malicious sites	Theft of coins	Non-Specific; Data Unavailable	None
BGP Hijack	Illegitimate takeover of groups of IP addresses by corrupting internet routing tables maintained using the Border Gateway Protocol (BGP).	Double Spend	Indirect; Data Not available	Delay in block propagation
Eclipse Attack	In an eclipse attack, the malicious actor will ensure that all of the targetâs connections are made to attacker-controlled nodes. Leverages a sybil attack on the blockchain overlay.	Disrupt information flow to create advantages for mounting 51% attacks	Indirect; Data Unavailable	Crawling Bitcoin overlay
Wallet Attack	Big leak of Wallet IDs, wallet attack can happen through different ways among which A possible breach of the wallet provider core protocol; DNS hijacking,phishing attacks,remote code injection, etc.	Theft of Coins	Can be both Specific and Non-Specific; Data Available	Inability to access wallet
DDoS	Distributed denial-of-service, when an attacker makes a machine or network resource unavailable to its intended users by disrupting services of the host connected to the Internet	Degrades the performance of a cryptocurrency exchange, Decreasing Volume traded could crash the exchange platform	Non-Specific; Data unavailable	Inability to access a trading platform
Dusting Attack	"Dusting" a large number of addresses by sending a few âcoinsâ to them. The next step is to of involves	Type of deanonymizing attack Theft of coins, Ransomware	Non-Specific; No Data Available	Insignificant coin amount sent from unknown user 'dust'

2.2.3 Majority Attack

A basic rule of PoW blockchains is that the most up-to-date state of the system is represented by the longest chain, and all rational miners should attempt to generate new blocks that extend it further to gain the next block reward. A majority attack can be mounted by someone covertly possessing a large enough share of hash rate that allows the attacker to produce blocks at a much faster pace than the rest of the network. In these circumstances, the attacker could covertly create a private chain which diverges from the 'official' one and which, once disclosed, will become the legitimate state of the system, rewriting its entire history from the branching point. This is known as a majority or 51% attack, whereby the attacker can exploit the inconsistency between the two chains to mount a "double spend" attack.

Double spending is what happens when the same digital currency can be spent more than once, i.e., a transaction uses the same input as another that had already been broadcast on the previous chain [70]. This type of attack can be highly profitable [68], depending on the holdings of the attacker, the liquidity of exchanges/merchants processing the fraudulent transactions, and the cost associated with procuring the computational capacity required to mount the attack. So far, there have been various recorded cases of 51% attacks on smaller cryptocurrencies, which we analyze in more detail in Section 2.5.

In practice, mounting a majority attack is not an easy task but it is still possible especially through so-called 'mining pools'. Joining a mining pool is common among miners as a way to make rewards from the mining process more predictable [71]: due to the high absolute difficulty of winning a PoW lottery, mining a block without having an extremely costly and potent mining equipment is very hard to achieve by solo miners. As [72] explains, a miner running a 3 TH/s (terahash per second) node which is priced at 4000 euros, was expected (in 2014) to find a block every six months on average. Hence, in order to reduce the risk of not finding a block and receiving a reward, pools allow small miners to contribute to the network's hash rate and together mine a block reward which will be later split among the mining pool participants. [73] argue that colluding miners' revenue is larger than their individual fair share. Likewise, the 'difficulty level' of finding a block has been gradually increasing as it is shown in Figure 2.2. Pools can unfortunately become a threat: [73] argue that honest but rational miners will have the incentive to eventually join the attackers, and the colluding group will increase in size until it becomes a majority. Today there are more than 15 known mining pools present on the Bitcoin network (see Figure 2.1) and in several occasions the biggest ones have become close to owning a majority stake of the mining power.

Regarding the cost of mounting an attack, [74] calculated the viability of attacking various currencies by estimating the price of renting enough mining power to match the overall network hash rate for an hour. For example, they observed

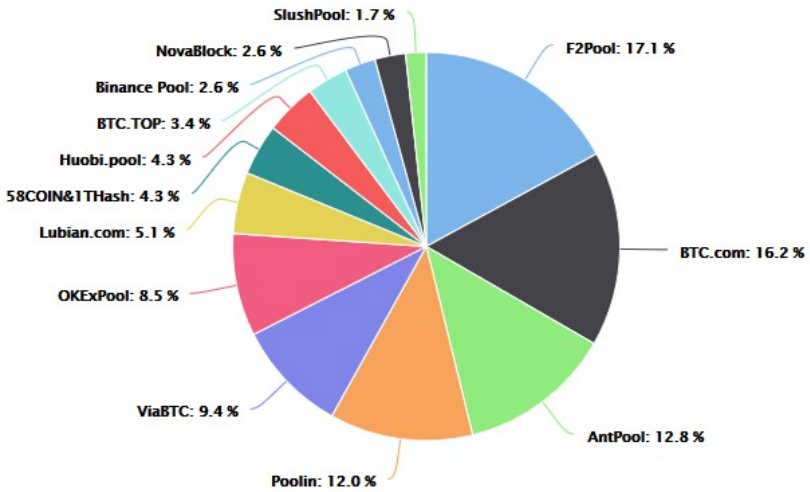


Figure 2.1: Share of mining capacity held by major mining pools. Source: conseils.crypto 2020

that attacking Bitcoin at the time would cost around 696,885 dollars for one hour, while for some minor coins such as LiteCoinCash the price of a double spend attack would be as low as 24 dollars per hour. Although these calculations may not be the most comprehensive and accurate due to other technical factors and to the challenge of covertly renting significant amounts of computing power [75], it can be noted that large miner populations make blockchains fairly resilient against majority attack. In other words, well-established cryptocurrencies tend to be impervious to this type of attack. This fact is important when considering that blockchains can become fragmented due to community splits - a *Hard Fork* may negatively affect the ledger's security against majority attacks.

2.2.4 Hard Fork

Forking is said to happen when a blockchain splits into two separate branches following a change in the rules of the system. Forks can happen for multiple reasons, usually because of disagreements among the user and developer communities (ex. increasing the block size in the case of Bitcoin Cash [76]) and sometimes as a response to a major hack (ex. the case of the DAO [1]) [77]. Depending on the nature of the rule change, forks can be categorized into Hard and Soft Forks. A *Soft*

[1]The "decentralized autonomous organization" (DAO) is a set of smart contracts on the Ethereum blockchain. The 2016 DAO hack resulted in huge losses, and a majority of the community subsequently voted to roll-back the ledger state. This vote resulted in a hard fork of the Ethereum blockchain from which Ethereum Classic originated.

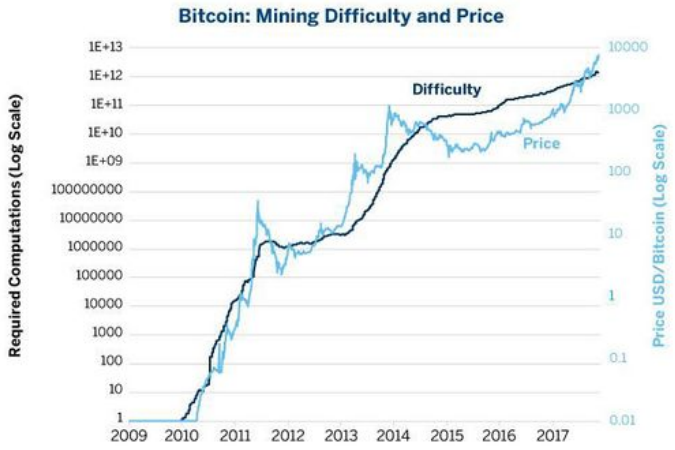


Figure 2.2: Bitcoin difficulty target over time. source:bitcoinwiki.org

Fork is a revision of the rules that is accepted by most stakeholders and usually backward compatible [78]. In other words, blocks that will be generated following the new rules are still valid according to the previous rules, hence nodes that did not adopt the changes may still operate normally. A *Hard Fork* is a change that is not backward compatible and that is the object of disagreement among stakeholders. In this case, when nodes generate a block following the new rules, it will be rejected by the nodes that did not approve of the change [78]. A Hard Fork basically creates a new coin, as in the case of Bitcoin Cash and Bitcoin Gold which are both derivatives of Bitcoin [76]. After a Hard Fork happens, unspent transactions outputs from the original blockchain are considered valid both in the old and the new currency: therefore users possessing 5 coins of currency X will also possess 5 coins of new currency Y.

Although the Hard Fork doesn't necessarily fall in the category of malicious attacks, such as the 51% attack, it can still be considered an attack because it causes a significant disturbance of the system's operation by its own community, creating a new 'competing' cryptocurrency and diminishing the size and security of both resulting systems [79], often casting doubts about the viability of the smallest one. But opposing interests and visions for the future of a cryptocurrency may lead communities to a point where substantial groups of stakeholders have no choice but go their separate ways [76].

Given the public nature of the conflicts leading to these events, hefty traders (e.g., investors holding large amount of coins) can make essential changes on the market in anticipation of a hard fork split. When a large trading entity anticipates that a hard fork is about to occur, it has a strong incentive to increase its stake in the parent token until the fork happens and later release tokens due to

the knowledge of artificially inflated prices. A focused analysis of crypto-market manipulation strategies is outside the scope of this chapter, although several past studies detected examples of manipulative responses [80, 81].

There are also several other issues related to hard forks in terms of their motivations. Many forks seem to be similar and not offer any new desirable feature. More than fifty forks of Bitcoin exist, but few currently show any trading volume at all. In some cases, announced forks were downright scams meant to manipulate the market or fool less knowledgeable investors, with no actual fork being carried out. Some scams were meant to drive Bitcoin price down (ex. Bitcoin Platinum) while others attempted to steal users' credentials and cryptoassets through a fake wallet website [82, 83]. The latter scam leads us to the next category of attacks, that may sharply affect the price of cryptocurrencies when carried out at a large enough scale: wallet attacks.

2.2.5 Wallet Attack

In order to transact with a cryptocurrency, users need to control a cryptocurrency wallet. A wallet can be 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. An attack on a wallet software or wallet service provider and its users can produce a big impact, resulting in a massive theft of coins and decreasing the trust in the system overall. Besides traditional wallet service providers (*e.g.*, Trinity, MyEther, Edge) cryptocurrrency holdings can be stored on other online platforms such as exchanges (*e.g.*, Coinbase, Bitfinex, Bithumb, Bittrex). Coinbase is a digital exchange and online cryptocurrency wallet provider which, contrary to single-coin wallets, allows for holding and trading several cryptocurrencies under a same account. Wallet attacks do not usually involve the blockchain: classic privilege escalation and the compromise of the provider's "hot wallet" (cryptocurrency wallet that is connected to the internet) credentials are the main technical vector leading to the theft of massive amounts of holdings belonging to their users. The table below shows some of the biggest wallet attacks of cryptocurrencies. We included a sample of both single-coin and multi-coin wallet attacks to test for its effects.

Moreover, attacks targeting individual wallet users can be mounted via a multitude of malicious techniques with the purpose of stealing user credentials and gaining access to their funds [84]. Besides the case of insider attacks by dishonest providers, possible attack vectors include DNS hijacking, virus/trojan infection from phishing attacks, cross-site scripting, and organized social-engineering attack.

2.3 Related Work: Event Studies, Cyber-Attacks and Cryptocurrencies

Event study analysis is commonly used to determine abnormal returns in stock prices resulting from unanticipated events [85]. The main premise is that efficient markets should ”price-in” new event information to the stock value of the impacted entity. In other words, the impact of a certain event can be measured by examining security prices surrounding the event [86], [87].

Several event studies in the literature focused on the effect of security breaches (cyber-attacks) on companies' stock performance [88, 89, 90, 91, 92] uses an event-study analysis to assess the impact of cyber-attacks on the market value of breached firms. Still, there are conflicting views about the economic impact of such breaches. [93] maintains the lack of understanding of the different types of cyber-attacks, as well as its effects. Whereas results generally suggest that companies do experience financial losses, expressed as a negative stock market reactions, some authors argue that the monetary effect depends on the type of the attack [89] and the length of the event window [90]. Hung studies the association between information security news and corporate stock prices [94]. Colivicchi and Vignaroli investigate the possibility to to manage cyber-risk by forecasting the daily portfolio volatility in relation to the fact that the stock market seems to recognize the impacts of a related cyber-attack [95] .

To the best of our knowledge, although some studies did focus on the impact of other types of events on cryptocurrencies, very few event studies were performed on the effect of security breaches and cyber-attacks on cryptocurrencies. [96] utilizes event studies to determine the stock price reactions of blockchain-related listed companies after corporate name changes and finds significantly positive abnormal returns on the event date. Also, [97] studies the effect of US monetary policy announcements on cryptocurrencies, protocols, and dApps. Hashemi Joo et al. study the cryptocurrency value after 51% attacks and Abhishta et al. studies the impact of DDoS attacks on cryptocurrency exchanges by the changes in transaction volumes traded [98, 99]. On the other hand, Auer and Claessens explore the cryptocurrency market reactions to regulatory news [100]. Apostolaki et al. explores the potential impact of IP routing attacks on the functionality of the Bitcoin cryptocurrency and alludes to the potential exploitation of BGP hijacks for manipulating the price of Bitcoin [62]. Koutmos maintained the dominant role of Bitcoin in terms of return and volatility spillovers among the 18 largest cryptocurrencies [101]. Caporale et al. reinforces this argument alluding that cyber-attacks targeting cryptocurrencies have a significant impact on the dynamic linkages where Bitcoin plays a dominant role [102].

2.4 Contribution

As noted before, the event study literature is mostly focused on corporate stock performance analysis. There are few prior event studies applying to cryptocurrencies attacks. In the following, we will adapt existing event study methodologies to specific crypto-related event scenarios so that we can analyze and understand their impact.

We agree with [89] about the importance of dividing the attacks into different categories depending on their type to estimate the economic effect. For the 51% attack, we utilize data based on the intrinsic feature of blockchain technology that tracks the exact time and date at which an attack happened by spotting the sudden changes in the network's longest chain and determining whether a transaction was been double spent. This technical scenario introduces a different set of challenges compared to company-related event studies, where the exact timeline of the propagation of information about the event (*e.g.*, a merger) is not clearly known and the event window needs to incorporate a number of days prior to the known event date in order to account for a possible information spill.

Despite the full availability of cryptocurrency data as part of the normal operation of public blockchain systems, spotting a 51% attack on a cryptocurrency requires technical skills not available to the general public, which introduces a potential delay between the actual attack and the reporting of it. For example, the BTG attack in 2020 was discovered by a researcher at MIT's Digital Currency Initiative [103]. Sometimes, it is once the information is spread by the media, that the public and the markets become aware of it. Based on the finding in [104] that cryptocurrency prices react quickly to 'bad news' in the press, and the magnitudes of cumulative abnormal returns (CARs) are larger for negative events than for positive events, implying that the market reaction to negative events is stronger than to positive announcements [105], we attempt to go further than [98], which uses media-publicized announcement dates of 51% attacks in their study. We can better approximate the length of the event window by finding the exact time when a 51% attack took place and can sometimes tell apart the effects of the attack itself from the consequences of the attack's awareness. In our analysis, we assume that once an attack (event) has happened the information is potentially accessible and available and the attacked cryptocurrency price can show a reaction. This is also supported by [105] which notes high abnormal returns on days prior to the news disclosure.

In the sample of cryptocurrency attacks analyzed in this chapter, we observe that there are cases in which the news of an attack gets published quickly (on the same day or in the following week) and cases where an attack was not officially reported for a period of one month or longer. Accordingly, our analysis organizes attacks into two categories, those that have been publicly 'known' (information

Table 2.2: List of 51% Attack Events Considered

Cryptocurrency	Date Attack	Date Pub.	Type
Bitcoin Gold (1)	5/16/18-5/19/18	5/18/2018	Known
Bitcoin Gold (2)	1/23/20-1/24/20	1/25/2020	Known
Ethereum Classic	1/6/19â1/8/19	1/7/2019	Known
Vertcoin (1)	10/12/18â10/18/18	12/2/2018	Unreported
Vercoin (2)	10/27/18â10/28/18	12/2/2018	Unreported
Vercoin (3)	11/29/18â12/2/18	12/2/2018	Known
Verge (1)	4/4/18	4/4/2018	Known
Verge (2)	5/22/18	5/22/2018	Known

released in the media up to 10 days from the day of the attack) and those that were 'unreported' (if the delay of the information spread was longer than 10 days from the day of the attack).

Furthermore, the 'unreported' category gives us an opportunity to test whether a 51% attack was already known to some actors before it was openly reported. In these cases, the imperfect availability of public information may still affect the market price of the attacked currency and generate abnormal returns. Here, a possibility of potential inflating of prices (hence generating higher abnormal returns) during an attack is also not excluded, if attackers manage to stay unnoticed to the rest of the public.

Another particularity we observe in the data is that some attacks last few hours while some last for multiple days, as it can be seen in Table 2.2. Although some of the longer incidents can be classified as separate block reorganizations, *i.e.*, subsequent distinct attacks of short duration, we choose to aggregate them into a single attack with a longer duration for two main reasons: first, these strings of events are usually reported by the media as 'an attack', and second, from a technical perspective, a number of block reorganisations happening subsequently is most probably caused by a same attacker (or organized group of attackers) trying to abuse the network. For example, Bitcoin Gold was hit by two chain reorganizations of over 10 blocks of length on January 23th and 24th in 2020. Although the reorganisations were six hours apart, this situation was described as a single attack both by the media and by the crypto-community. In the following, when a majority attack lasts for longer than a day, we shall consider the first day as the starting point of our event window, *i.e.*, [0,0].

In the case of hard forks, we set out to understand the impact of protocol changes on the prices of forked currencies. In our analysis, we use a sample of five hard fork event traces, which we select to ensure the relevance and the absence of interference from multiple confounding factors. Hence, we omit fork events (ex. such as the Ethereum vs. Ethereum Classic fork) where the fork immediately followed a cyber-attack event which greatly distorted the price of the

Table 2.3: List of Hard Fork Events Considered

Cryptocurrency	Forked Currency	Date
Bitcoin	Bitcoin Cash	8/1/2017
Bitcoin	Bitcoin Gold	10/24/2017
Litecoin	Litecoin Cash	2/18/2018
Bitcoin Cash	Bitcoin SV	11/15/2018
Bitcoin Cash	Bitcoin Candy	1/13/2018

Table 2.4: List of Wallet Attacks Considered

Exchange	Loss (USD)	Cryptocurrency	Date
IOTA Trinity Wallet	1.6 mil	IOTA	2/12/2020
Bithumb	19 mil	XRP,EOS	3/29/2019
Bithumb 2	30 mil	BTC,ETH,XRP	6/16/2018
IOTA Wallet Theft	4 mil	IOTA	1/19/2018
Bitpoint	32 mil	BTC,XRP,ETH	7/10/2019

cryptocurrency, to avoid mixing up the consequences of the hack with the actual effect of the fork. Also, in the case of Bitcoin, a vast number of hard forks have occurred over the recent years, most of which show low to no trading volume and negligible miner adoption. Hence, we focus on Bitcoin Gold and Bitcoin Cash as the most successful and relevant forks of Bitcoin. We also include Bitcoin Candy (the first fork of Bitcoin Cash) and Bitcoin SV (the fourth leading cryptocurrency, also a fork of Bitcoin Cash). Moreover, we consider Litecoin Cash as a hard forks of Litecoin (another leading cryptocurrency). The full list of hard forks we consider is presented in Table 2.3. Finally, Table 2.4 enumerates a sample of five different wallet attacks to both exchanges and wallet providers.

2.4.1 Data and Methodology

We use the CoinGecko cryptocurrency API to obtain longitudinal data sets regarding the price of the cryptocurrencies that are being tested. For majority attack and hard fork we are able to know the exact date of the event, while for wallet attacks we rely only on the news release for estimating the event date. For all three types of attacks, we use a set of media articles from various sources that released information regarding the attack that help us understand when the attack first became publicized and how long the information was trending. To determine whether the event had an impact on a given cryptocurrency we apply two study models for asset pricing.

The Market Model (MM)

One of the most common models used in event study literature is the *market model* [106] [107]. We use the model to compute the abnormal returns, that is the actual ex-post return of the cryptocurrency minus the 'normal' return of the asset throughout the duration of the event. The normal return on day t, of a given cryptocurrency i, is defined as the return that would have been expected if the event had not taken place.

$$AR_{i,t} = R_{i,t} - \hat{R}_{i,t} \tag{2.1}$$

where daily returns on day t are calculated based on asset price P^i as follows:

$$R_{i,t} = \frac{P^i_{t+1} - P^i_t}{P^i_t} \tag{2.2}$$

This model assumes a stable linear relation between the market return $R_{m,t}$ and the security return. The market model is used to compute the expected returns utilising the regression:

$$\hat{R}_{i,t} = \alpha + \beta \cdot R_{i,m,t} + e, \tag{2.3}$$

In the market model, the expected return is computed over an *estimation window* ahead of the event considered. The parameter α is called intercept term, and the parameter β is the slope parameter, both are commonly used as regression coefficients. Studies show that the market model performs better than Capital Asset Pricing Model (CAPM) and Arbitrage Pricing Theory (APT), implying that the validity of the restrictions imposed by these models are questionable and the gains from using them over the market model in this context are low [108] [106].

As a proxy for the market return, in our analysis we use the Crescent Crypto Market Index (CCMIX) which is a rules-based cryptocurrency market index that is designed to measure the performance of the largest and most liquid cryptocurrencies. Upon examining the most popular crypto-market indexes (including CCMIX), we observe that most of them put a high weight on Bitcoin as the benchmark of market behavior. We therefore account for this fact when performing event analysis on Bitcoin data, as the results given by MM are expected by construction to exhibit a strong correlation to the index, while there is limited significance in capturing the abnormal behavior of smaller cryptocurrencies.

The Mean Adjusted Return Model (MAR)

We introduce a second model, the Mean Adjusted Return model (MAR), as an alternative and more robust metric for the computation of abnormal returns of cryp-

tocurrencies, also based on observations found in the literature on the shortcoming of using crypto market indexes to describe the behavior of all cryptocurrencies [98]. The MAR model avoids relying on a market index, which is a useful property in cases when the index is strongly correlated with few major cryptocurrencies. Although MAR is less sophisticated than MM, it has been observed to yield results that are often similar to the ones of more advanced techniques [109][110]. In the MAR model, the abnormal return in the event window is the return of cryptocurrency i on day t, minus its average return in the estimation window W:

$$AR_{i,t} = R_{i,t} - R_W \tag{2.4}$$

Where

$$R_W = \frac{1}{T_1 - T_0} \sum_{t=T_0}^{T_1} R_t. \tag{2.5}$$

Quantifying the Cumulative Abnormal Returns (CAR)

It is common practice for event studies about the stock market based to consider a range of around 115-120 days prior to the event as their estimation window [85]. Whereas the literature is rich in examples based on stock market data, the conventions of stock markets cannot be directly applied to crypto-market event studies. Based on the prior work of [99] on cyber attacks and cryptocurrencies we adopt their standard of estimation windows reflecting the much higher volatility of cryptocurrencies.

To measure the total impact of an event over an ensuing period of time (or 'event window'), we define the Cumulative Abnormal Returns (CAR) metric that aggregates the abnormal returns observed during the event window.

$$CAR_{(t_1,t_2)} = \sum_{t=t_1}^{t_2} AR_{(i,t)} \tag{2.6}$$

We observe normality in the distributions of AR values and use two tailed t statistic to test at 95 percent level of confidence.

$$t_{stat}^{AR} = \frac{AR_{(i,t)}}{S_{AR}} \tag{2.7}$$

where S_AR is the standard deviation of the abnormal returns in the estimation window,

$$S_{AR}^2 = \frac{1}{M_i - 2} \sum_{t=T_0}^{T_1} (AR_{i,t}^2) \tag{2.8}$$

and t statistic of the cumulative abnormal returns for each cryptocurrency is defined as: Null Hypothesis $(H_0) : CAR_i = 0$

$$t_{stat}^{CAR} = \frac{CAR}{S_{CAR}} \tag{2.9}$$

The value of S_{CAR} is defined as:

$$S_{CAR}^2 = L \cdot S_{AR}^2 \tag{2.10}$$

where L is the length of the estimation window (calculated relative to the event day).

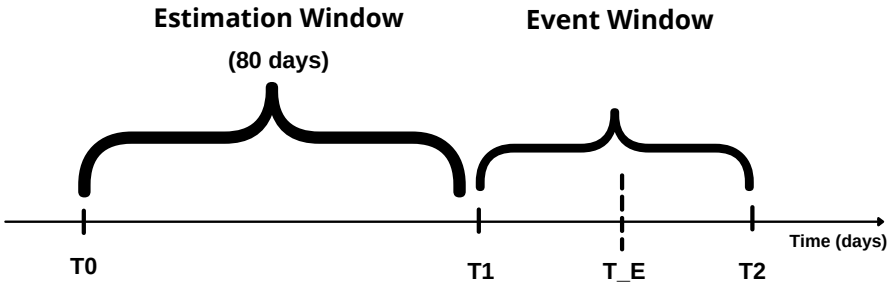
In Figure 2.3 we indicate the general structure of estimation windows and event windows in our study, illustrating our choice of parameters for the specific attack scenarios. In the case of 51% attack, we know with certainty the exact event date and time, hence we set the starting point of the event window at the exact time and date at which the start of the blockchain reorganization is detected. We note a usual trending of news up to ten days post attack: this is consistent with [105], which shows that the announcement effect on CARs in the cryptocurrency market can linger for around a week after an event and suggest that the information flow in the cryptocurrency market is visibly slow. Hence, in our study we test the effects of the majority attack reflected in the CAR metric for the full range of event windows sizes in a ten day event frame, *i.e.*, with event window lengths ranging from one day [0, 1] to ten days [0, 10]. In the case of hard forks, due to the assumption of market anticipations and pre-buying of original tokens with the aim of obtaining the novel token after the completion of the fork, we focus our analysis on the pre-event window period and we derive CAR for multiple event window lengths starting up to two weeks before the fork happens, until five days after the fork, *i.e.*, [-14, 5]. As for wallet attacks, where the exact date of the event is usually not available, we base our analysis on released public information. We assume that due to the high impact of this type of attack (in terms of USD losses) and scale (in terms of number of people affected) the information spread is faster. Accordingly, we test for multiple event windows in a shorter time span starting five days before the attack (accounting for information spill) up to five days after, *i.e.*, [-5, 5]. In our analysis, we consider the following Research Questions:

Q1: Is there a significant impact from 51% attack on the attacked cryptocurrency returns during the event period?

Q2: Is there a significant impact from 51% attack on the attacked cryptocurrency returns' during the event period if the attack has not been publicly known (assuming tech savvy people can still know about it)?

Q3: Is there a significant impact from Hard Forks to the forked currency returns during the event period?

Q4: Is there a significant impact from Wallet Attacks on the attacked cryptocurrencies' returns during the event period?



51% Attacks	Hard Fork	Wallet Attacks
$T_1 = T_E$	$T_1 = T_E - 14$	$T_1 = T_E - 5$
$T_2 = T_E + 10$	$T_2 = T_E + 5$	$T_2 = T_E + 5$

Figure 2.3: Estimation and Event Window for the attack scenarios considered in the study

2.5 Analysis and Results

This section presents the results from the application of the above techniques to the CoinGecko data. As a general consideration, we find that the Market Model (MM) does not fit well the dynamics of the prices for most minor cryptocurrency assets, which appear to show low linear correlation with the market index. On the other hand, Bitcoin and Litecoin are well explained by MM, with R^2 values respectively around 0.7 and 0.3. A strong correlation with the index implies that, in case of attack, both the asset price and the market index will be affected thus biasing our appraisal of what the normal return would have been. Consistent with [98], we find that the MAR model, albeit simpler, provides more robust results. In the following pages, we will discuss results for both MM and MAR models. The figures we provide to illustrate our results show the magnitude of the CAR in our event studies; we highlight the CAR values we deem significant (p-value < 0.05; 95% confidence) with bullets superposed onto the plot lines.

Q1 (Known 51% attacks - Figure 2.4) Generally speaking, 51% attacks have a predominantly negative effect on the cryptocurrencies we studied. However, not all of them had a persistent significant impact on the returns. Under the MM, the double spend attack that hit Bitcoin Gold in 2020 did result in negative cumulative abnormal returns of 7% on the day after the attack finished when the news started trending, although this effect appeared not to be persistent throughout the rest of the event window. MAR highlights a more prolonged impact on CAR over the 3 days following the event, showing an increase in the negative magnitude of the returns to up to -15%. On the other hand, the attack that impacted Bitcoin Gold two years prior (2018) appeared to produce a longer lasting significant negative impact

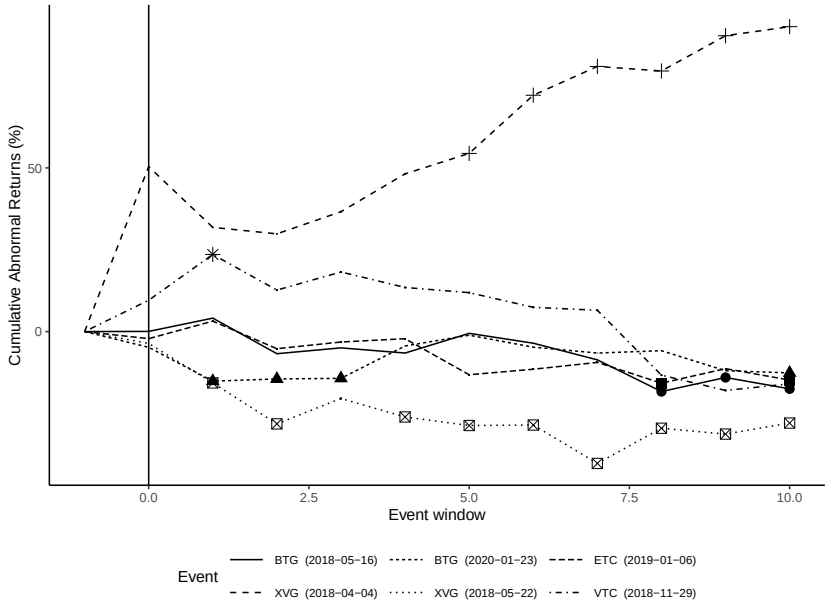


Figure 2.4: CAR of **known** 51% attacks (MAR model) with significant values ($p < 0.05$)

that remains visible over multiple days towards the end of the event window, with a magnitude in negative cumulative returns reaching up to -7% under MM. MAR confirms the impact of the attack towards the end of the event window, increasing the negative effect on the cumulative abnormal returns to -18%. The 51% attack that affected Ethereum Classic in 2019 did not exhibit any significant negative abnormal returns following the event under the MM. However MAR shows a significant negative impact on CAR up to -15% towards the end of the event window. Interestingly, under MM Verge's first attack on April 4th 2018 had *positive* and significant cumulative abnormal returns. Verge showed an initial negative effect on the abnormal returns; then shortly after the attack Verge launched a new marketing campaign, where an important industrial partnership was announced. The later part of the 10 day event window did likely reflect some of the positive effects that this news had. In this event, the marketing campaign that Verge mounted probably out-weighted the negative effect of the attack, distorting the common behavior of 51% attack. MAR confirms the positive impact on CAR in the second half of the event window. As it would be expected, the second attack on Verge did bring a significant negative effect on CAR in all event windows during the 10 day period tested, rendering a negative CAR of up to 12%. MAR confirms the negative impact on CAR over all event windows in the [0,10] period range, rendering an effect of up to -40%. The case of the Vertcoin "known attack" also

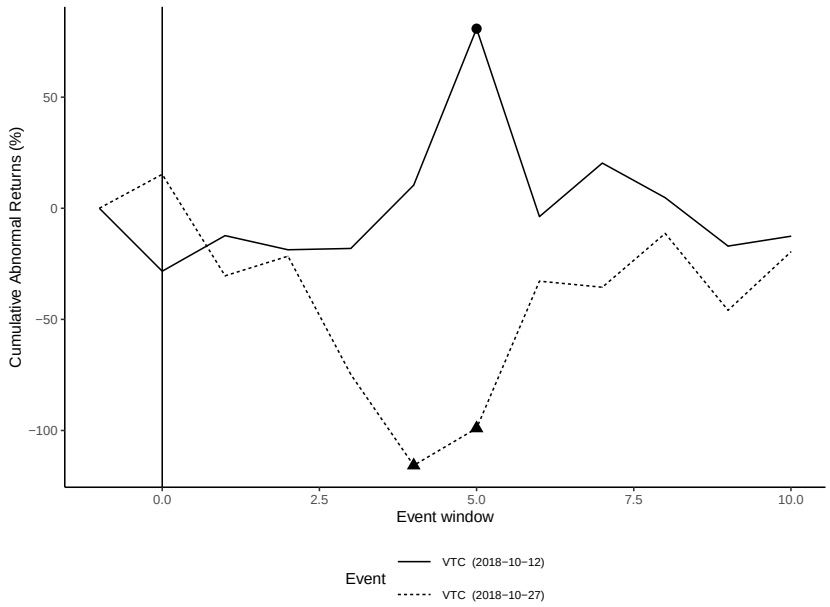


Figure 2.5: CAR of Unreported Attacks (MAR model) with significant values ($p < 0.05$)

shows a significant impact on CAR persisting throughout multiple event windows with a negative effect of up to 25% using MM. Under MAR positive significance is noted at the event window [0, 1].

Q2 (Unreported 51% attacks - Figure 2.5) In the case of the first unreported 51% attack, which occurred on the Vertcoin blockchain, there was a significant positive effect on the CAR on the overall 10 day event window under the market model. Under MAR these results are reduced as there is a shown significance in just one event window [0,5] in the ten day event period. In the second unreported 51% attack the results of MM and MAR differ greatly. While the market model shows a small positive impact on CAR over several event windows, the effect shown by MAR is negative. We also remark that, since 51% attacks differ in duration and number of reorganisations, adversarial profit-making strategies may vary where the attack is not known to the public. In cases where the attack was not reported publicly, the market cannot efficiently price-in the information of a majority attack. Moreover, performing a double spend while the price of the attacked cryptocurrency is so 'inflated' could ultimately lead to higher gains for malicious attackers, especially if the attack takes a long time to be discovered. As noted, misaligned trading crypto prices can be a result of 'pump and dump' by attackers or by those that hold private information about the attack [111]. However,

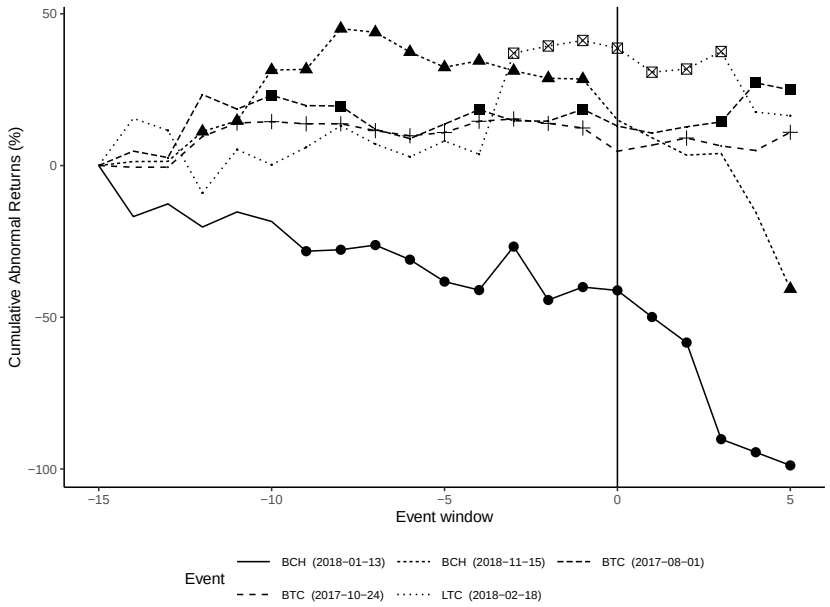


Figure 2.6: CAR of Hard Fork events (MAR model) with significant values ($p < 0.05$)

analysing 'pump and dump' episodes observed on the crypto market is out of our research scope.

Q3 (Hard Fork - Figure 2.6) We now analyze the anomalous return traces for the reported cases of Hard Fork events in Table 2.3. In the case of the first fork on Bitcoin Cash we note a negative impact on the CAR (up to 60%) under the MM that starts building significantly a week prior to the fork event and continues to show negative abnormal returns in the days following. MAR extends the significance over more event windows in the pre-forking period and increases the negative impact to 98%. In the second fork on Bitcoin Cash we also observe a significant negative effect on cumulative abnormal returns of up to -19% under MM in the post-fork period. Under MAR we observe similar situation, where there is an initial significant positive impact in the pre-forking (pre-event) period that reflects in a sharp fall after the event, resulting in negative impact under MAR of up to -40%. The only difference in sign of impact that we observe under the two models in forks is in the instance of Litecoin. Under MM we observe a significant negative impact on Litecoin of around 13%, while a positive one under MAR of up to 40%. Both forks on Bitcoin show a significant positive impact of up to 11% for the fork with Bitcoin Cash for and 2.7% for the one of Bitcoin Gold under MM. MAR shows higher impact of 27% for the fork with Bitcoin Cash and 15%

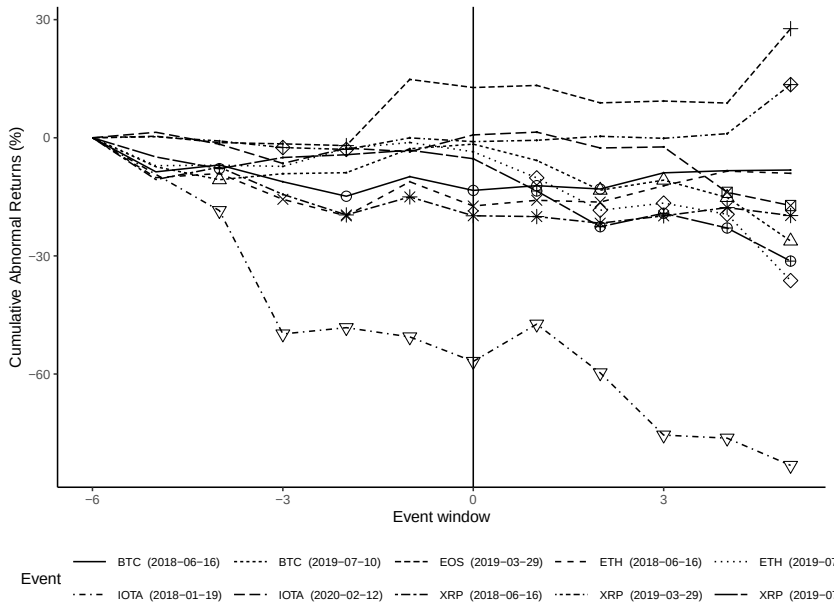


Figure 2.7: CAR for Wallet attacks (MAR model) with significant values ($p < 0.05$)

for the fork with Bitcoin Gold for the event windows inspected.

In this case, we note significance on CAR in all Hard Fork scenarios and reject the Null hypothesis. Our analysis shows that in general the sign of the effect of CAR can be either positive or negative: we can try to explain this phenomenon by relying on the intrinsic properties of the cryptocurrencies. From a technical perspective, a fork reflects a community split: in a PoW-based blockchain, this reduces the post-fork security of both systems. If the original cryptocurrency were to lose a significant part of its user base, we could expect a negative outcome on its price due to a perceived security weakness and loss of trust. On the other hand, economic gain could be possible if the new currency gains momentum without compromising the original one. If the new forked cryptocurrency is expected to succeed, buying original tokens ahead of the fork might grant a high return as it also yield valuable new currency tokens. We note that bigger and stronger cryptocurrencies such as Bitcoin did receive a positive impact on CAR in the event of a hard fork, while the effect was negative for smaller coins, where fear of community split and reduced security might have out-weight the prospects of economic gains from token-doubling.

Q4 (Wallet Attacks - Figure 2.7) We study the outcomes in terms of anomalous returns of the wallet attacks listed in Table 2.4. The attack that targeted Bithumb

during late March 2019 led to an initial significant negative impact on CAR for both of the stolen tokens (EOS and Ripple) both under MM and MAR. However, in the subsequent days their prices recovered, offsetting the negative response and in fact leading to a positive CAR for the end part of the event window under both models. A possible explanation for this could be the fast detection of the attack by the affected exchange, which immediately released a statement maintaining that no user's funds were affected as they were timely moved into a safe cold wallet storage. The fast reaction might have prevented a market panic. Interestingly, a wallet attack that had affected Bithumb one year before did create a bigger impact when 30 million (USD) in Bitcoin, Ether, Ripple and other alt-coins were stolen: that event likely affected the crypto market. The market model showed low negative impact on the cumulative abnormal returns, however MAR showed a higher significant consecutive negative impact for multiple event windows where cumulative returns appeared to be up to -20% for ETH and XPR and -15% for BTC than normally expected.

The attack on the Bitpoint exchange that affected these three currencies the next year also showed a steady and significant negative effect on CAR during multiple event windows, exhibiting negative cumulative returns for up to -18% for Ripple, -28% for Bitcoin and -26% for Ethereum under MM. MAR confirms the significance of the results rendering a negative impacts on CAR for BTC of up to -27%, up to -36% for ETH, and -31% for Ripple. A similar behavior is visible in other events: IOTA was impacted negatively by the coin theft that occurred in 2018 which showing an impact on CAR of -39% under MM and -83% under MAR. However, the smaller attack that affected this wallet provider in 2020 showed no negative impact on CAR under the market model, but it did render a significant impact under MAR of -17%, a result of the higher robustness of MAR for the analysis of smaller cryptocurrencies. We note an overall negative effect on CAR during the the event period and reject the Null hypothesis for all wallet attacks.

2.6 Conclusions

In this chapter, we analyzed the real-world economic behavior of cryptocurrencies under several categories of technical and community events that can be qualified as blockchain attacks. Our contribution includes a) a taxonomy of various types of cyber-attacks and adversarial behaviors applicable to blockchain technology and b) an analysis of the economic implications of the most relevant categories of attacks, evaluated in terms of their cumulative abnormal returns on the affected cryptocurrencies. To sum up our results in few statements: in general known 51% attacks affect the returns of the attacked cryptocurrency negatively under MM and

MAR models. While the first unreported 51% attacks lead to a significant positive impact on CAR under both MM and MAR, the second unreported attack differed in the impact under the two models. We emphasize that unreported attacks can create opportunities for pump-and-dump strategies (which may increase the attackers' profits further on top of the proceedings of a double-spend). Depending on the size and perceived security of the forked cryptocurrency, hard forks can lead to either significant positive (large cryptocurrency) or negative (smaller altcoin) effects. In general, wallet attacks lead to a negative impact on the "stolen" cryptocurrencies' returns. By treading lightly on the balance between real-world costs and in-kind incentives, cryptocurrencies exist on top of a potentially dangerous feedback loop mediated by the market valuation of their tokens. Based on the above observations, we believe that policy measures encouraging the timely disclosure of attack information could limit the damage of cyber-attacks and lead to a more efficient market response. Future research should investigate and model the price reaction to adverse blockchain-related events - ranging from direct attacks to the infrastructure to disagreements and splits in the community - and thus help defuse the potential profit-making strategies that exploit vulnerabilities of blockchains for financial gains.

Chapter 3

NAVIGATING THE GAP: CYBERSECURITY CHALLENGES IN BLOCKCHAIN AND CRYPTO REGULATION

This chapter is based on the article: Ramos, S., Melon, L., & Ellul, J. (2022). Exploring Blockchains Cyber Security Techno-Regulatory Gap: An Application to Crypto-Asset Regulation in the EU. *10th Graduate Conference in Law and Technology*, Sciences Po Paris. [44].

3.1 Introduction

The diverse palette of cyber security risks and vulnerabilities pertaining to the usage of blockchain technology and its applications has been recognized amongst experts and regulators. As we showed in Chapter 2, cyber-attacks related to blockchain and cryptocurrencies have significantly increased over the last decade. The Carbon Black report uncovered a total of $1.1 billion in cryptocurrency-related thefts during 2018 [112]. However, despite recognizing the urgency of the matter, the intricate technical nature of blockchains means that many cyber risks continue to evade comprehensive resolution. Interestingly, many of the cyber risks associated with public blockchains are closely linked to the publicly perceived attractive features of this technology such as its decentralized nature, the immutability of smart contracts, as well as the annonymous/pseudonymous nature of the network participants. As discussed in [20], blockchain technology brings novel types of cyber risks (particularly in the domain of crypto-assets) for which further attention is required.

In this chapter we focus on examining regulatory measures that could result in improved technical resilience of the blockchain system and its applications. While the task of designing resilient and sustainable distributed ledger technologies lies mostly in the hands of private entities and (de)centralized 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.

The remaining of this chapter is structured in the following manner. Section 3.2 gives a regulatory overview of the emerging fields of cybersecurity, blockchains and cryptocurrencies in the European Union. In section 3.3 we discuss the existence of a techno-regulatory gap, and explore the ways blockchain technology poses challenges to traditional cyber security measures. In the following section, we discuss viable measures that could mitigate certain 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.

3.2 Blockchains, 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. For example, the NIS Directive, adopted on 6th of July 2016, represents the first EU-wide rule book on cyber security.[1] Via the implementation of the EU directive (EU 2016/1148) for network and information security, Member States are supposed to create and enforce a national security strategy to deal with cyber-security risks. Recently 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[2]. The NIS Directive introduced the idea behind 'security by regulatory su-

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

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

pervision' requiring Member states to create cybersecurity authorities in order to supervise the providers of digital services and their compliance with the national cybersecurity strategy [113]. The EU Cyber Security Act introduced an EU-wide cybersecurity certification framework for ICT products, services and processes. It has paved the way for establishing a unified cybersecurity approach, enabling providers to operate seamlessly across the entire common market, eliminating the requirement for separate certificates from each Member State [113]. Likewise, the EU Directive on attacks against information systems[3] takes a rigorous approach, by holding cyber attackers criminally liable for attacks they commit against systems within the Union [113].

In relation to cryptocurrencies (and the underlying DLT), the European Securities and Markets Authority (ESMA) identified cyber attacks as one of the most significant risks, emphasizing 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) [45]. Recognizing the gap that exist in relevant law, the European Parliament in the recommendations to the Commission on 'emerging risks in crypto-assets' called 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 [46]. 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 [114]. 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 [115] and indeed given the nascency of the sector many jurisdictions have not taken any measures.

In 2019, 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 [116]. 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."*[117]. In an effort to determine the legal status of crypto-assets as part of the 'Digital Finance Package' initiative, as well as to reinforce cyber resilience within the union, the EU issued three regulatory proposals in 2020. A proposal on Markets in Crypto-Assets

[3] See Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.

(hereafter: MiCA) [17], a proposal for regulation on a Pilot Regime For Market Infrastructures Based On Distributed Ledger Technology [118] and a Proposal On Digital Operational Resilience for the Financial Sector (hereafter: DORA) [119]. After several stages of discussions, these regulatory proposals were approved in May 2023. Some of main objectives of these regulatory frameworks 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 [17].

Overall, DORA aims to create a framework on digital operational resilience whereby financial entities ensure they can withstand ICT-related disruptions and threats, in order to prevent and mitigate cyber threats. MiCA focuses in particular on defining crypto asset types, creating a framework for issuance, provision and services related to crypto-assets. MiCA differentiates between three main categories of crypto-assets (asset-referenced tokens, electronic money tokens, utility tokens). Arguably, MiCA centers its attention on the regulation and issuance of crypto-assets, with a particular emphasis on asset-referenced tokens and e-money tokens, as well as the facilitation of crypto-asset services[4] [120]. MiCA excludes from its scope fully decentralised[5] finance and native cryptocurrencies like Bitcoin [120]. Although MiCA does not automatically impose requirements for crypto-assets generated as rewards for maintaining a distributed ledger or validating transactions (such as the requirement for releasing a white paper), providers offering exchange services for the trading of such crypto-assets are regulated [120]. The scope of MiCA does not encompass digital assets already regulated as financial instruments or any other products falling under existing EU legislation. Instead, financial instruments are addressed by the DLT Pilot Regime Regulation[6].

In this thesis, we frequently direct our attention to the 'unregulated' space, which commonly involves native cryptocurrencies such as Bitcoin and instances of decentralized finance (DeFi). Once deemed financially negligible by European regulators, a recent report from the ECB acknowledges the transactional advantages presented by Bitcoin, particularly in developing countries, thereby elevating

[4]Crypto-asset service providers (CASPs), include custodial wallets, exchanges, Crypto-trading platforms, crypto-asset advising firms, etc.

[5]although the definition of 'decentralized' is blurry as we discuss further in this chapter.

[6]The DLT Pilot Regime applies to financial instruments (e.g., bonds, stocks, derivatives, etc.) that are issued, recorded, transferred and stored using DLT. The regime specifically targets DLT multilateral trading facilities, DLT settlement systems, and DLT trading and settlement systems. This regulatory framework grants these DLT market infrastructures certain exemptions from the stringent legal obligations imposed by MiFID II/MiFIR[121].

its economic significance [122]. As for DeFi, its market size was valued at around 14 billion dollars in 2022 and is expected to expand at a compound annual growth rate (CAGR) of 46.0% from 2023 to 2030 [123]. Noting the significance, in later sections, we examine this landscape from a cybersecurity standpoint which reveals substantial implications, as it exposes users to the intricate dynamics and vulnerabilities inherent to blockchains.

3.2.1 United Cyber Resilience Front within the EU

With the 'digital package' entering force, the European Union (EU) has successfully achieved important milestones regarding user protection in the domain of crypto-assets. First, the EU achieved a remarkable stride towards regulatory harmonization by fostering a cohesive framework among Member States. This alignment in regulatory policies and standards ensures a level playing field across the EU, promoting consistency, clarity, and a conducive environment for market participants. Such harmonization streamlines operations and ultimately cultivates a unified and efficient regulatory landscape for better cybersecurity resilience within the EU. However, its important to note that the blockchain ecosystem operates extensively across borders, necessitating the harmonization of rules and standards, along with global information exchange, to ensure the effectiveness of regulatory measures. Therefore a global coordination might be an imperative to ensure the high effectiveness of regulatory measures, as blockchain technologies and its applications often transcend geographical boundaries.

Second, the EU has taken proactive steps to institute cybersecurity measures by extending their purview to encompass third-party service providers (within the realm of crypto-assets) as well as issuers of asset-referenced tokens[7] as defined by MiCA (under Article 16). Now, third-party service providers such as crypto-asset trading platforms, exchanges, and wallet services providers, in the EU must operate with certain cyber security arrangements in place. In particular, this approach effectively enhances cybersecurity within the digital financial ecosystem. In the following section we discuss in more details the scope of EU regulation to safeguard against cyber risks related to service providers and other third parties in the crypto eco-system.

[7] Asset-referenced tokens are also known as stablecoins. They aim at maintaining a stable value by referencing several currencies that are legal tender, one or several commodities, one or several crypto-assets, or a basket of such assets.

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

In the crypto asset eco-system, the existence of service providers, including custodial wallet providers 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 eco-system. However, their economic significance has made them a significant vulnerability point, whose exploitation can compromise a large part of the ecosystem. By way of example, wallets are essential for a 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 [124]. When trading via centralized exchange (CEX), the exchange is basically the online service which has the custody over the assets deposited by users. In other words, when users deposit their cryptocurrencies into a CEX, those assets are held in the exchange's wallets or accounts.

In relation to security, wallet attacks usually target CEXs as a successful attack could result in massive thefts of coins. For example, Coincheck exchange hack resulted in losses of around 500 million U.S. dollars. As such, CEXs are seen as important players in the blockchain and crypto-asset eco-system as an attack on them could lead to a negative effect with important financial implications [125]. In the last years, exchange platforms and wallet service providers have often been a target of 'large-scale' cyber-attacks. Forbes estimated that around 27 percent of all cyber-attacks in the blockchain eco-system target crypto exchanges. According to [126], the primary reasons behind these hacks were attributed to the weak security measures employed by exchanges' hot wallets. Table 2.4, gives a list of different wallet attacks on exchanges and wallet service providers, and the losses incurred in millions of dollars.

DORA acknowledges the high cyber risk associated with the operation of these third-party service providers, which has not been previously adequately addressed in the EU legislation. With the increased adoption and usage of crypto-assets, DORA acknowledged the existence of regulatory gap and alluded to the need of harmonized oversight and monitoring framework, in order to tackle ICT risks stemming from third-party service providers, including concentration and contagion risks for the EU financial sector[8]. Moreover, DORA mandates for regulatory measures that will establish a suitable ICT risk management framework, including ICT-related incident reporting, testing and oversight of critical

[8]See (pg.3) of Regulation of the European Parliament and 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

ICT third-party service providers.

With DORA into force, crypto exchanges operating within the EU will need to implement comprehensive security standards, where vulnerability points are identified and properly addressed. In addition, critical third-country ICT service providers to financial entities in the EU will be required to establish a subsidiary within the EU so that oversight can be properly implemented. As noted under MiCA, crypto-asset service providers should also be held liable for any losses resulting from an incident related to information and communication technology, including an incident resulting from a cyber-attack, theft or any malfunctions. This is an important step, as it reinforces liability measures over the custody of users assets. On the negative side, elevating regulatory benchmarks, which entail increased monitoring expenses for cryptocurrency exchanges and relevant service providers, could potentially escalate the overall operational cost, increasing transacting fees for users. A complementary strategy to safeguard users' funds may involve the introduction of a 'crypto insurance' option [127]. Implementing a 'cybersecurity insurance' approach may serve as a means to differentiate users based on their risk tolerance. Simultaneously, this approach allows for more efficient allocation of resources by utilizing insurance fees to fortify areas most susceptible to cyber-attacks.

It is important to note that when transacting via CEX, a user does not per se have a direct contact with the blockchain itself, as CEXs are external entities to the blockchain main infrastructure. Likewise, a CEX may interact with the blockchain (such as withdrawals or deposits) but is not in charge of maintaining its operations. Likewise, CEXs do not have control over the governance of the blockchain. Governance decisions, protocol upgrades, and consensus mechanisms are determined by the blockchain's community or network participants, not by the CEX. This point in relevant when discussing cybersecurity measures and regulatory frameworks. The distinction between CEXs and the blockchain's core infrastructure may be crucial when considering the effectiveness of certain regulatory measures. Cyber measures such as the ones underlined by DORA, may have limited applicability especially when it comes to attacks that target directly the blockchain infrastructure, although these attacks may also have a spillover effect that can be noted by the users of an exchange. As we noted in Chapter 2, a majority attack will create negative abnormal cryptocurrency returns for users, even though the cryptocurrencies of these users were not stolen per se. Hence, users that transact through a CEX are not protected from security vulnerabilities and attacks that target the blockchain infrastructure and its incentive design.

3.2.3 Deterrence by Prevention: Viable Risk-Mitigating Measures

Certain EU directives[9] and DORA allude to the need for reinforcing 'soft measures' that can act as possible ICT risk-mitigating measures, preventing or diminishing the negative consequence of a given cyber-attack [99, 119]. Soft security can refer to immediate security measures which do not require high investment. We argue that certain soft measures (with a solid technical reinforcement) could be useful in a DLT setting, mitigating cybersecurity risks to a certain extend. In this regard, as possible viable measures in the context of DLT systems we note the following:

1. Monitoring
2. Increasing Awareness of users
3. Early Detection
4. Timely Reporting
5. Technology and security audits
6. Employee compliance standards

Tools that can be effective in certain cyber-attack situations are monitoring and blockcking of transactions when suspicious activity occurs on the network (even if its not related to the activities and the software) of the centralized exchange itself). In other words, in the case of theft of coins via a deep chain reorganization, a CEX could act by blocking internal 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 [128].

Monitoring a public blockchain to detect potential attacks can be considered a viable measure, although certain technical expertise and monitoring cost is required [129]. 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 [130]. As noted, attack monitoring helped Coinbase safeguard users funds [131]. Furthermore, investing in cyber-detection techniques may be one of the possible ways

[9] See Directive 2013/40/EU, Directive 2016/1148, Directive (EU) 2022/2555

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 Kok et al. explored the possibility for early detection of crypto ransomware using pre-encryption detection algorithms [132].

Timely reporting of attacks may also reduce the negative consequences. As seen in Chapter 2, 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.[10] Furthermore, prior research has emphasized the effectiveness of user awareness policies in significantly enhancing cybersecurity skills and actions [133]. Incidents such as the attacks on BitThumb, NiceHash, and YouBit exchanges were facilitated by compromised access to exchanges' employee login credentials. Consequently, adherence to compliance standards, cyber training initiatives, and regular technology and security audits are needed to reduce vulnerability points and enhance cyber resilience.

Overall, these measures are relevant to specific entities, such as centralized exchanges within the blockchain and crypto-asset ecosystem. However, it's essential to clarify that these measures do not necessarily pertain to a regulation of the blockchain infrastructure itself; instead, they concentrate on external operations connected to the blockchain. In other words, while transactions can be temporarily 'blocked' on the exchange software, they cannot be blocked on the blockchain. Consequently, the efficacy of these measures is limited, as we discuss in the following sections.

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

Overall, EU cyber-security related regulations such as the NIS Directives, often focus on organized, centralized entities and providers (e.g., DNS service providers, domain name registration services, cloud computing service providers, providers of online marketplaces, etc.), therefore might not be entirely applicable to the full scope of the blockchain eco-system, its operations and governance. Here the fundamental idea of the EU legislator has been to establish a digital environment

[10] 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)

where software failures are tackled at the root (risk-based approach), and the regulatory focus has been centered on entities involved in crafting digital products or delivering digital services, particularly in the design phase of products that incorporate software elements [113]. In contrast, the absence of a central authority, the open source nature of many DLT based systems as well as the the cross-border and pseudonymous nature of its participants makes it challenging to apply conventional regulatory approaches as we discuss in details in the following sections. Likewise, the EU 'Digital Financial Package' (including MiCA and DORA), primarily center around digital financial markets, financial entities and their operations, encompassing aspects like the issuance of crypto-assets and the provision of related services by third parties, as outlined in [119].

Overall, the current regulations are deficient in providing necessary measures and technical assurances particularly for decentralized blockchain systems and applications [115]. Given the frequent occurrence of software failures even in conventional systems, as indicated by [113], introducing technological assurances becomes crucial for enhancing system's security. Moreover, the inherent nature of blockchain systems exposes a variety of specific cybersecurity risks, not only associated with the software itself but also linked to the incentive mechanisms upon which the system relies (often composed of decentralized operating entities such as miners and validators). Specifically, in public blockchains, incentives can lead to malicious (dishonest) player behavior, such as miners colluding and executing majority attacks. This behavior can lead to serious economic consequences, endangering the security of the system and causing significant economic impact as noted in Chapter 2. In addition, incentive design at the block building level can also play role in market manipulation and front-running attacks (often by insider participants) - activities illegal in traditional finacial markets, which we discuss further in Chapter 4.

While the provisions of the EU regulations allude to the protection of user funds from hacking, degradation, illegal access, loss, cyber-attack or theft, not much further explanation has been given in particular to the technical complexity of blockchain technology. Besides security issues such as vulnerabilities in databases, protocols, APIs, etc. for which traditional cyber measures exist, current EU regulations do not 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, etc. has not been made.

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 what has been stated in current regulatory frameworks. We discuss this issue

in more details in Chapter 5.

In contrast, the People's Bank of China implemented the Financial Distributed Ledger Technology Security Specification whose purpose its to install DLT specific standards, specifically to ensure that security remains the main underpinning principle when delving further through the possible use-cases of DLT. The document addresses various aspects of such systems such as basic hardware and software, cryptographic algorithms, protocols, smart contracts, and operational and maintenance requirements [115]. Likewise, The Federal Reserve Bank of Boston introduced the concept of a 'supervisory node', which is a designated blockchain node established to fulfill supervisory functions within the blockchain based systems under regulatory oversight [115]. Nevertheless, these measures are not all-encompassing, as they still cannot fully cover the extent of the blockchain ecosystem, especially in situations where decentralization is prominent, whether in native cryptocurrencies or decentralized markets. In the following section we discuss the technical features of blockchains that constrain a more encompassing regulatory invention.

3.3.1 Challenges in applying regulatory measures

The decentralized nature of public blockchain systems is frequently recognized as one of its main attractive features. Here, the system's operations are maintained by decentralized nodes who are incentivized by the propensity of receiving a reward with an economic value (e.g., Bitcoin). The implementation of protocol rules, upgrades and other relevant software improvements usually involve the voluntary contribution from developers (distributed globally) with a characteristic of community-driven approach where decisions are made collectively, and contributors may not have formal relationships with the project. This has brought in place a regulatory dilemma, mostly due to the lack of a distinguishable dominant decision making authority which can be held accountable in case of attacks, failures and other security problems.

As argued by [134], on-chain conduct by network participants may render issues of tortious liability and non-contractual disputes, for which further regulatory clarity is needed. However, certain important blockchain-based operations seem to bypass current regulatory control [135]. 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. Addressing these concerns via regulatory measures in order to mitigate cyber risks (e.g. cyber-attacks) is a challenging task that requires further discussion and analysis. 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.

In the following paragraphs, we provide examples where the aforementioned points increase the challenges associated with regulatory intervention and cyber-security safeguarding measures.

3.3.2 Regulating 'Insider' Adversarial Behavior?

One could argue that one of the fundamental elements in upholding trust and security within a decentralized system lies within the consensus mechanism and the incentive engineering around it. 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 based on incentive models where each network participant is at the same time contributor and shareholder [136]. Incentive design can be portrayed as a pay-for-performance reward system, which compensates individuals for their 'honest' behavior [137].

Nissembaum [138] approaches trust and security in ICT as a conglomeration of two main factors, namely composed of insiders (e.g., miners, validators, core developers[11], etc.) and outsiders (e.g., hackers), maintaining that very often security issues can appear from an 'adversarial insiders'. This perspective has been essential when analyzing blockchains, as the system operations are primarily maintained by 'insiders', such as miners, whose 'dishonest' behavior may put the security of the system at stake. Figure 3.1, shows the tendency for attacks made from insiders for two consecutive years in the blockchain eco-system.

As maintained by Gambetta, trust in a system depends on the agency of others [139], and in the absence of trust in the agency of participants, further security measures are needed [140]. Arguably, regulatory frameworks ought to reflect the way economic incentives are propagated along with the structural roles of the agents involved [135]. 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 certain fiduciary duties

[11] includes leading the software development process or taking the main technical decisions about the program policies.

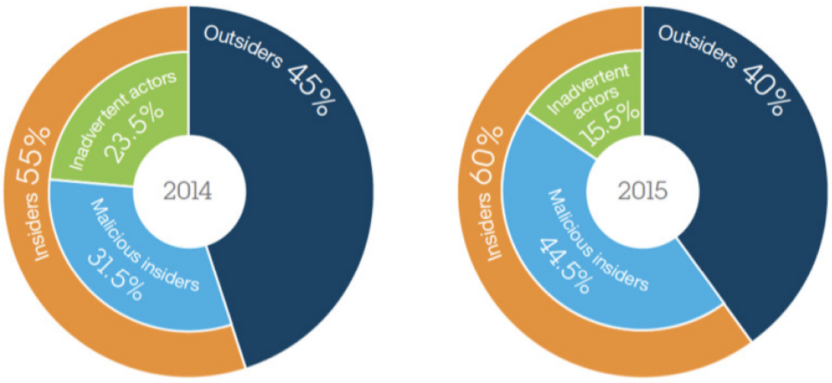


Figure 3.1: Insider vs. Outsider Attacks. Source: [1]

should be assigned to core developers and dominant miners) [141, 142]. For example, a suggestion has been made that developers working on smart contracts be held legally responsible if they were able to 'reasonably foresee' that their smart contracts will be used illegally.[12]

Nevertheless, certain challenges arise from this approach. Although protocol developers may exercise an influential role in the creation and implementation of certain software applications, protocol developers do not function as corporate fiduciaries, and labeling them as such could render negative effects in the blockchain ecosystem [143]. 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 [141]. By a way of example, Bitcoin is one of the most noted decentralized blockchain-based application, where anyone is free to voluntarily contribute resources to the network and the system operates thanks to the contributions of hundreds and thousands of people across the globe, collectively in charge of maintaining the network's operations [144].

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 further motivate rational miners[13] to group and form mining pools - which can act

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

[13]Rational agent or miner refers to one the fundamental principle of economics that every agent acts in his own self-interest and chooses what is best for him given his preferences and perceived economic outcomes.

as a colluding power with propensity to increase in size until it becomes a majority, thus having the possibility to perform organized majority attacks [145]. In a recent case in the English court, a dispute involved the developers of several blockchain networks and a user who loss his private keys due to a hack. The court acknowledged the importance and evolving nature of the relationship between developers and users in the blockchain ecosystem. However, the court emphasized that developers make a 'fluctuating, and unidentified body,' in the blockchain system, making it impractical to impose ongoing obligations. The English High Court concluded that there was "no serious issue to be tried" regarding claims of fiduciary or tortious duties owed by the developers [146]. Furthermore, blockchains are complex ecosystems where different liability rules may apply depending on a careful distinction of the layer and use cases [147]. Likewise, sometimes an attack on one layer can also have an impact on another, underscoring the significance of accurately distinguishing the nature of the attack.

Moreover, the anonymous/pseudonymous nature of network participants such as miners increases the challenges of assigning and enforcing regulatory measures [147]. 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 [148], 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 across the globe, hence associating and locating attackers (both insiders and outsiders) may increase the detection cost [147]. Arguably, enforcing necessary measures such as penalties can be challenging when it comes to DLT. Nevertheless, while regulating miners might be hard, certain measures to insiders might be possible in a context of a PoS setting (under the PBS design), as we examine in more details in Chapter 4.

3.3.3 DeFi and DEXs

The notion of how to apply regulatory standards designed for centralized systems in a world where there is no clear centralization, has sparked a discussion among academics and experts, particularly as adoption of DeFi has increased. A recent report by The International Organization of Securities Commissions [149], puts Decentralized Finance (DeFi) at the forefront of regulatory discussions, underlining the need for further regulatory intervention in order to ensure market integrity and investor protection. Decentralized finance (DeFi), has an aim of creating an entirely new financial system which is independent of the traditional centralized economy. DeFi is a diverse and rapidly evolving sector consisting of decentralized

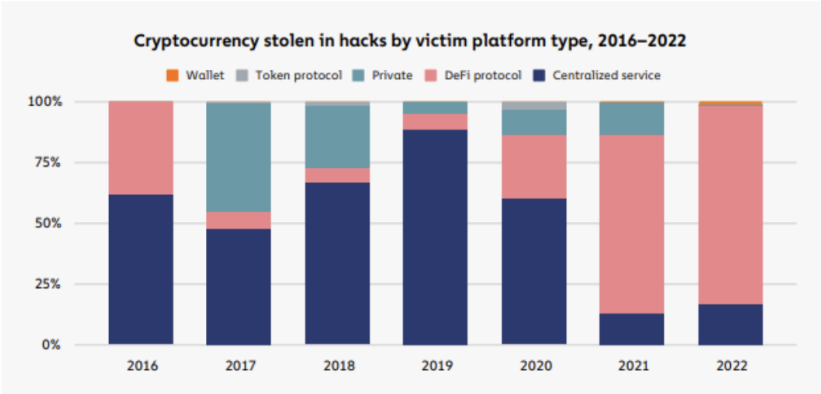


Figure 3.2: Attacks on DeFi Protocols vs. Attacks on CEXs. Source: Chainalysis The 2023 Crypto Crime Report

exchanges, automated market makers and other type of Dapps. Dapp is a decentralised application that can operate autonomously, typically through the use of smart contracts [149].

Decentralized exchanges (DEX), refers to a software program implemented through smart contracts integrated into a distributed ledger (such as Ethereum) [150]. This integration enables autonomous settlement of peer-to-peer transactions directly on the ledger. Decentralized exchanges allow for direct peer-to-peer cryptocurrency transactions without the need for a trusted intermediary. In contrast to centralized exchanges (CEXs), decentralized platforms are non-custodial, meaning a user remains in control of their private keys when interacting with the smart contract and transacting on a DEX platform. This advancement in technology is expected to significantly impact how users engage in asset exchange and interaction across various economic sectors. Here, the software is no longer a tool to be used by the people running the exchange; the software is the exchange. In other words, the software sets the prices and transfers assets automatically between buyers and sellers upon agreed set of conditions [151]. Regulatory measures involving the need of monitoring the blockchain to detect potential attacks, reporting them, and temporarily blocking operations, is challenging to implement in this context as there is no human entity responsible for these decisions and enforcing them in a smart contract setting might be overly difficult. The volume trading on DEXs as well as the global market size of DeFi have increased significantly over the last years [152, 123]. Likewise, the attacks targeting DeFi protocols have rapidly increased in the last years. Figure 3.2 show the increase of cyber attacks on DeFi protocols over CEXs.

According to [150], the structure of DEXs incorporates the following main

components: a) the blockchain platform and its technical execution, b) the mechanism for discovering counter parties, c) the algorithm for matching orders, and d) the protocol for settling transactions. There are two main ways DEXs can operate, depending on the way liquidity is provided: a) Order book based liquidity providers and b) Automated liquidity providers.

The order book liquidity provider model is similar to that of Central Limit Order Book centralized exchanges use. Order book based liquidity providers can be distinguished in two main categories, on-chain and off-chain order books. As noted in [153], on-chain order books involve the submission of all orders and their verification directly on the blockchain. Users are required to pay for each update made to the order book and wait for the network to achieve consensus. In contrast, off-chain order books handle all orders in a centralized manner, with only the final confirmation of transactions enforced by a smart contract on the blockchain [153]. This differentiation could prove significant when assessing the degree of (de)centralization and human intervention for potential regulatory measures. Lastly, Automated Market Makers (AMMs) are smart contracts designed to autonomously furnish liquidity in electronic markets. They introduce a novel approach to generating liquidity by exchanging two tokenized assets. Rather than determining prices based on demand and supply, AMMs aggregate liquidity and establish prices using a predefined pricing formula, eliminating the requirement for counterparties (buyers or sellers) [153]. As shown in [154], there are different security attacks that can impact DEXs. In Chapter 4, we examine in more details certain types of attacks related to AMM and evaluate the potential for regulatory intervention.

Although centralized exchanges (CEX) are still common, DEXs offer certain features that can can be considered as comparative advantageous in the future. DEXs transactions are characterized as non-custodial, automated, cross-border and pseudo anonymous [155]. In many instances, the pseudoanonymous nature of the system participants also adds constrains in identifying and enforcing any type of cyber requirements, assurances and penalties. Also, the cross-border nature of this system and the lack of regulatory harmonization on a global level adds to the difficulty of potentisly enforcing security measures. In other words, current cyber regulatory measures are often limited to blockchain based systems that are operated by private entities, organisations or communities where clearly distinguishable governance rules are set in place such as CEXs. As noted by [151], the regulatory efforts are misguided because the technology of DEXs is different from the technology for which traditional laws were created and large part of DeFi falls outside of current regulatory frameworks and proposals.

For example, under MiCA crypto service providers (e.g., CEX) ought to be registered and pre-authorized by a competent EU authority, where competent authorities may limit the withdrawal of authorisation to a particular service or sanc-

tion if an offence has been made[14]. This would be arguably difficult to achieve in a DEXs ecosystem where the smart contract code is the one acting as an exchange based on predetermined set of rules and users are the ones that have full custody of their funds and wallet IDs. The risk of massive wallet attacks (leak of Wallet IDs) is lower in DEXs as users have individual control of their wallet IDs (rather than a CEXs which stores all user wallet IDs). However, most of DEXs allow for full anonymity (e.g., no KYC is required) when transacting which creates the risk of criminal activities and fraudulent transactions on-chain such as money laundering and terrorist funding. According to the ECB, the 5th EU Anti-Money Laundering Directive does not cover decentralized exchanges, implying higher risk of criminal activities.

While not fully clear, MiCA's recital 22 maintains that where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation. Nevertheless, the same recital states that MiCA does apply even when some part of such activities or services are performed in a decentralised manner [156]. Therefore this raises a question over how decentralization is defined (e.g., technical, governance, economic, etc.) and how much decentralization is necessary to stay out of scope. Legal uncertainty over this issue is yet to show its consequences in possible litigation cases. Additionally, it's crucial to acknowledge that decentralization is not merely a binary classification but rather a dynamic continuum over layers that may evolve over time.

In the DeFi eco-system, current regulatory recommendation in the EU and in the US, have revolved around the ability to potentially identify centralized points and Responsible Entities[15]. For example, Bank of France argues that DeFi protocols and DEXs are often accessed by the average (non-tech user) through intermediaries such as: a) the (front-end) web interfaces of decentralised protocols and b) centralised intermediaries who make investments in the DeFi ecosystem on behalf of their clients, hence controlling their access[2]. Similarly, the International Organization of Securities Commissions argues for the identification of key responsible entities in the DeFi ecosystem for which future regulatory measures could be applied. These entities include: founders and developers of a project, those who have or take on the responsibility of maintaining/updating the protocol or other aspects of the project, holders and/or voters of governance/voting tokens, those with access to material information about the protocol or project to which other participants lack access, those with administrative rights to smart contracts and/or a protocol (i.e., with the ability to alter the coding or operation of the pro-

[14]See Article 57 and 58 of MiCA

[15]Responsible Entities are considered to be the ones that provide or actively facilitate the provision of products or services.

tocol to some degree) [157]. The report also suggests of identifying responsible entities with potential 'Conflict of Interest' such as builders or validators under PoS for which we discuss in more details in Chapter 4.

Overall, depending of the level of decentralization in the relevant layer, imposing certain regulatory measures (including cyber security measures) in the domain of DeFi can render to be extremely complex. A profound understanding of the the technical, governance and economic structure of the DeFi eco-system as well as the blockchain architecture is needed. As shown in Figure 3.3, the DeFi architecture can be complex, where access can be granted through both decentralized and centralized means. Regulatory intervention targeting centralized intermediaries and identifiable 'responsible entities' could create artificial disadvantages, making them less competitive in the market.

Furthermore, as previously mentioned, the blockchain system is in a state of continuous evolution, and the concept of decentralization can prove to be highly dynamic. Absence or/and the inability to identify an entity 'in-charge' can appear across layers and use cases. This can span from protocol/network (ex. Bitcoin mining) to the application layer (ex. decentralized exchange). Likewise, certain attacks can happen on one layer but have negative spill over effects across layers (e.g., front running at the consensus layer can have negative effect on price slippage).

On a contrary view, [151] argues that while regulatory efforts aim to cover the scope of DEXs in order to protect users, the nature of DEXs is overly beneficial and in line with regulatory aims. The authors maintain that given the transparent and traceable nature of blockchain technology, DEX software inherently empowers law enforcement in tracking and combating illicit activities. This fosters a competitive landscape for software solutions that assist regulators in monitoring suspicious behavior. Likewise, there are certain benefits to society for privacy and private transactions. However, here the question might be how much privacy is the optimal amount in order to ensure both protection and innovation.

3.3.4 DAOs

Decentralized Autonomous Organizations (DAOs) are a paradigm shifting innovation within the realm of blockchain and decentralized technologies. Many DeFi projects are governed by DAOs which can act as a virtual organisation built and run by code and blockchain technology. DAOs operate on the principles of decentralization, consensus, and smart contract automation. Essentially, a DAO is an autonomous entity governed by a set of rules encoded as smart contracts on a blockchain. These rules dictate the DAO's operations, decision-making processes, and allocation of resources [158]. Members of a DAO typically hold tokens that represent their ownership or stake in the organization, providing them with voting

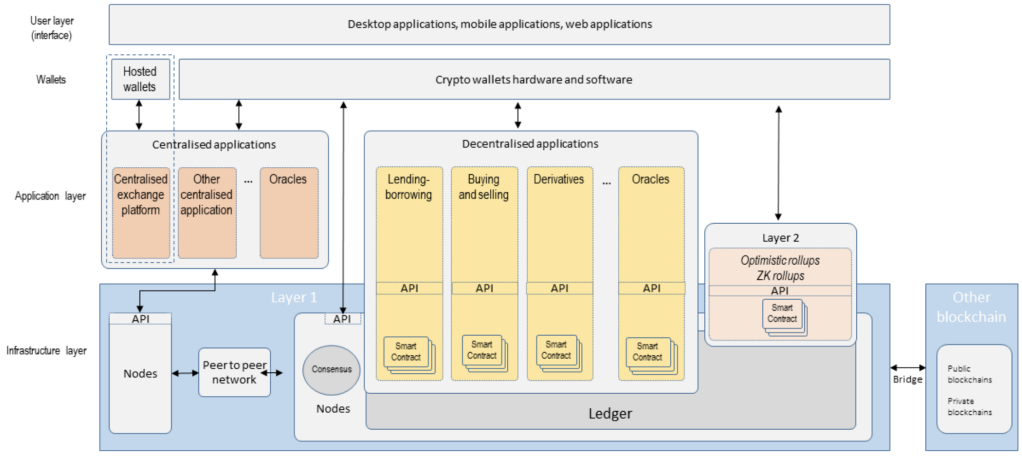


Figure 3.3: Example of DeFi Architecture. Source: [2]

rights to influence decisions. DAOs facilitate a democratic and transparent approach to decision-making, allowing participants to collectively determine the organization's actions, investments, and future direction [32]. However, challenges such as security vulnerabilities and potential regulatory scrutiny underscore the need for careful design, execution, and continuous evolution of DAO structures.

There is still no European or internationally agreed regulatory approach to DAOs. There are currently around 13,000 DAOs in existence, with a combined total treasury (invested funds and liquid assets) of 23 billions of dollars, as of May 2023 [159]. The profitability of DAOs also presents a dual-edged scenario, introducing a host of security challenges and vulnerabilities to potential cyber attacks. DAO hacks refer to unauthorized breaches or exploitations of Decentralized Autonomous Organizations (DAOs), resulting in unauthorized access to funds, manipulation of governance mechanisms, or disruption of normal operations. These breaches can occur due to vulnerabilities in smart contracts, governance flaws, or security weaknesses in the underlying blockchain technology. When successful, these hacks can lead to substantial financial losses and undermine trust and confidence in the DAO and broader blockchain ecosystem. The well known, Ethereum DAO hack, occurred in 2016, where a flaw enabled the attacker to initiate a recursive call exploit, siphoning off approximately 3.6 million ETH (equivalent to around 50 million of dollars at that time) [160].

While the immutability of blockchains and smart contracts ensures trust and transparency, it poses challenges in correcting vulnerabilities or addressing hacks that exploit the code. In other words, once a smart contract is deployed, its code is set in stone. If a vulnerability is discovered or exploited, it's not possible to directly modify the contract's code to fix the issue. To address a vulnerability or

exploit, developers may need to create a new version of the smart contract (an upgrade only if pre-stated in the conditions of the original smart contract) or initiate a network fork (such as the case of hard forking Ethereum mentioned in Chapter 2). However, these actions require consensus from the network participants and can be complex and contentious processes.

Another widely discussed regulatory challenge is the lack of central authority for intervention. Normally, traditional software can be patched or updated by a central authority or developer. However, in a decentralized environment, there's no central authority to make changes, making it harder to swiftly respond to security breaches. Therefore, it might be important to look further into the governance structure of a DAO, and hopefully distinguish a 'responsible entity' or any other decision making authority as it can be the case of majority token holders. In relation to DAOs, the International Organization of Securities Commissions recommends policy makers to take a regulatory direction of identifying majority holders and voters of governance/voting tokens in DAOS as well as DAOs founders or other relevant participants [157]. However, considering the cross-border nature and often pseudonymous feature of DAO participants, any regulatory measure (e.g., in case of identified liability) might prove to be challenging [158].

Likewise, distinguishing decision making power (and governance) by voting is not an easy task. Voting in DAOs is particularly complex topic for which there is an ongoing research in several disciplines [161]. For example, in quadratic voting, entities with most tokens do not always get to have the most decision power. In quadratic voting, the principle is that individuals can express their preferences on different issues by spending tokens. However, the unique aspect of quadratic voting is that the cost of expressing preferences increases quadratically with the number of tokens spent on a specific issue [32]. In other words, while people with more tokens can indeed express their preferences to a greater extent, they don't necessarily get a disproportionately larger decision-making influence. In fact, the quadratic nature of the voting system aims to prevent the accumulation of decision-making power in the hands of a few wealthy individuals [161].

While imposing liability measures, particularly in a case of cyber attacks may be very difficult in a DAO setting, a recent case of a hack has brought DAO token holders to a court. According to Coindesk, a U.S. court in California has ruled in favor of plaintiffs who alleged that the bZx protocol, and governance token-holding members of its decentralized autonomous organization (DAO), were negligent and liable for losses resulting from a hack that drained its treasury. The case was an example of a putative class action against bZx, its founders and software developers. Although certain claims were rejected by the court, such as holding founders personally accountable for breaching their fiduciary duty, the court's decision to allow the negligence claims to move forward represents a significant legal precedent in the somewhat ambiguous realm of governance token holders'

liability within DAOs [162]. Arguably, when there exists a clear founding entity or centralized authority, it becomes more feasible to implement effective regulatory measures.

3.4 The Case of Malta: Advanced approach to regulation

While regulating thoroughly the blockchain eco-system may seem like an impossible task, some countries have managed to apply more detailed approaches, particularly in the realm of cybersecurity protections and technical assurances. 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: 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 [115] 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 [163], which includes amongst other aspects:

1. functionality and code review
2. vulnerability, incident and security management
3. disaster recovery
4. risk management
5. 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).

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 [164]. 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:

1. Threat Agents (e.g., script kiddies, hackers, insiders, etc.);
2. Malware, phishing, DDoS attacks;
3. Hacking of a website/ web application;
4. Protocol design errors
5. Disruption of critical infrastructure of other parties;
6. 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 [165]. 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 [165].

As a EU member state, Malta is obligated to implement the recently enacted digital regulatory package. This section provides an illustrative example of a advanced regulatory approach, incorporating specific technological remedies suitable for the DLT domain.

3.5 Conclusion

The technological change and pace being witnessed in the cryptocurrency and DLT sector poses an ever moving 'regulation defying' target - for which a regulatory balance must be found to promote innovation whilst also protecting users and businesses. Jurisdictions around the world have and are investigating different approaches to regulating the sector. In this chapter, we delved into efforts being made by the EU to provide certain security assurances in the blockchain and crypto-asset domain through its recent regulatory frameworks. We highlight a techno-regulatory gap arising due to the technical nature of blockchain and its applications. We argue that users are not yet fully protected from the security challenges blockchain brings, specifically in certain sectors such as DeFi. With the ongoing expansion of this sector, both users and regulators may encounter additional challenges stemming from heightened cybersecurity threats.

Chapter 4

MEV DYNAMICS: CYBERSECURITY CHALLENGES AND POLICY PERSPECTIVES

This chapter is based on the article: Ramos, S., & Ellul, J. (2023). "The MEV Saga: Can Regulation Illuminate the Dark Forest?" In *Proceedings of the 35th International Conference on Advanced Information Systems Engineering under the Advanced Information Systems Engineering Workshops*.

4.1 Introduction

A basic rule of blockchains is that the most up-to-date state of the system is represented by the longest chain, and rational miners (under PoW) or validators (under PoS) are incentivized to generate new blocks that extend the chain further in order to gain the next block reward (and any fees associated with transactions included in the block). The higher the computational power of a miner (under PoW) or staking power of a validator (under PoS) the higher the probability of acquiring the ability to execute the next block is. Miners (or validators) receive transactions from various users and also may broadcast submitted transactions to other miners (or validators). Given the distributed and decentralized nature of the network, it is difficult to know the order in which users transactions were submitted - and therefore, it is up to the miners (or validators) to determine the order within which transactions are executed for the specific blocks a specific miner (or validator) is attempting to generate.

As transactions get published, they end up residing in memory pools (mem-

pools). Each miner (or validator) maintains its own mempool of pending transactions, and as discussed above, it is up to each individual miner (or validator) to decide on how to sort the transactions within the mempool. A node may decide to use a naive sorting strategy, where it simply appends transactions in the order the particular node received the transactions or it might perform a profit-maximizing strategies [166]. The ability for miners (or validators) to order transactions creates important challenges in the network which consequently impacts users and the overall system security.

Miner (or maximum) extractable value (MEV) is a measure of the profit a miner (or validator, sequencer, etc.) can make through the ability to arbitrarily include, exclude, or reorder transactions within the blocks they produce - and, of course, rational miners (and validators) do their best to ensure they make maximum fees. As a result, this may lead to front-running, 'sandwiching' and other forms of attacks and market manipulation strategies, which can affect market prices, users' funds and the overall trust in the system. While MEV extraction can be considered an inherited part of the block building design, the evolution and adoption of Automated Market Makers (AMM) opened new arbitrage opportunities bringing MEV to another level. Unlike traditional scenarios where miners/validators primarily determine the transactions included in a block, the introduction of smart contracts running market exchanges empowers them not only to shape block content but also to influence market movements. This dynamic introduces a novel layer of complexity and potential manipulation, as miners, through MEV strategies, can prioritize transactions that yield the highest returns. Consequently, the blockchain, instead of serving solely as a transparent ledger, becomes intertwined with market dynamics, posing concerns about fairness, market integrity, and the overall trustworthiness of decentralized exchanges. The interplay between smart contracts and miners' strategic decisions amplifies the need for careful consideration and potential mitigations to preserve the principles of decentralization and equitable market participation. Currently, statistics show that MEV is so pervasive that one out of 30 transactions is added by miners for this purpose, while MEV related sandwich attacks cost users more around 90 million dollars in 2022 [25, 26, 27].

Likewise as noted by [24], MEV posses some of the biggest centralization challenges in the Ethereum network. The issue of centralization emerges when a limited number of validators control a considerable share of the MEV extracted. In a Proof of Stake (PoS) system, validatos with larger stake pools are at a higher likelihood of being selected to build a block. This confers a notable advantage to larger validators in the extraction of MEV and the formulation of algorithms geared towards maximizing their revenue [24]. In the Ethereum ecosystem alone, the combined value of MEV after the Merge has surged by over 19,000%, totaling more than 300,000 ether (ETH). This remarkable increase occurred in less than a

year and is valued at around 490 million dollars based on current prices [167].

In traditional financial markets, user transactions are sequenced by a trusted and regulated intermediary in the order in which they are received. In a blockchain, by contrast, the updating of a block can be competitive and random. According to some critics, since these intermediaries can choose which transactions they add to the ledger and in which order, they can engage in activities that would be illegal in traditional markets such as front-running and sandwich trades, opening the discussion for the need of certain regulatory measures [168]. There have been several open questions on whether current regulation on insider trading is directly transferable to MEV. Recently, the Bank of International Settlements has emphasized this concern and asked for further regulatory research and adequate measures [26]. The International Organization of Securities Commissions, argued that miners (or validators) can be regarded as entities with certain 'conflict of interest' for which further regulatory attention is needed. The report also argues that MEV strategies may be subject to, or prohibited by, existing laws and regulations and that regulators should seek to hold relevant entities liable [168]. From a general standpoint, MEV related challenges could be analyzed and potentially mitigated from two angles (one does not exclude the other):

- by introducing technical solutions in the blockchain system and associated smart contracts, which includes developing incentive mechanisms under which the negative effects of MEV would be mitigated.
- by introducing regulatory measures that could mitigate the negative impact of MEV and protect users and other affected parties.

In this chapter we first examine some of the main technical developments in this field, that aim to reduce the negative effect of MEV. Second, we discuss potential policy intervention and their effects in a (de)centralized setting. Arguably, in order to make effective policy, a solid understanding of the technicality behind MEV is needed as regulatory solutions can find it useful to follow the current development on the technical side - in order to understand where things could have negative impact (or where centralization may occur) and what kind of related cyber attacks may prevail.

4.2 MEV basics: The dark forest and Flash Boys 2.0

The ability of miners to access the mempool and rearrange transactions in accordance to perceived fee value has been at the core of MEV. In general, there are harmful and unharmful activities that involve MEV. For example, arbitrage and liquidations are noted as potentially benign activities (unharmful) which tend to

promote market efficiency [169]. On the other hand, the harmful ones have predominated in market discussions as they have dramatically increased in the past few years costing users millions of euros.

While some articles regarding MEV focus on miners as profit maximizing entities that utilize mempool information to generate extra profits [26], the current system design enables other adversarial entities to target user transactions by creating diverse types of attacks. For example, currently many users have suffered from adversarial actions (such as front-running, back running, sandwich attacks, etc.) done by very specialized Arbitrage Bots that detect arbitrage opportunities across the network and replicate users transactions with a higher gas price hence managing to extract additional value, and overburden the system by creating bot-to-bot competition attacks [170]. Arbitrage bots constantly monitor pending transactions in the mempool and are able to rapidly detect and exploit profitable opportunities.

As emphasized in one of the earliest articles on MEV - 'Ethereum is a Dark Forest', the authors explain a situation where front-running arises because the transaction broadcasted by the legitimate claimant to a smart contractual payment, can be seen and slightly altered by others - specifically, arbitrage bots - to direct token payment to an alternative adversarial owned wallet [171]. By offering higher transaction fees and leveraging on the lag involved in this process, these bots can have the same transaction recorded with an earlier time-stamp, on the same or on an earlier executed block than the legitimate claimant, hence making the bot transaction valid and overruling the transaction of the legitimate claimer. This front-running example is very similar to the one described in [172]. There, front-running involves racing to take advantage of arbitrage opportunities that are created in the nanoseconds after someone engages in an asset purchase on financial markets but before the transaction has reached the market. Likewise, this type of front-running often occurs when bots try to take over arbitrage opportunities between cryptocurrency exchanges.

Alongside front-running, the most common MEV attacks also include back running, and sandwich attacks. Sandwich attacks are common adversarial techniques. For a sandwich attack to occur, imagine that Josh wants to buy a Token X on a Decentralised Exchange (DEX) that uses an Automated Market Maker (AMM) model. An adversary which sees Josh's transaction can create two of its own transactions which it inserts before and after Josh's transaction. The adversary first transaction buys Token X, which pushes up the price for Josh's transaction, and then the third transaction is the adversary transaction to sell Token X (now at a higher price) at a profit. Since 2020, total MEV has amounted to an estimated USD 550-650 million just on the Ethereum network [26]. MEV can also essentially increase the slippage in the trading price for users. Slippage is a de facto a 'hidden price' impact that users experience when trading against an auto-

mated market maker (AMM). When trading via an AMM, the expected execution price can differ from the real execution price because the expected price depends on a past blockchain state, which may change between the transaction creation and its execution because of certain actions (e.g., front-running transactions).

4.3 PBS: How does it work and why is it important

Proposer/Builder Separation (PBS) is a blockchain design feature that divides block building into the roles of block proposers and block builders. Block proposal is the action of submitting a block of transactions for the approval of network validators, while block building is the action of transaction ordering. When a blockchain protocol separates these two actions, it simplifies the process of completing each task and allows actors to specialize in one or the other. On most blockchains, a singular actor completes both tasks. For example, before Ethereum completed 'The Merge'[1] there was no proposer/builder separation and miners had a sole control. Arguably, proposer/builder separation (PBS) mitigates these problems by splitting the block construction role from the block proposal role.

In simplest terms, at first, users/searchers send transactions to block builders through public or private peer-to-peer transaction pools. A separate class of actors called builders are responsible for building the block bodies essentially an ordered list of transactions that becomes the main 'payload' of the block, and submit bids. Block proposers receive a block from their local block builder, and sign and propose it to the network. For their work, the chosen builder receives a fee from the validator after the execution of the block [173]. An important party in the block building ecosystem, Flashbots, play a crucial role in this system. Considered an important entity, Flashbots focus on mitigating the existential risks MEV could cause to blockchains like Ethereum. In essence, Flashbots provides a private communication channel between Ethereum users and validators for efficiently communicating preferred transaction order within a block. Flashbots connect users/searchers to validators while allowing them to avoid the public mempool [173].

As noted in figure 4.1, searchers (users) may send transactions via so called bundles through a block builder such as Flashbots itself. Bundles are one or more transactions that are grouped together and executed in the order they are provided. The builder simulates the bundles to ensure validity of transactions, and then builds a full block. In this way users can hide their transactions (avoid public mempool) before they are publicly executed in a block. Hence, users/searchers

[1]The upgrade from the original proof-of-work mechanism to proof-of-stake of the Ethereum network is called The Merge.

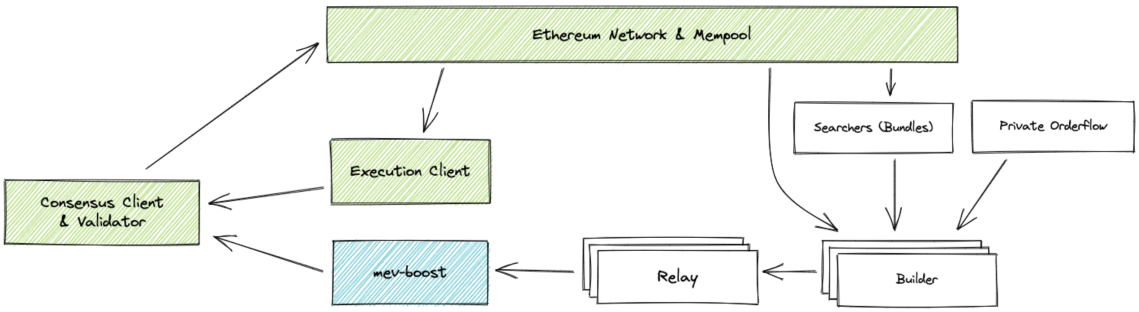


Figure 4.1: PBS Architecture. Source: Flashbots.net

can avoid potential front-running and other types of adversarial attacks by using Flashbots.

Whilst PBS is optional for validators, as they can decide to arrange transactions in their own way and extract MEV, PBS is beneficial for them as it minimizes validator computational overhead. Hence it is likely that rational validators would eventually resort to using PBS. However, PBS ultimately incentivizes builder centralization, shifting the need for trust from validators to builders. In essence, PBS does not fully avoid front-running attacks, as these can still be done by builders. Builders can still act as searchers and include their own MEV extracting transaction, ultimately front-running the users delegated transaction. In the effort to increase modularity and increase democratization amongst builders, Flashbots also introduced MEV-boost as part of the PBS structure. MEV-boost is a relay (a open source middleware) which helps create a competitive block-building market. MEVboost act as a trusted party and aggregate blocks from multiple builders and identify the most profitable block to submit to the block proposer (validators). At the moment this part is far from truly decentralized. Data from mevboost.org shows that there are six major active relays currently delivering blocks in Ethereum, including Flashbots which operates also a builder. The other active relays are BloXroute Max Profit, BloXroute Ethical, BloXroute Regulated, Blocknative and Eden. Ultimately, there are still certain security risks that can occur under the PBS design, such as:

- Builder Centralization
- Builder/Relay Collusion
- Malicious Relays

Understanding the risks associated with centralization and collusion are important as they open a regulatory discussion. Arguably, a centralized builder/relay

ecosystem, gains the ability for censorship and access to exclusive transaction order flow from which front-running types of attacks can be executed. Ultimately this creates market inefficiencies and impacts users negatively. For example, consider a wallet trying to send exclusive order flow to a single builder. For this order flow to be executed, it has to be included in a block on the blockchain which may take time. In order to avoid execution delays, a rational user will minimize this delay by sending the order to the builder with the highest inclusion rate, further increasing their dominance and centralization of the market. In that case, exclusive order flow would allow a builder, or small group of colluding builders, to capture the builder market, making it effectively uncompetitive. Also, a dominant builder would have a significant amount of private transaction information, allowing him to be in a more privileged position to extract MEV through front-running or other attacks.

4.4 Can Regulation illuminate the Dark Forest?

Arguably, MEV remains a niche topic and has demonstrated to be an evolving force, as evidenced by the proposed changes for block building design. Besides certain theoretically derived scenarios noted by [166], there are no other studies (to the best of our knowledge) that investigate the impact of MEV on welfare and measure the macro impact - an important factor that could merit regulatory intervention. Hence, we have resorted to looking at MEV from a security perspective - trying to understand when and how things could go wrong for users, in terms of attacks and vulnerabilities exploits (such as sandwiched user transactions) or in terms of transaction censorship (such as purposely excluding user transactions from the building block). We agree with [171] argument on the need for a more well-defined and detailed differentiation of the notion of what a 'victim' is in an MEV scenario. In other words, someone that has been deprived of something that was rightfully theirs may not be the same as someone whose 'transaction or trade-based profit' decreased due to certain market movement. Arguably, regulation is not meant to protect users by enabling conditions for them to achieve profit maximizing. Also, this definition may be interpreted differently as non-adversarial forms of MEV extractions (e.g., liquidation) may still indirectly render a negative impact on users via its effect on the market as a whole. In this chapter, we follow [174] and [171] differentiation of MEV under three broad categories: Monarch, Mafia and Moloch.

- 'Monarch' extractable value refers to the more broadly accepted understanding of MEV, as value extractable due to the power to order and allocate (block) space.

- 'Mafia' extractable value arises when one agent (coalition of agents) gains an asymmetric knowledge of another agent's private information (asymmetric sophistication).

- 'Moloch' extractable value arises from inefficient coordination methods.

In the following sections, unlike [169] we focus mostly on Monarchs (which can extract value based on their ability to dominate transaction ordering) and Mafia - referring to value that arises when an entity has asymmetric information of users' transaction information. We look at these two occurrences as potentially being performed by 'insiders' such as builders due to their ability to create adversarial attacks and market manipulative strategies in order to achieve higher profits. The regulatory recommendations on DeFi, maintain that regulators ought to seek 'Responsible Entities' in DeFi use-cases in order to be able to establish certain regulatory requirements that would protect users and investors from cyber attacks, market manipulations, frauds, and other types of negative effects [26, 168, 2]. Table 4.1 highlights some of the key entities that constitute the MEV ecosystem, some of which we refer to in our discussion.

4.4.1 Front-running in Traditional Finance vs. DeFi

In traditional finance, front-running is considered unethical and often illegal. The premise of illegality is based on the notion that a trader possesses and acts on an inside information to achieve personal gains. The non-public information concerning certain transactions ought to be of a 'material size' - meaning that it is significant enough to cause a price change in the futures or options contract and thereby allow the front-runner to profit [175]. An example of front-running in traditional finance is when a broker exploits significant market knowledge that has not yet been made public. This is similar to insider trading, with the minor difference that the broker works for the client's brokerage rather than inside the client's business [176]. In reality, front-runners profit by exploiting the discrepancy between the security's true value and its market value [175]. Consequently, the market price of the security being bought and sold does not reflect the true value of the security which distorts market efficiency. Enforcement of insider-trading regulations is currently a high priority for the Securities and Exchange Commission (SEC) [177].

The possibility that insider information can impact cryptocurrency returns has been noted in [22], where the authors show the impact of cyber-attacks news on price changes of the attacked cryptocurrency (in terms of abnormal losses). This example involves both a case of insiders and outsiders having a privileged information. Under 51% attack, malicious insiders such as miners performing the

Table 4.1: Taxonomy of Entities in the MEV Eco-system

Entity	Description	Threat
Developers	Design the protocol, creating potential for MEV opportunities	Can also create software tools, such as MEV Boosting Software, to extract MEV.
Miners	Under PoW, miners attempt to generate a block in a randomized loterry process.	Can extract MEV by deciding the order of transactions they include in a block
Validators	Under PoS, observes the pending transactions in the mempool and typically decides the to order the block with the highest gas fee paid	Can engage in front-running activities. Validator Centralization
Proposers	Proposer is essentially a validator under PBS that has been randomly selected amongst all the validators to build a block for a given slot.	Under PBS, treat is mitigated as proposer cannot see the contents of the block.
Builders	Under PBS design, builders generate blocks including transactions through the execution of algorithms and simulations aimed at arranging bundles of transactions within a block template to maximize profit.	Can engage in front-running activities. Builder/Relay Collusion, Builder Centralization.
Relay	A relay facilitates communication and aggregate blocks from builders to provide the most profitable block to proposers for validation.	Builder/Relay Collusion; Malicious Relays.
Bots	Seek and identify MEV opportunities, often through the use of complex algorithms. Bots often pay higher gas prices to place their transactions at specific positions within a block.	Front-running activities.

attack have this information which can cause market movement. In the other example, outsiders such as hackers attack a CEXs, holding an privilege information before the news come out and affect market prices. As mentioned in Chapter 2, the disclosure of wallet attacks to the public typically takes several days, allowing hackers or exchange employees with insider information ample time to take action.

In relation to MEV, insider information at the block building layer occurs amongst insiders such as miners (under PoW). In other words, front-running at the block-building layer can be exploited by insiders - due to the ability of miners to arbitrarily include, exclude, or reorder transactions in blocks, allowing them to even place their own transactions when they identify a profitable opportunity. This can be seen to be a much more serious case of front-running as it is not due to abnormal temporal shocks to the system (such as an unexpected cyber-attack) but as a byproduct of the block-building design.

On the one hand, miners may be seen as having access to insider information, but on the other hand, one could argue that this results from technical constraints causing a delay in recording transactions across nodes distributed in various geographical locations. For example, different nodes (e.g., a node in Australia and a node in Alaska) would not have a same view of the mempool's list of transactions, although there would be some overlap and similarities. This happens because every node receives transactions from different neighbouring nodes at different times. Also, the incentive design of the block-building (due to the restricted block size) is made as such to incentivize miners to prioritize transactions with higher fees. As shown by [178], transactions with zero or negligent fees wait for days to be included. Nevertheless, besides the mere incentivization to reorder and include transactions with higher fees due to basic economic incentives, the appearance of AMM gives miners (or builders) an important 'material' information which can be exploited beyond the fee generation.

When it comes to transaction ordering under PoS and the PBS designs, users can send transactions to builders via a private channel. This gives builders an exclusive insider information over potential front-running opportunities. As noted in [173], a centralized builder ecosystem or a single builder that dominates the market because of its outsized influence, achieves the ability for censorship and access to exclusive transaction order flow. According to [169] under the PBS design, a user can send a transaction only to one builder, placing this entity in a privileged position with 'material' information. The way a builder may arrange transactions could result in front-running or other types of adversarial attack which may impact the user's transaction gains negatively. Nevertheless, in this case there could be a loss of trust to the selected builder party which could disincentivize the user to send private flow transactions via this entity again.

4.4.2 MEV: Regulatory Challenges at the Block Building layer

A global securities regulatory body recently emphasized that regulators should aim to hold relevant entities accountable for identifying and mitigating strategies related to MEV. According to IOSCO, *"The ability to reorder, insert and otherwise control transactions enables conduct that in traditional markets would be considered manipulative and unlawful,"* [157]. Nevertheless, as we noted in Chapter 3, although dishonest (adversarial) on-chain conduct (e.g., majority attack) may render issues of tortious liability for miners/validators, treating them as fiduciaries would discourage them from participating in what may be considered a socially beneficial project, due to a fear of potential liability, and without them contributing processing power the system risks disappearing. Also, the anonymity/ pseudonymity and cross-border nature of the miner/validator system makes any identification and potential regulatory enforcement very challenging. As noted by [179], there might be little effectiveness of regulation of in a system that is composed of a decentralized and distributed (also no-easily-identifiable) group of entities. In a MEV scenario, we are facing similar challenge. While a sandwich attack can be noted on the chain [27], the pseudo-anonymous trait of miners makes it very difficult to regulate. As such, sanctioning 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. Also, while on-chain data is public, it is voluminous and complex, making it difficult to interpret and requiring specialized skills and significant infrastructure costs. Also some mempool data may not be always available - as it can be unique to individual nodes [168].

According to the Board of the International Organization of Securities Commissions, regulators should identify responsible central points in the eco-system and seek to hold a provider of a DeFi product or service responsible for MEV related activities, including front-running and sandwich attacks [168]. Whilst regulating decentralized system composed of many miners (under PoW) can be difficult, identifying centralized points under the PBS design (under PoS) might render easier. Under the PBS design the anonymity trait of builders is essentially reduced. This is because, while anyone can be a miner, builder entities tend to be more organized due to the overhead needed in their operation [24]. As noted by [180], the top three builders (Flashbots, builder0x69, and beaverbuild), consistently accounted for more than half of all blocks on the Ethereum network. Thus, with enough investigative effort it may be possible to identify the few builders involved in block building activities that rendered adversarial MEV strategies. Consequently if, adversarial builder action can be detected and if regulation has means to punish builders - than applying certain type of monetary sanctions may render useful in deterring malicious behavior (e.g. to perform front-running). A data analysis by [180], discovered that the number of MEV transactions included in a

block was significantly higher under the PBS blocks (one build by builders) than in non-PBS blocks. In other words, it shows that builders indeed have more 'material' information and ability to extract more MEV profits than proposers building their own blocks. The study shows that MEV profits account for a significant proportion of the total block profit.

Another measure that can possibly reduce some of the negative effects related to MEV, is for governments (or other trusted institutions) to have their own builders on important public blockchains. However this would imply a partial switch of trust to a heavily centralized governmental institution and a potential increase in transaction censorship. Government interference at block building level in public blockchains has been already shown in practice to have negative impact on the censorship resistance on the network. As noted, after OFAC (Office of Foreign Assets Control in the USA) sanctioned Tornado Cash and several Ethereum addresses associated with it, there was a noted difference in block building (transaction inclusion) - as blocks stopped including transactions coming from the mixer[2] (non-OFAC compliant) [181]. This basically means that block building players would either exclude any sanctioned addresses in blocks they propose or refuse to attest to any blocks that include such sanctioned addresses.

Another possibility for regulatory interference under the PBS design is via the Relays. Interestingly, most of the blocks involve a MEV relay which is an essential part of the overall selection of blocks that involves transaction ordering [25]. The MEV relay ecosystem is very centralized, as 81% of the MEV-relay market is dominated by Flashbots (as of October 2022) increasing the potential for block censorship due to a fear of potential liability (as 52% of blocks from MEV-boost relays enforced OFAC sanctions) [25]. Likewise, an analysis by [180] shows that some relays (bloXroute,bloXroute, bloXroute, and bloXroute) run their own builders, confirming the potential builder and relay collusion. In terms of censorship, several relays stated that they would comply with OFAC sanctions (Blocknative, bloXroute (R), Eden, and Flashbots), confirming the application of regulatory measures at the block building layer. Possibly due to a fear of liability (as regulatory MEV related statements have increased), a relay (bloXroute) claimed to filter out generalized front-running and sandwich attacks related transactions [180]. Arguably, MEV related measures might have an impact in the current the PBS design ecosystem, ultimately affecting the decisions by the still heavily centralized block builders and relays [182].

Alternatively, a type of monitoring measure that can be used by governments to make sure that transaction ordering is random (hence no strategy for front-running) is to oblige builders to use TEE (Trusted Execution Environment). Such

[2]Mixer is a services that is used to obfuscate the transaction trail of cryptocurrency, increasing user privacy.

TEE code could be programmed and then audited by governments to assure transaction ordering takes place in the desirable manner (e.g., random). While this would in theory avoid front-running by builders, it would increase the overall cost of using the system, as it adds another step in the process (increasing fees) and would decrease overall welfare creation. Moreover, this could potentially incentivize spamming the builder, as a malicious player could send many transactions which would increase the likelihood of one of the transactions being placed in front of the targeted transaction. Recently, encrypted mempools have also been mentioned as an extended trust and security effort which could also make it impossible for builders and proposers to know which transactions they are including in a block until after the block was already broadcast [183], overly reducing front-running activities.

4.4.3 No-regulation or Self-regulation

Overall, it is important to mention that regulatory measures (placed in a PBS scenario) will amount to not selecting a transaction to be included in a block (left in the mempool) due to a fear of liability, not an ability to 'block' fully a transaction as it is usually done in traditional finance. Likewise, applying regulatory measures at block-building in public blockchains may also undermine some of the most important traits of the system such as censorship resistance. Moreover, considering the cross-border nature of the blockchain network, regulatory arbitrage may appear when operators (e.g., builder) decide to register or operate from a place of favorable jurisdiction[169]. In addition, it is important to note that a propensity for centralization (e.g., builders, relays) does not always mean that the dominant entity would exert its power to over-run the system (or perform front-running activities).

An alternative which merits further discussion is the ability of the system for self-regulation. In line with Lessig's 'code is law', an argument can be made for the ability for on-chain governance to incorporate certain constitutional (regulation-like) principles into its block-building design which would imply a certain level of regulation and protection from colluding and centralized powers [179]. For example, as a desired outcome of the PBS design - if in the future a certain optimum is achieved as to create a competitive market for builders - a reputation system can be established as a form of self-regulation and user protection. In other words, a reputation system can be created where users could record if they suspect that any of their transactions were front-runned or sandwiched. This could serve as a security assurance for users, when selecting which builder to send their transaction to. Consequently, this type of system would reinforce trust in a potentially centralized setting. Likewise, on-chain incentive design suggestions imply a creation of a 'fee escalator system'. Under this system market inefficiencies seem to be corrected

(in theory) as the user is put in a seemingly powerful position to run an auction 'facing the other way' in the MEV supply chain. In other words, the situation can be flipped so that MEV extractors offer bids to users to execute their order. In line with [169], on-chain based self-regulation would avoid the high cost of regulatory intervention, such as monitoring, detection and enforcement of penalties.

As maintained by [47] and cited by [48]: *"Trying to apply centralized solutions to decentralized problems fails. It fails to scale, and it fails to achieve any of the stated goals. Although, it does push the decentralized platforms to try to innovate elsewhere. The answer is really simple. If you want to solve decentralized problems, solve them with decentralized solutions.... "*. This argument is in line with the resent statement by Bank of France underlining that the regulation of disintermediated finance cannot simply replicate the systems that currently govern traditional finance. On the contrary, regulations must take into account the specific features of DeFi. The report maintains that, such regulation should not be conceived as a monolithic block, but rather as a combination between traditional financial regulations and regulations inspired by other economic sectors [2].

4.5 Conclusion

In this chapter we dived into the MEV phenomena, shining light at the evolution of the blockchain (block building) design under certain economic incentives such as the presence of transaction fees and the market. We explain the novel Proposal Builder Separation (under PoS) and the vulnerability factors associated with it. Acknowledging the potential risks under PBS, where dominant entities like builders may harm users and the system through the extraction of MEV via front-running types of attacks, a mitigation of risks might be found in the advancement of a) technological solutions and b) regulatory capabilities. By identifying centralized entities in the MEV eco-system we discuss the potential for regulatory intervention. Nevertheless, we also warm over the possible negative effects of regulatory intervention at block-building layer due to their impact on censorship as shown in the case of the recent OFAC regulation. Lastly, we argue over the possibility for the system self-regulation and the need of novel regulatory approach when addressing challenges in the DeFi domain.

Chapter 5

CLOSING THE INFORMATION GAP

This chapter is based on the article: Ramos, S., & Mannan, M. (2022). "Watch the Gap: Making code more intelligible to users without sacrificing decentralization?" In *Proceedings of the IEEE 24th Conference on Business Informatics; Workshop towards Decentralized Governance Design* (Vol.24).

5.1 Introduction

A smart contract is an autonomous computer program designed to execute the terms of the contract automatically, eliminating the need for third-party involvement. The concept of smart contract was first introduced by computer scientist and cryptographer Nick Szabo in the late nineties [184]. Szabo described a smart contract as a 'smart' agreement tool that can automatically execute certain pre-programmed steps. Nevertheless, Szabo didn't argue for the superiority of smart contracts over paper contracts, as he noted that they should not be seen as intelligent tools that can phase out traditional contracts - as traditional contracts are designed to be understood by people and smart contracts by machines. In 2013, Ethereum's implementation of a virtual machine allowed for snippets of code (smart contracts) to be executed in a decentralized way without third party interference, bringing a whole new spectrum of applications and possibilities. Under this system, parties can coordinate themselves according to a set of protocols and rules incorporated into the self-executing code [29]. This has led some to describe blockchain and smart contract as 'trustless' technology due to the absence of need to trust an intermediary [185].

However, although disintermediation and decentralization have been regarded as ones of the most innovative traits of blockchain technology (and the smart con-

tracts relying on it), blockchain-based systems are complex socio-technological assemblages. These systems are made up not only of code, but they also involve large variety of actors operating at different layers [185]. As such, centralization can occur at different layers. We showed different situations of centralization: in Chapter 2 the concentration of mining pools and mining farms under PoW (as way to make mining rewards more predictable due to the increased difficulty level), or through the centralization of builders under PoS and PBS design noted in Chapter 4, or in the concentration of intermediaries operating on top of the blockchain such as CEXs noted in Chapter 3. Arguably, blockchain can be considered a type of algorithmically run 'confidence machine', in which users rely on the predictability of the technology but which inevitably involve trusting actors (such as developers, miners, wallet service providers, exchanges, etc.). In other words, blockchains do not eliminate the need for trust but provide reliable records and automation for transparent processes that may facilitate cooperation between agents [186]. This is also evident in the smart contract settings as we demonstrate in this Chapter.

Smart contracts can be created on top of public, decentralized and distributed ledgers, accessible to everyone willing to enter in a contractual relationship of a certain type. However, creating smart contracts requires certain technical knowledge and expertise, where average (non-tech) users are not able to develop nor fully understand a written smart contract code [2]. Hence, for a non-tech user to access smart contracts, he has to resort to a trusted party with sufficient technical expertise. This has ultimately limited the speed of expansion and adoption of smart contracts among the general public and created policy dilemmas among regulators. According to [37], the inability of average consumers to understand and interpret smart contracts in intelligible language has been seen as a challenge to consumer protection rights and the duty of information.

Arguably, the smart contract governance model focuses on proof-based automation of pre-stated functions run by the system and puts aside relevant legal rules and practices related to consumer protection and duty of information. In other words, this model focuses on providing function-based information written in a programming language (e.g. Solidity) needed for proper code execution, which may not be understandable to the average user. For example, Hyperledger Fabric business smart contracts are defined with specific programming-based terminology where function based queries are executed using transaction logic [187]. Thus, a user would need a trusted third party with sufficient technical expertise to 'translate' the rules and operations in executable programming code.

In this chapter, we focus on the issue of 'information gap' that appears when users are not able to understand the smart contract code or be provided with relevant information in an intelligible language. We underline the regulatory concerns this gap raises regarding consumer protection and duty of information, and the potential cybersecurity implications it can bring. Accounting for a wide-spread

adoption of smart contracts, we give examples of several ongoing initiatives that aim at closing the information gap, discussing the limits and opportunities of the prose-to-code paradigm. We maintain that although potentially beneficial for a wider adoption and legal recognition of smart contracts, the proposed solutions introduce a new type of intermediary in the system which ultimately affects the notion of trust and decentralization, creating a centralized intermediary which might need further regulatory oversight. Overall, we aim to make a practical contribution of relevance to the wide-spread adoption of smart contracts and bridge the gap that exists between legal and technical research.

5.2 Information Gap and Smart Contracts

There is still not a global consensus on the definition of the term 'smart contract' nor a systematic classification of its applications, as this term is still widely discussed among legal and technical experts [187, 188, 189], although the recent Data Act proposal in the European Union supports the setting of standards for smart contracts[1]. In general, the word *contract* can indicate that the agents involved are fulfilling certain contractual obligations or exercising certain rights and may take control of certain assets within the shared ledger. At present, the application of smart contracts has expanded across several sectors. Some of the noted benefits of smart contracts include a faster, cheaper, immutable, automated, distributed and more transparent way of creating and executing a contractual relationship.

In response, various legislative bodies and policymakers have initiated discussions over creating an innovation friendly approach to smart contract regulation which could include smart contract as legally binding if certain conditions can be met. For example, Arizona's Governor Doug Ducey signed HB 2417, which clarifies some of the enforceability factors associated with the use of blockchain and smart contracts under Arizona law, in particular with respect to transactions relating to the sale of goods, leases, and documents of title [190]. In June 2017, two other US states - Nevada and Vermont - passed laws concerning blockchain, with the legislation following the regulatory direction enacted in Arizona [191]. In Europe, a statement by the UK Jurisdiction Taskforce reasoned that smart contracts are capable of constituting legally binding contracts provided that the common law requirements for contract formation are satisfied [192]. Arguably, contract law is one the most important private law institution of individual self-determination and autonomy and it has evolved frequently to respond to the emergence of new contract models [193].

[1] See Chapter VIII of the Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act)

The inability of the average user to read and understand code is one of the biggest challenges in regulating smart contracts [168], alongside with inability to stop or correct code even if buggy [37]. However, the difficulty of transposing abstract concepts into contractual terms had been acknowledged long before the adoption of smart contracts [194]. Limited information and certain behavioral biases can also lead to non-optimal outcomes and efficiency losses in contract formations [195]. In recent decades, contract formation has also faced the challenges of digitization, raising issues such as the legal capacity of parties to enter in contracts and the genuineness of (informed) consent [195]. With the ongoing development and evolution of blockchain and smart contract systems, this challenge has taken on new dimensions, such as the publicity of (private) contract terms, the deterministic enforcement of unfair terms and (unless deliberately provided otherwise) the lack of an option to address and amend the inherent incompleteness of contracts [196].

Regulatory challenges regarding code-to-prose translation and interpretation have been discussed on an EU level [197]. In the EU countries, the applicable contract law includes not only respective national contract law but is also strongly influenced by European Union law. The proposed requirement for information disclosure depends on the type of a contract considered. Both the Directive 2000/31/EC on e-commerce and the Consumer Rights Directive 2011/83/EU focus on the formation of a contract on the internet. They establish precontractual obligations for consumer contracts to inform the consumer about relevant facts, which could be interpreted as also containing certain information about security vulnerabilities in a smart contract setting. As noted, failure to provide consumers with information in a clear and comprehensible manner may lead to heavy penalties [197].

Overall, in 'traditional' contract setting, consumers are granted information rights, which alludes to the right of a party to understand the agreement in intelligible language before any contractual arrangement is established. Under Spanish law, for instance, the requirements go even further as consumers who have entered into an agreement that has been drafted by a commercial entity have the right to obtain the terms and conditions of a contract on paper at any time [198]. In general, contract terms must be drafted in plain, intelligible language. Contract terms must not only be grammatically clear, but the consumer must be able to understand their economic consequences. This broad understanding of transparency entails that contracts should also provide clear information to agents regarding the potential implications and economic consequences of the contract.

In a smart contract setting, the issues that may arise due to misinformation or misunderstanding may entail high economic costs for the contracting parties. As noted in [199], ex-ante information costs to determine all contingencies could make smart contracting overly costly. Overall, reducing human intervention and

formalizing the creation of smart contracts can increase ex-post costs arising from bugs, coding errors and the implications of immutability. As a result, smart contract developers are faced with a dilemma - even if it is possible to transpose smart contract code into a written paper form, the terms may not be clear, plain and intelligible to the average user. With increased smart contract adoption, a question has been posed over the need for both lawyers and judges to develop sufficient expertise in understanding smart contract code and the underlying blockchain technology [200].

While some may argue that the role of the lawyer can be analogue to the role of the developer in a smart contract setting, this can be easily contested. In other words, non-lawyers typically can understand simple short-form agreements as well as many provisions of longer agreements, especially those setting forth business terms, while a non-programmer would be at a total loss to understand basic smart contract code [201]. In addition, as it can be seen in Figure 5.1, the high diversity of programming languages used to code smart contract further increases the complexity of the problem even for tech users. Likewise, as noted in [3], current programming languages are unsafe in the sense that it is easy to write code that expresses a behavior that is not intended.

One reason is that only a few operations are defined by the language itself and that programmers are allowed to create new functions with arbitrary names. Certain platforms such as Corda, use a more simplified type of code language (e.g., natural language programming) and can relate to the low-code initiatives that we discuss further in this chapter. While, they reduce the complexity of programming/understanding code for developers/tech entities they do not per se close the information gap for the average user. In [202], the authors argue that software's plasticity interacts with automation and immediacy to produce consequences that set it apart from both law and physical architecture.

As a result, some have argued for the establishment of legal institutions that will help decipher the meaning and intent of the code providing assistance in case of a dispute requiring adjudication. Decentralized arbitration services providing assistance for disputes (e.g., Kleros) have also appeared as a stepping stone in bringing technology and law closer. Moreover, in [197], the authors maintain that (in addition to future AI systems used for code interpretation), there will be a need for legal-tech experts capable of translating and interpreting smart contracts in natural language. The author notes that these experts will be in high demand and often out of reach for certain parties (e.g., average consumers who cannot afford high fees). This proves not only problematic in private enforcement but also in the absence of litigation [197].

From an economic policy perspective, the idea to establish a system of court-appointed experts to help decipher the meaning and intent of the code may be useful, however it would significantly increase the cost and burden to the legal

Platform	Ledger/Consensus	OPCode/ Language	Features
Bitcoin	UTXO, PoW	Scrip/Ivy	Linear execution conditions
Ethereum	Accounts, PoW	EVM/Solidity	General Purpose computing
Neo	Accounts, BFT	NeoVM/C+, Java	Many compilers for high-level language
NXT	Accounts, PoS	Temlates/Website Forms	Just parameters, no coding
Corda	UTXO, Raft	JCM/ Java, Kotlin	Stateless functions
Cardano	UTXO, PoS	IELE / Plutus	Functional programing
Tezos	Accounts, PoS	Michelson/Liquity	Formal verification

Figure 5.1: Programming languages used to code smart contract. Source: [3]

system. In contrast to automated control, ex-post audits can increase cost for regulators and show to be burdensome for businesses and operators [203]. Also as noted in [204], technical tools such as Al and API systems such as GPT3 and NaturalyCode are still not fully developed, providing not precise code to prose translation.The idea to use human based oracles (as external entities) to verify the validity of a contract in terms of consumer protection and provision o relevant information has also been suggested [193]. However, in this case, provision of contracts to external entities would still require some sort of precise conversion between code-to-prose. In [205], the author argues that programmers and lawyers should work together to create better smart contracts, while legislators focus on laws to ensure that smart contract code is audited by trusted third parties. In the following section we discuss the initiatives aiming at closing the information gap that exists between non technical agents within a predominately technical setting. We show a spectrum of low-code to no-code projects that introduce a new element to the smart contract governance model.

5.3 Low-Code and No-Code Initiatives

5.3.1 Low-Code Initiative

A 'low-code' platform is usually designed to make it easier for users to become blockchain developers, while in the case of 'no-code' initiatives, users are not re-

quired to have technical knowledge to interact with a smart contract. There have been several market initiatives, ranging on a spectrum between low-code and no-code. For the sake of simplicity, in this article we address these initiatives as Smart Contract as a Service (SCaaS). On the low-code side, a platform called Settlemint, specializes in low-code 'tool-kits' for building blockchain apps [206]. Via their platform, a user can interact and deploy a smart contract more easily. In other words, the company offers pre-written smart contract code, "zero config" REST APIs, along with zero-config admin UI and dashboard solutions. A similar initiative, SIMBA Chain's platform enables streamlined low-code smart contract deployment [207]. Low-code initiatives help users upgrade their technical knowledge or assist them in the creation and execution of smart contracts via a provision of technical 'tool-kits'. However, low-code solutions do not mitigate the information gap per se.

5.3.2 No-Code Initiative

'No-code' smart contract initiatives aim at assisting non-technical users in creating and interacting with smart contracts in their natural language. Although a full spectrum of translations between code and prose doesn't exist, these initiatives provide a solid step towards merging the information gap. As individuals and organizations become more interested in automating routine and business processes, bridging this gap can lead to an increase in the adoption of smart contracts and their applicability.

Most no-code initiatives fall under these two categories: template-based and DSL-based. Templates are the base for document generation. This premise can also be used for generating code-based smart contracts. While the user is not per se involved in creating a smart contract code, what he does is filling up a template based legal contract (written in natural language). The template later gets transposed in a smart contract code via a compiler of other similar computing mechanism provided by the SCaaS. The template also gets checked to make sure the data filled by the user is correct and will not modify the expected behavior of the code. A solid implementation of prose-based template for smart contract is Openlaw that gives the possibility for users to fill a prose based template and consequently generate contract transposed to a smart contract code on the Ethereum blockchain [208]. MyWish is another no-code smart contract platform, where users fill up a template looking document, specifying their requirements which MyWish later deploys via a smart contract [209].

Extending 'template specifications' creates Domain-Specific Language or DSL which is a more complex system that can allow for a higher flexibility and variety than a simple pre-certified prose-based template. A DSL can be seen be 'group' of templates that the user can arrange and fill to be able to define a more com-

plex requirement for code. DSL may be customized to the drafting of contracts for a given sector and can be (i) embedded in a general programming language (understandable for a programmer) or (ii) designed as a separate language (more understandable for a lawyer/average user if using a controlled natural language with user-friendly interface) [210]. One implementation example is Marlowe Run for the Cardano Blockchain. In the Marlowe Run platform, users can select a type of pre-written financial contract templates, fill it up and run it [211]. For more flexibility and options in building smart contracts Cardano created Marlowe Playground. However, Marlowe Playground is designed for users with some technical/developer knowledge. Hence, although DSL could potentially allow for much higher flexibility and creativity around contract development by no-tech users, its current applicability is still limiting and not as simple for users as template-based agreements. Intentional programming is another area of research that could provide flexibility and ease of use in the future.

5.4 Closing the gap?

5.4.1 Introducing a New Intermediary

The choice of 'no-code' initiatives is still limiting as it does not offer a comparable variety of code-to-prose agreements. Arguably, while smart contracts aim to avoid intermediaries such as lawyers and notaries, a suggested 'no-code' system introduces a centralized intermediary of another kind. This brings into perspective 'the Pitfall of the Trustless Dream' as defined by [212], arguing that despite the promises of decentralization, several instances in the blockchain eco system show signs of centralization.

From a technical perspective, the introduction of SCaaSs may increase the overall adoption of smart contracts, but it does not close the information gap per se. First, the uncertainty of whether a SCaaS platform is truly 'translating' smart contracts into natural language remains. As such, the non-technical users of 'no-code' smart contracts could become vulnerable to the whims of those operating these initiatives and users would need to take a 'leap of faith' that these initiatives would act in their best interest [185]. This creates a relationship of trust with the 'no-code' smart contract initiatives acting as intermediaries. Second, in line with [115], smart contract code is a piece of software and software failures due to bugs and errors have been common for years, in different systems across the world. Unlike traditional contracts that may include detailed clauses, meaningful context, or even legal language that provides insights into the parties' intentions, smart contracts primarily consist of code logic which defines its own concepts based on small set of operations and language primitives (e.g., comparisons, 'if' functions,

branches, etc.). The absence of human-readable elements in the code makes it difficult to precisely interpret the original intent or purpose behind the smart contract code. As the Debian project's 2008 discovery related to their OpenSSL package showed, the ('innocent') removal of only one line of code in critical software can go unnoticed for a long time while inducing serious consequences to its security properties [213]. Therefore, it is very difficult to arbitrate the mismatches between the intent and the actual behavior of the code [3].

According to [212], blockchain networks have also seen the introduction of intermediaries and developed certain 'chokepoints' such as SCaaS which aim to address certain challenges but might also bring new set of vulnerabilities in place. However, the growing adoption of SCaaS platforms has the potential to shield users from some cyber risks. The emergence of this new intermediary market, SCaaS, could facilitate the creation, testing, and legal certification of prose-to-code templates, thereby mitigating risks to a certain extent.

5.4.2 Security and Regulation

While automation via smart contracts can be viewed as beneficial because of reasons such as reduced costs and time of execution, it is essential to consider in the balance the coding errors, bugs and the effects of their possible exploitation. When interacting with smart contracts via SCaaS platforms, users face risks stemming from vulnerabilities in the smart contract code (e.g., issues related to logic, authorization, etc.) and misunderstandings of the operation of the contract (some related to prose-to-code translation) which can lead to unexpected outcomes.

While determining who is at fault in a smart contract setting is generally hard, as there can be many factors at the root of any issue, the presence of a registered intermediary (e.g., SCaaS) may increase user protection due to the specialized nature of the intermediary and the possible fear of liability for coding errors. Nevertheless, identifying a fault in terms of unintended behavior of the code can be complex. Unlike traditional contracts, which may be written in natural language and contain detailed clauses, smart contracts express their logic through programming code. Overall, even in presence of SCaaS the complexity of the situation remains high as the code may indeed dictate one form of behavior, despite the user's potential expectation of another [115]. Also, there might be a mismatch in user expectations, as the role of a SCaaS is not analogue to a lawyer in regard to drafting 'legal' contracts. In contrast to a SCaaS platform or a smart contract developer, lawyers bring legal expertise to the process of drafting traditional contracts, considering legal frameworks, regulations, and the specific needs of the parties involved.

An adequate response to these challenges is still discussed amongst regulators and experts at a global level. Overall, in the spectrum of liability, which is gaining

greater attention in the context of ongoing EU efforts to regulate crypto-assets, the SCaaS ecosystem may become a matter of regulatory concern as well. Bank of France argues that smart contracts and DeFi applications are often accessed by the average (non-tech user) through intermediaries such as web interface front-ends and centralised intermediaries, facilitating the prospect of regulating entities such as SCaaS in the future [2].

In the EU, liability of service providers within the cryptocurrency and blockchain realm could be evaluated through the prism of the Digital Financial Package, provided that safekeeping or controlling of crypto-assets was done on behalf of clients by the service provider. Other type of regulatory frameworks may apply such as the Directive 2000/31/EC on e-commerce and the Consumer Rights Directive 2011/83/EU which focus on the formation of a contract on the internet. Ellul et al. [115] suggest that technological assurances are also needed in parallel with sector specific (finance related) regulation present in the EU such as MiCA and DORA [119]. Providing technological assurances, in particular to DLT can be crucial in mitigating cybersecurity attacks and vulnerabilities, also present in a smart contract setting.

The Board of the International Organization of Securities Commissions underlined that what is written in a smart contract may need to be analyzed to determine whether it actually reflects what it is purported to represent. The report suggest that enhancements to the skills, datasets, and tools necessary to analyze DeFi data could improve a regulator's ability to oversee DeFi arrangements and activities [168]. Another potentially relevant EU regulation - the proposed Data Act, amongst other things seeks to set clear rules and standards for smart contracts used to automate data-sharing. As noted in the proposed Data Act, smart contracts must offer a high degree of protection against functional errors and manipulation by third parties. In addition, smart contracts must have internal functions which can reset the contract or stop its further execution (safe termination and interruption) [214]. Measures such as these ones, could plausibly strengthen the cyber resistance of smart contracts introducing obligations for relevant entities. Nevertheless, the Data Act does not identify who should have the power to give the command for a reset or stop actions and under which circumstances. Moreover, this might also not be entirely enforceable via technical measures or may prove too burdensome a requirement for smart contract service providers. The proposed act has already been strongly criticized by industry and experts as constraining innovation in the blockchain sector [215, 214].

In essence, a smart contract is a piece of software. In the EU, the proposal for an update of the Product Liability Directive[2], adopts a relatively inflexible position

[2]Proposal for a Directive of the European Parliament and of the Council on liability for defective products,

regarding software failures, instituting a strict liability framework for software developers [113]. According to some experts, developers of blockchain protocols and smart contracts should hold fiduciary duties (e.g., duties of care) towards users and others who rely on their actions, even if liability for software is contractually disclaimed, thereby opening the prospect of claiming remedies against them should they fail to abide by these duties [216, 217]. The role of 'core developers' includes leading the software development process and taking the main technical decisions about the policies and features to be embedded in the smart contract code [218]. However the inherent nature of blockchains and smart contracts makes this field challenging for regulators. As noted in [218], the existence of a breached duty of care is extremely complex to prove, particularly in the case of smart contracts, as the 'terms' - and any potential misbehavior they might lead to - are written in a programming language. Similarly, the tests to identify the developer's duty of care vary across the legal systems, bringing again to the forefront the cross-border nature of decentralized technology and its operators [218].

Errors in smart contracts are common and even additional check ups and auditing measures may not render this situation risk-free. According to [115], to minimize bugs in deployed systems, entities dealing with code should adhere to quality assurance processes, commonly encompassing:

- developer support tools that aid in error reduction during code writing;
- testing conducted by independent programmers or teams;
- verification techniques to ensure correct software operation before deployment; and
- in cases where bugs persist in deployed systems, a corrective approach involves fixing the identified bug in a new version of the code, subsequently updating the running system.

These requirements could be crucial if imposed on SCaaS, as they would enhance the assurance of code reliability and security to certain extend. These quality assurance processes, are not only pertinent to conventional software development but are equally applicable and essential when dealing with the implementation of smart contracts [115]. Given the immutable nature of data stored in DLTs, a meticulous adherence to these processes can increase the overall security, and functionality of the smart contracts. Hard forking is also suggested as a possible measure when bugs emerge that cannot be otherwise fixed. Nevertheless, hard forks also have impact on the system beyond the mere protocol split. They can have economic consequences and side effects on the perception of trustworthiness of the system, as we showed in Chapter 2.

5.4.3 Standardization and Certification

In general, a legal contract would include rights and obligations that accrue to the different parties and that are legally enforceable. These are often expressed in complex, context sensitive, legal prose and may cover not just individual actions but also time-dependent and sequence dependent sets of actions [219]. There may also be overarching obligations on one or more of the parties such that a lack of action could be deemed to be a wrong-performance or non-performance of the contract. That being said, [219] argue that there are two aspects the semantics of legal contracts being translated into a smart contract code:

- the operational aspects: these are the parts of the contract that can or should be automated, which typically derive from consideration of precise actions to be taken by the parties and therefore are concerned with performing the contract

- the non-operational aspects: these are the parts of the contract that shouldn't or cannot be automated.

In other words, the smart contract code is assumed to be standardized code whose behavior can be controlled (to a certain extent) by the input of parameters, while some of the values in the template may not have an operational impact and therefore should not be passed to the smart contract code. Hence, transposing legal prose into a smart contract code by SCaaS platforms may require for a clear distinction between operational and non-operational aspects.

The notion of creating standardized contract templates is not new in legal practice. For example, the oneNDA initiative established a singular contract template for NDAs [220]. According to the World Bank, there has been along tradition of the use of standardized contract agreements for the procurement of goods and services for traditional public works projects [221]. Other initiatives such as Template.net are helping users create their own legal contracts by filling up an already certified template with a legally appropriate contracting structure. In [222], the author maintains that smart contracts will likely prove suitable for specific industries and sectors, which would make templates and certification easier.

The Bank of France supports the idea that to strengthen the security of smart contracts, certification mechanisms should be used. The report suggests that certification should cover the security of the computer code, the nature of the provided service and its governance. In their view, certification would be obtained following an auditing process performed by a human expert, by using formal methods, or via a combination of these methods [2]. Certification would need to encompass a sizable list of requirements:

- To certify a smart contract, the prerequisite would be the certification of all the called components.
- Certification would adhere to fundamental principles: it should be revocable at any time; it should only be granted for a finite period to account for advancements in IT security knowledge and techniques.
- Furthermore, certification should be renewed after any significant alteration to the computer code.
- Lastly, if, in the future, smart contracts were to integrate specific regulatory requirements directly into their code, certification might involve checks to ensure the accurate translation of legal provisions into computer language.

The ability to design a sector/case specific contract template that would be certified, easily reproducible and translatable to a code by a compiler could bring economies of scale and increase adoption of smart contracts. In normal development practice, smart contracts are usually reviewed by third party developers to check that there are no bugs or exploits possible as noted in the section above. That takes time and can be costly, sometimes more than the development of the contract. By having certification frameworks (from a regulatory body), smart contracts can be certified to reduce the occurrence of bugs and errors, also increasing to certain extent the trustworthiness of of code-to-prose translation. This would also make potential auditing much more cost and time effective.

We see these two approaches working together - one from regulators and one from the industry. In Figure 5.2, we show how a user picks a template contract that's drafted in legal language, covering operational details. The regulator helps ensure the language of these templates is certified. Then, the template goes through a compiler, run by a Smart Contracts as a Service (SCaaS) platform, which turns the human-readable text into code that machines can understand. The compiler's execution is made secure with technical measures such as Intel Software Guard Extensions (SGX) to enforce the correspondence between the certified compiler's code and its deployed version. The techniques used, like machine learning, are in the hands of the SCaaS, which is motivated to make a better product for prose to code translation. After that, the SCaaS platform goes back over the code, checking for bugs and errors using various methods to make sure the implemented code matches the expected behavior. The regulator also certifies that requirements are embedded in the code, such as regulatory demands. If everything checks out, the code is then executed on the blockchain. Regulators will also have to be up to date with technical developments in order to revoke certification or apply other measures for certification if needed. In such a system, regulatory bodies will need to possess specific technical expertise or delegate relevant parties for

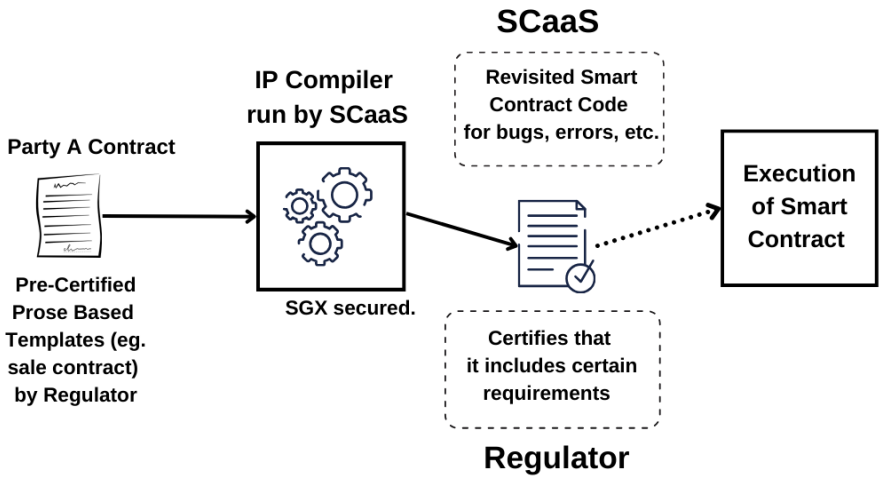


Figure 5.2: A RegTech system for prose-to-code smart contracts

technical certifications and audits. It's important to note that while this system doesn't make smart contracts completely risk-free, it can help reduce the potential negative consequences from attacks and vulnerabilities.

5.4.4 Is decentralization a dream after all?

The idea that blockchain-based systems could not fully operate outside of the purview of the law has been discussed by legal academics and experts. Lawrence Lessig argues that even in a smart contract setting the State is always part of the contractual relationship, because the value of a contract comes from its ability to be legally enforceable [200]. Nevertheless, he maintains that with current technological evolution, legal practitioners are not yet fully familiarized nor able to understand or properly interpret code-based contracts. Therefore, in the presence of 'code illiteracy' among judges and arbitration entities, there is a necessity to create specialized legal tech auditing bodies. These entities would be responsible for scrutinizing code to enhance the assurance of code intent and correctness, recognizing that achieving complete certainty in determining intent may not be feasible.

Hence, the question is not whether 'no code' initiatives bring centralization in a decentralized world but rather the real question is, where centralization is placed

to account for the information gap: in the hands of public authorities (often ex-post), or of private market initiatives (often ex-ante), or in a combination of both. Overall, the combination of operating initiatives plus regulatory and auditing bodies contributes to an increase in the overall confidence in the system (rather than relying purely on trust and the prospects for betrayal). From an economic point of view, certified intermediaries may be more cost-effective, as the 'checking' of code happens ex-ante, while in the case of public legal-tech auditors the correction would be made ex-post, once a problem has already appeared, hence a complementary approach would be arguably more effective. In [205], the authors argue that when regulating smart contracts, it makes more sense to prevent problems from arising than trying to correct them afterwards. These are not necessarily exclusive approaches, as regulators often opt for complementary solutions [197], especially when implementing a risk-based approach [223].

The idea that attention towards smart contracts and their overall cost will shift from execution to the drafting stage is highlighted by Shadab, who argues that parties would have to specify a more detailed range of contingencies and outcomes before committing themselves to abide by the decisions of a software-driven contract [224]. In [225], the author argues for ex-ante focus on code's production. He maintains that through ex-ante guidance of designers' production of technological normativity, it can be ensured that the illegitimate effects toward which computational legalism tends are minimized as far as possible.

Evidently, even the most apparently decentralized systems have shown the capacity to produce economically and structurally centralized outcomes [226]. The author maintains that for decentralization to be a reliable concept in formulating future social arrangements and related technologies, it should come with high standards of specificity. A rather optimistic thought would be that, as the smart contract market evolves and adoption of the technology increases, SCaaS initiatives would become better at prose-to-code translation. Likewise, if SCaaS initiatives evolve towards being open source projects there will be a potential increase in the transparency in the prose-to-code translation. Open source projects are typically organized in a distributed and decentralized manner, where certain factors determine the long term sustainability of the operations and the community involved [227]. The process of decentralizing SCaaS initiatives, if done right, could contribute further to building trust in the overall system.

5.5 Conclusion

Despite the evident advantages that support the utilization of smart contracts, such as transparency, automation, and immutability, the widespread adoption of smart contracts by non-technical users faces a significant hurdle at the intersection of law

and code. Guided by principles from contract law and consumer protection, we draw attention to the 'information gap' that exists between users, including judges and legal entities, and the intricacies of the smart contract code. In response to this challenge, we discuss a spectrum of initiatives ranging from low-code to no-code solutions (SCaaS) designed to bridge this information gap. Our discussion delves into the potential establishment of legal tech bodies tasked with scrutinizing code intention, translation, and interpretation. We explore how and to what extent regulations can address cybersecurity challenges arising in the context of SCaaS initiatives. Additionally, we reflect on the concept of decentralization, asserting that a temporary period of centralization is unavoidable in endeavors aimed at closing the information gap. Our overarching argument posits that the combination of operating SCaaS initiatives alongside regulatory bodies has the potential to enhance the security and trust in the system, mitigating cyber risks to a certain extend.

Chapter 6

BLOCKCHAIN FOR AI: EU AI ACT COMPLIANCE FROM A CYBERSECURITY VIEWPOINT

This chapter is based on the article: Ramos, S., & Ellul, J. (2023). "Blockchain for AI: Enhancing Compliance with the EU AI Act through Distributed Ledger Technology. A cybersecurity perspective." *International Cybersecurity Law Review Journal.*

6.1 Introduction

As we write this chapter, in parallel to the developments of DLT, it is evident that there are also an ever-increasing advancements in Artificial Intelligence (AI) technologies, a rapid adoption of AI-based products and services and national efforts to provide safeguards against the potential negative consequences of AI. The European Commission's Communication Report defines AI as: *"Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions - with some degree of autonomy - to achieve specific goals"* [228]. The International Data Corporation, a market intelligence firm, estimates that the worldwide AI market will reach a compound annual growth rate (CAGR) of 18.6 percent in the 2022-2026 period, peaking at 900 billion dollars in 2026 [229].

Beyond AI's potential, it is also a prominent example of a technology where cyber risks are becoming an alarming threat [230]. As adversarial actors are actively acquiring knowledge and skills to enhance the efficacy of their attacks, AI technology is becoming a focal point of attack due to its ever-increasing economic and social significance. Whilst AI systems are susceptible to attacks that are com-

monly encountered by traditional software, they are also vulnerable to specific attacks that aim to exploit their unique architectures based on knowledge of how such AI models operate. Furthermore, in AI systems, data can be weaponized in novel ways, necessitating changes in data collection, storage, and usage practices [231].

In response to such cyber threats, the European Union Agency for Cybersecurity (ENISA) has recently released a report that delineates the prevailing cybersecurity and privacy threats, as well as vulnerabilities inherent in AI use cases [232]. The analysis primarily concentrates on the identification of threats and vulnerabilities associated with machine learning techniques, while also considering broader aspects of AI systems. The field of AI presents several unresolved challenges that necessitate further research including: attaining verifiability, reliability, explainability, auditability, robustness, and unbiasedness in AI systems.

Additionally, the quality of datasets emerges as a critical concern, as: (a) the maxim 'garbage in/garbage out' highlights the requirement for high-quality inputs to yield satisfactory outputs; and (b) unwanted biases could emerge due to unbalanced datasets[1]. These issues are listed as open research questions by ENISA, alongside the need for designing more attack resilient AI systems. The regulatory concern over AI cyber risks was also noted in 2020, with the release of the document on the EU's Cybersecurity Strategy for the Digital Decade [233], maintaining: *"Cybersecurity must be integrated into all these digital investments, particularly key technologies like Artificial Intelligence (AI), encryption and quantum computing, using incentives, obligations and benchmarks"*. The need for improved cybersecurity measures in AI systems extends beyond the European Union. The Center for Security and Emerging Technologies in the United States has also underscored the urgency for policymakers to swiftly and efficiently address potential avenues for reducing cyber vulnerabilities in the realm of AI [234].

The proposed AI Act by the European Union seeks to establish a comprehensive regulatory framework for AI systems, with a primary focus on addressing ethical and legal considerations - yet it also recognizes and emphasises the significance for cybersecurity within AI systems[2]. During the same period the AI Act was being discussed and developed, blockchain was posing similar techno-regulatory concerns around the World particularly due to its use in cryptocurrencies - for which technology - focused regulation was proposed and eventually the EU's Markets in Crypto-Assets (MiCA) regulation was passed [235]. While aspects of blockchain and other Distributed Ledger Technologies (DLT), partic-

[1] See Section on Open Issues and Challenges under the Artificial Intelligence and Cybersecurity Research Report, ENISA. (2023).

[2] See Article 15 of the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM(2021) 206 final (April 2021)

ularly their decentralised nature and immutable offerings, have posed challenges to regulators as noted in previous chapters, we see their potential to fill certain compliance and risk gaps the AI Act leaves. We herein suggest how blockchain affordances can be used to mitigate certain AI-related cyber issues increasing the overall security of AI-based systems. In this chapter we examine how blockchain and DLT can enhance compliance with the EU AI Act and further reinforce cyber security measures.

In a widely complex eco-system such as AI and cybersecurity, academic literature has been generally focused on either the technical or purely legal aspects, creating an interdisciplinary gap that requires further attention. On the technical side, considerable attention has been devoted to exploring the diverse range of cybersecurity challenges associated with AI models [236, 237, 238, 239]. A plethora of studies have been conducted to delve into the technical aspects and vulnerabilities that arise in AI systems [240, 241]. Studies have investigated various dimensions of AI security, aiming to identify potential attack vectors and develop effective defence mechanisms. It is worth noting that this field, like the development of the technology itself, is highly dynamic and continuously evolving. As attack techniques are becoming increasingly complex and sophisticated, there is a need for ongoing research to uncover new vulnerabilities and develop robust countermeasures.

On the regulatory side, several studies explore the connection between AI and cybersecurity. For example, in [242], the author analyse the regulatory intersections between AI, data protection and cyber security within the EU legal framework. In [243], the study examine cybersecurity issues of medical devices from a regulatory standpoint, underlining novel challenges arising from the AI Act and NIS 2 Directive proposals. In [231], the author has highlighted the disconnect between cyber policy and AI systems. The author asserts that effectively addressing cyber issues associated with AI necessitates novel approaches and solutions that should be explicitly incorporated into relevant regulations. In a similar direction, the authors examine the upcoming European Regulations on Artificial Intelligence and Cybersecurity and provide an overview on the status of related policy actions related to cyber regulation in AI [58]. In [235], the authors argue that regulation should not be AI-specific but focused on software used in specific sectors and activities and later, while in [113], the author propose the need for techno-regulatory solutions to support software (and AI) related regulation.

When it comes to the intersection between blockchain and AI, in [56], the authors performed a bibliometric and literature analysis of how blockchain provides a security blanket to AI-based systems. Likewise, in [57], review is made regarding emerging blockchain applications specifically targeting the AI area. The authors also identify and discuss open research challenges of utilising blockchain technologies for AI. Furthermore, the authors converge blockchain and next-generation

AI technologies as a way to decentralise and accelerate biomedical research and healthcare. Another study examines how blockchain based technologies can be used to improve security in Federated Learning Systems [244].

To the best of our knowledge, there is a lack of research examining the integration of blockchain as a policy related tool for AI cybersecurity management. In line with [113], who maintain that the problem of technology regulation can be also addressed through the use of technology itself, in the following paragraphs we aim to examine how blockchain can be used to mitigate certain cybersecurity risks and attacks related to high-risk AI systems and to what extent these measures meet some of the cyber requirements positioned in the AI Act.

More specifically, we propose that blockchain can (a) address certain cyber attacks, such as data poisoning in trained AI models and datasets. Likewise, by employing decentralised infrastructure and blockchain technology, (b) AI systems can benefit from cryptographically-secured guardrails, reducing the likelihood of misuse or exploitation for adversarial purposes. Furthermore, we explore (c) how developers can restrict AI's access to critical infrastructure through tamper-proof decentralised infrastructure such as blockchains and smart contracts. Additionally, we examine (d) how blockchain can enable secure and transparent data sharing mechanisms through decentralised storage, augmenting data integrity and immutability in AI systems. Furthermore, we analyse (e) how blockchain facilitates independent audits and verification of AI systems, ensuring their intended functionality and mitigating concerns related to bias and malicious behaviour.

By leveraging blockchain technology, AI systems can align with some of the requirements mandated in the AI Act, specifically in terms of data, data governance, record-keeping, transparency and access control. Blockchain's decentralised and tamper-proof nature helps address some of these requirements, providing a potential foundation for accountable and trustworthy AI systems. Through this research, this chapter aims to shed light on the potential of blockchain technology in fortifying high-risk AI systems against certain cyber risks, contributing to the advancement of secure and trustworthy AI deployments (both in the EU and beyond).

The rest of the chapter is organised as follows: in section 6.2 we give an general overview of the cybersecurity risks in AI systems emphasising attack vectors relevant for our analysis. In section 6.3 we touch upon the AI Act and cybersecurity. In section 6.4 we delve into analysing the application of blockchain as a cybersecurity tool in mitigating certain cyber risks of AI, in parallel with some of the requirements of the AI Act. In the last section we present some closing thoughts and conclude the chapter.

6.2 AI: security vulnerabilities and attack vectors

Under the hood, AI systems typically make use of machine learning, logic based reasoning, knowledge driven approaches, target-driven optimisation (given some fitness function), or some other form of statistical technique. Indeed, the definition of AI has been debated for decades - and it is not the intention of this chapter to add to this debate, and neither support a particular definition of AI or what should be classified as AI or not.

Many such AI systems have the capability to operate within the realm of human-defined objectives, generating a spectrum of outputs that exert profound influence over the environments they interact with - for example consider AI algorithms used to moderate, filter and promote different content which can sway the public narrative. Through their intrinsic computational prowess, AI systems can manifest as tools for generating high-quality content, making accurate predictions, offering personalised recommendations, and rendering impactful decisions. If done right, these outputs possess the potential to reshape industries, optimise processes across a broad spectrum of domains and affect the fabric of society [245].

Upon collecting information, AI system engineers need to develop into such systems a profound process of interpretation, potentially leveraging vast knowledge repositories to extract meaning, identify patterns, and draw insights from the past data and/or the data at hand. Armed with this synthesised understanding, they are used to perform intricate reasoning, whilst contemplating a multitude of factors, associations, and dependencies to arrive at informed decisions. By integrating logical frameworks, probabilistic reasoning, and pattern recognition techniques, AI systems possess the aptitude to unravel complex problems, devise innovative strategies, and chart a course of action tailored to achieving their prescribed goals [246, 247].

However, AI systems are not impervious to vulnerabilities or weak points, as they can be targeted by various means, including attacks that exploit their inherent architecture, limitations or weaknesses [237]. These attacks can encompass a wide range of techniques, targeting underlying algorithms, data inputs, which may even involve exploiting physical components connected to AI systems. The susceptibility of AI systems particularly arises from their complex and interconnected nature, which creates many opportunities for adversaries to exploit potential weaknesses in their design, implementation, or deployment. In certain situations, AI systems may need specific cybersecurity defence and protection mechanisms to combat adversaries [237]. While one cannot ensure a fully secure AI system [230], in the following sections we take a close look at some prevalent cybersecurity risks concerning AI systems and how they can be mitigated with the help of blockchain technology.

6.2.1 AI attack vectors: data and humans

This chapter does not aim to provide a comprehensive overview of all AI cyber attacks, as it is a complex and extensive topic that warrants volumes of literature. Yet, we will focus on specific vulnerabilities and threats, for which blockchain can be a useful tool. In particular, we discuss data and human factors as potential attack vectors that can be exploited to target AI systems. The explanations provided are not exhaustive but serve as illustrative examples to enhance readers' understanding in the second part of the chapter.

Data-focused attacks:

Input attacks involve manipulating inputs that will be fed into an AI system in aim of achieving the attacker's desired outcome to alter the system's output [231]. Since AI systems function like 'machines' that take input, perform computations, and generate output, manipulating the input can enable attackers to influence the system's output. The importance that data plays throughout the lifecycle of such systems cannot be overestimated, from the building and validation of such systems to its live operation, it is at the core of the learning process of ML models. One of the most prevalent input attack vectors involves poisoning (i.e. manipulating) data utilised to train such models [248, 249]. Data poisoning attacks are a major concern in AI cybersecurity as they can cause substantial damage that can lead to undesirable socio-economic consequences. Consider a scenario where a public sector AI system is used to calculate levels of social help that should be given to (poor) families. Then consider that an attacker could poison the data so that the system delivers a result that particular types of families are not entitled to support.

Likewise, consider an attack scenario where the attacker has gained access to the training data and is able to manipulate it, such as incorrect labels or biassed information. This attack leverages the vulnerability of machine learning models to the quality and integrity of training data. If the attacker can inject poisoned data that influences the model learning process, they can alter its decision boundaries and compromise its performance [250]. Data poisoning attacks can occur at different stages, including during data collection, processing, or labelling. Adversaries may use various techniques, such as injecting biassed samples, modifying existing data points, or even tampering data within the training pipeline itself [251]. As put by [231], data is the 'water, food and air of AI' - and therefore, poisoning the data, one can attack the whole (or most) of an AI system.

Another similar form of attack, targets deep neural networks[3]. Here, the at-

[3]Deep neural networks (DNNs) are a crucial component of the artificial intelligence (AI) landscape due to their ability to perform complex tasks such as object detection, image classification, language translation, etc.

Attacks	Explanation
Evasion Attacks [253]	Manipulating input data to bypass detection or classification systems, enabling malicious content to go undetected.
Data Injection Attacks [254]	Inserting malicious or specially crafted data into an AI system to exploit vulnerabilities or trigger unintended behaviours.
Sensor Attacks[231]	Similar to the evasion attack. Here an attacker is manipulating input signals from sensors (e.g., cameras, microphones) to deceive AI systems relying on sensory input, such as in autonomous vehicles or security systems.
Concept Drift Attacks [255]	Introducing gradual changes in input data distribution to cause the AI system to make erroneous predictions or fail to adapt to new scenarios.

Table 6.1: Description of types of data-focused attack

tacker introduces subtle modifications in an attempt to manipulate the AI system's predictions. For example, attacks such as Projected Gradient Descent (PGD) and Square attack exploit the model's sensitivity to small and carefully crafted perturbations in the input data, causing the deep neural networks to produce false predictions [252].

As noted, data alterations can be carefully designed to deceive the system, causing it to produce incorrect or biassed results. These attacks can be challenging to detect, especially if the modifications are carefully designed to evade detection mechanisms or maintain normal system functioning in non-attack scenarios. A non exhaustive list of data-focused attacks is presented in table 6.1.

Human-focused attacks:

Attackers may attempt to manipulate or deceive individuals with access to the system, such as administrators or users, into revealing sensitive information, sharing credentials, or performing actions that compromise the system's security. Likewise, developers play a key role in building, maintaining, and securing AI systems. Developers typically have privileged access to underlying code, infrastructure, data sets and configuration settings of AI systems. They possess the technical knowledge and expertise required to modify, update, and maintain such systems. However, their access also presents a potential vulnerability that can be exploited by malicious actors through various means including social engineering.

Consider a code alteration type of attack, where a malicious party gains access and a modification is made to the code of an AI system (which may include model

parameters) in order to manipulate its behaviour or achieve malicious objectives[4]. While this could be also said for other types of systems, one of the main differences (between traditional systems and AI-based systems) is that such changes may result in system behaviour that still seems to be correct. Also, code alterations in high-risk AI systems, can have detrimental consequences to users and society in general. For example, an autonomous driving system relies on computer vision algorithms to detect traffic signs. In a code alteration attack, an attacker could modify the source code responsible for sign recognition to deliberately misclassify stop signs as yield signs. This alteration could lead to potentially dangerous situations on the road, as the autonomous vehicle may not respond correctly to the altered signs.

This brings to light the importance of access control protection for developers and other important stakeholders as an essential security measure. In [256], the authors maintain that if the developer access is not properly protected, attackers may gain unauthorised access to their accounts or exploit their privileges to modify the code, inject malicious components, or introduce vulnerabilities in the AI system. Moreover, developers often have access to sensitive data used in AI systems. Inadequate access controls can expose this data to unauthorised access or increase the risk of data theft, leading to breaches of confidentiality and potential harm to individuals or organisations.

6.3 The AI Act and Cybersecurity

Following the European Commission's release of its long-awaited proposal for an AI regulatory framework in April 2021 [257], there has been notable progress among EU institutions and lawmakers in establishing the EU Artificial Intelligence Act (hereafter: AI Act). The AI Act aims to fulfil the commitment of EU institutions to present a unified European regulatory framework addressing the ethical and societal dimensions of AI. Once enacted, the AI Act will have binding effects on all 27 EU Member States, marking a significant milestone in the regulation of AI at the European level[5].

While the AI Act primarily focuses on ethical and legal aspects of AI, it also addresses the importance of cybersecurity in AI systems. In relation, the AI Act emphasises the need for AI systems to be designed and developed with cybersecurity in mind[6]. It requires that AI systems incorporate appropriate technical

[4]These attacks typically target the underlying algorithms, configurations, or functionality of the AI system.

[5]Nonetheless, it remains unclear when the AI Act will come into force, given anticipated debate over a number of contentious issues, including biometrics and foundation models.

[6]See Article 15 of the Proposal for a Regulation of the European Parliament and of the Council

and organisational measures to ensure their security and resilience against cyber threats. For example, the AI Act mandates that AI developers and deployers conduct thorough risk assessments to identify potential cybersecurity risks associated with their systems [258]. Based on the risk assessment findings, organisations are required to implement appropriate mitigation measures to reduce the identified risks and enhance the cybersecurity posture of the AI system.

Furthermore, the AI Act recognizes the importance of data security in AI systems. It requires that personal and sensitive data used by AI systems be adequately protected against unauthorised access, disclosure, alteration, and destruction. The Act also promotes the use of privacy-enhancing technologies to safeguard data privacy and confidentiality. Furthermore, it emphasises the importance of transparency and explainability in AI systems, which includes cybersecurity aspects. It requires that AI systems be designed in a way that allows auditors and regulators to assess the system's security measures, including cybersecurity controls, to ensure compliance with regulatory requirements. In the event of a cybersecurity incident or breach involving an AI system, the AI Act requires incident reporting to the relevant authorities[7]. It also encourages cooperation and information sharing among stakeholders to address and mitigate cybersecurity risks collectively[8]. The AI Act introduces a voluntary AI conformity assessment framework, which may include cybersecurity criteria. The framework allows AI systems to obtain certification to demonstrate their compliance with the Act's requirements, including cybersecurity measures[9]. The AI Act designates supervisory authorities responsible for overseeing compliance with the Act's provisions, including cybersecurity requirements. The authorities will have the power to audit, assess, and enforce compliance with the measures outlined in the Act - aspects of the approach have similarities to what was proposed by the Malta Digital Innovation Authority [113].

The AI Act categorises AI systems into four risk levels: unacceptable risk[10], high risk, limited risk, and minimal risk. Each category is subject to specific regulatory requirements, determined by the potential harm they may cause to individuals and society. The proposal clarifies the scope of high-risk systems by adding a set of requirements. AI systems listed in Annex III of the AI Act shall be considered high-risk if they pose a 'significant risk' to an individual's health, safety, or fundamental rights. For example, high risk AI systems listed in Annex

laying down Harmonised Rules on Artificial Intelligence and amending certain Union Legislative Acts (Artificial Intelligence Act), COM(2021) 206 (April 21, 2021).

[7]Procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62 of the proposed AI Act

[8]See Title 8, Chapter 1. of the AI Act

[9]See Article 42 on Presumption of conformity with certain requirements of the AI Act

[10]Under the AI Act, AI systems that carry 'unacceptable risk' are per se prohibited.

III include those used for biometrics; management of critical infrastructure; educational and vocational training; employment, workers management and access to self-employment tools; access to essential public and private services (such as life and health insurance); law enforcement; migration, asylum and border control management tools; the administration of justice and democratic processes, etc [259].

With the goal of contributing to the mitigation of risks, our focus in this chapter centres primarily on the high-risk category. This specific category not only holds significance but also offers an avenue for leveraging supplementary measures, like blockchain-based tools. It is worth noting that, the AI Act and the NIS 2 (Network and Information Systems) Directive share significant commonalities in terms of cyber security requirements. Both the AI Act and the NIS 2 Directive adopt a risk based approach to cybersecurity. They emphasise the importance of identifying and assessing risks associated with AI systems and critical information infrastructure, respectively. Furthermore, both frameworks impose obligations on relevant stakeholders to ensure the security of their systems. The AI Act requires AI developers and deployers to incorporate appropriate technical and organisational measures to ensure the security and resilience of their AI systems. Similarly, the NIS 2 Directive mandates operators of essential services and digital service providers to implement robust cyber security measures to protect critical infrastructure. Likewise, both frameworks designate supervisory authorities responsible for overseeing compliance with their cybersecurity provisions. These authorities have the power to audit, assess, and enforce compliance with the requirements outlined in the AI Act and the NIS 2 Directive. Among other things, their role is to ensure that relevant stakeholders adhere to robust cybersecurity practices and measures.

In addition, recently ENISA (European Agency for Cybersecurity), released a report on providing an overview of standards (existing, being drafted, under consideration and planned) related to the cybersecurity of artificial intelligence, assessing their coverage and identifying gaps in standardisation [260]. The report examines the role of cyber security within a set of requirements outlined by the AI Act such as data, data governance, record keeping, risk management, etc. Overall, the AI Act recognizes the significance of cybersecurity in AI systems and establishes measures to ensure their resilience against cyber threats. By incorporating cybersecurity requirements, risk assessment and mitigation, data security, transparency, incident reporting, and compliance mechanisms, the AI Act aims to promote the safe and secure deployment of AI technologies in the European Union.

6.4 Blockchain for AI: A tool to achieve compliance with cyber and data security requirements under the EU AI Act.

6.4.1 Data Integrity and Immutability

Data integrity and immutability are critical aspects of ensuring the reliability, security and trustworthiness of AI systems. The AI Act highlights the significance of employing high-quality training data, unbiased datasets, and ensuring that AI systems are not trained on discriminatory or illegal data. The Act states that data quality should be reinforced by the use of tools that verify the source of data and the integrity of data (i.e. to prove that data has not been manipulated). It also underlines that access to data should be limited to those specifically positioned to access it. The Article 15 of the AI Act argues for the implementation of *"technical solutions to address AI specific vulnerabilities including, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws."*.

Blockchain technology offers a robust solution to address these concerns by providing a decentralised and tamper-resistant ledger for securely transferring, storing and verifying data [261]. Indeed, it must be noted that data stored in a public blockchain implies that the data would be available for anyone to see, yet various different techniques may be adopted to both: (i) ensure data is kept private (and not directly stored on a public blockchain); and (ii) ensure data integrity can be upheld (through storing cryptographic hashes of data on a blockchain). In Chapter 7 we demonstrate a blockchain enabled privacy preserving protocol which ensures data confidentiality.

Blockchain's immutability feature mitigates these risks by creating a permanent record of data transactions that cannot be altered or tampered with. When data is recorded on the blockchain, it is stored across all nodes in the network, forming a decentralised and synchronised ledger. New data, such as the addition or modification of training data, is cryptographically linked to previous transactions, creating a chain of blocks that is generaly resistant to modification. This ensures that once data is added to a blockchain, it becomes impossible or infeasible to alter or manipulate without the consensus of the network participants. Any attempts to tamper with the data would require significant computational power and/or consensus among the majority of network participants, making it economically and practically infeasible.[11]. Furthermore, applications digitally sign data

[11] As we discuss in previous chapters, attacks at the consensus layer in blockchain systems are

transmitted to a blockchain, and therefore it would be possible for an application to verify whether any data the application itself has submitted has since been manipulated.

These features of immutability and verifiability can further help applications to comply with the AI Act's proposition regarding incorporating 'logs' in AI-based systems. The regulator emphasises the need of having high-risk AI systems designed and developed with capabilities enabling the automatic recording of events (logs) during operation of such systems[12]. By leveraging blockchain for data integrity, AI systems can maintain a reliable and verifiable record of training data used - indeed, as discussed, consideration would need to be given with respect to the type of blockchain used (public/permissioned/hybrid) and the extent to what data is stored on the blockchain (e.g. raw data on-chain, or cryptographic hashes on-chain with off-chain raw data, or some other suitable configuration). To further emphasise the point, blockchains can facilitate data provenance, date and time of recording and other characteristics. This can also enable transparency and trust in data sources and provide a means to verify that AI models are trained on accurate and untampered data. As discussed, indeed, the characteristics of blockchain technology align with several requirements outlined in the AI Act, specifically in relation to data and data governance, record-keeping, transparency, and the provision of information to users.

It is important to note that while blockchains ensure data integrity and immutability, they do not guarantee the quality or accuracy of the data itself. Blockchain technology can provide assurances that the data has not been tampered with, but it does not address the issue of data bias, incompleteness, or representativeness. Ensuring the quality and reliability of the data used for training AI systems remains a separate challenge that requires additional research.

6.4.2 Data Sharing

According to the AI Act: *"European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high quality data for the training, validation and testing of AI systems."*.[13] Moreover, the AI ACT maintains that in order to facilitate the development of high-risk AI systems, specific actors, including digital innovation hubs, testing experimentation facilities, researchers, experts etc. should have access to and utilise high-quality datasets within their relevant fields

still possible, although attacks that try to amend block input (51% attack) can be detected, hence alarming relevant parties if needed.

[12] See Article 12 of the AI Act

[13] See paragraph 45 of the AI Act

of activities, as per the guidelines set by this Regulation. In relation, secure data sharing and storing can become critical concerns when it comes to collaborative AI training systems involving multiple parties.

Blockchain technology can provide solutions that enable secure data sharing among parties, facilitating collaboration while maintaining data privacy to a certain extent. Although still developing, the field of privacy preserving blockchain solutions is on the rise. In [262], the authors discuss novel privacy-preserving solutions for blockchains, where users can remain anonymous and take control of their personal data following a Self-Sovereign Identity (SSI) model. Moreover, Dusk network leverages zero-knowledge technologies to allow for transactions on the blockchain to benefit from confidentiality [263]. In other words, the network acts like a public record with smart contracts that store relevant information in a confidential fashion, thus solving the shortcomings of similar platforms, such as Ethereum. Furthermore, [264] build a publicly verifiable and secrecy preserving blockchain based auction protocol to address privacy concerns.

Blockchain along with secure multiparty computation (MPC) techniques can be used to allow multiple entities to collectively train AI models while keeping their individual data private whilst at the same time providing guarantees with respect to future verifiability of the data such models were trained on. MPC enables computation on encrypted data, ensuring that no participant gains access to another party's sensitive information [265, 266]. In this case, the blockchain serves as a trusted intermediary that orchestrates the computation and provides guarantees in respect to the integrity of the training process.

Likewise, through the use of smart contracts, the rules and protocols for data sharing and collaborative training can be defined and enforced on the blockchain [267]. Smart contracts could be used to specify the conditions under which data can be accessed, processed, and shared among the participating entities - yet it is important to note that control to accessing such data needs to be handled by a centralised component (since all data on a public blockchain is publicly available). This can help ensure that data sharing occurs in a controlled and auditable manner, promoting transparency and trust among participants. By leveraging blockchain for auditable data sharing, participants can retain ownership and more control over their data (stored off-chain) while still able to benefit from collective intelligence and insight gained through collaborative AI training.

IPFS (InterPlanetary File System) is a distributed file system that provides a decentralised approach to storing and sharing files across a network [268]. It enables secure and efficient content addressing, making data retrieval resilient to censorship and data corruption - in a public manner, i.e. all data is publicly available. IPFS uses content-addressable storage, which ensures that files are uniquely identified by their content rather than their location, thus enabling tamper-resistant data sharing - since any change in content would result in a different file address

(the address and the content are intimately linked).

Overall, decentralised data sharing aligns with the principles and objectives outlined in the AI Act by promoting transparency and accountability. The AI Act places importance on data protection and security. Decentralised data sharing can enhance data tamper-proofness by utilising cryptographic techniques, access controls, and distributed storage mechanisms. By distributing data across a network of nodes, decentralised systems reduce the risk of a single point of failure. Moreover, the AI Act emphasises the rights of individuals regarding their data and the necessity for obtaining explicit user consent. Decentralised data sharing aligns with these principles by giving users greater control over their data. Through decentralised technologies like blockchain, users can directly manage and grant access to their data, ensuring that their consent is obtained and that they have a say in how their data is used - yet the actual storage providers (whether centralised or decentralised) must still be trusted to release data only when such blockchain-based access control policies are followed.

Furthermore, the AI Act emphasises the ethical implications of AI systems, including fairness, accountability, and non-discrimination. Decentralised data sharing can support these ethical considerations by enabling collective decision-making, facilitating consensus, and transparent governance models [269]. These features promote fairness, accountability, and can help prevent discriminatory practices in data sharing and AI system development - since the actual development and learning processes become more open and democratised. Likewise, the AI Act promotes interoperability and data portability to foster competition and innovation. Decentralised data sharing can facilitate interoperability by enabling different AI systems to access and utilise data from various sources in a standardised and tamper-proof manner. It may also facilitate data portability, as users can easily share their data across different platforms or services without being locked into a specific provider's ecosystem - provided that standardised interfaces or means of connecting such different systems/data models are made available.

6.4.3 Auditing and Accountability

Auditing and accountability are crucial aspects in ensuring the responsible and ethical deployment of AI systems [270]. Today many AI systems are closed-source. Without access to the code and algorithmic details, it becomes impossible or infeasible to identify whether biases exist within models. Moreover, without access to source code, external entities such as experts, auditors, or regulatory bodies face challenges in conducting thorough audits or assessments of a system's fairness, bias, or potential vulnerabilities. Likewise, code alterations and data poisoning attacks might be harder to detect in closed systems.

The AI Act states the obligation for ex-ante testing, risk management and hu-

man oversight to minimise the risk of erroneous or biassed AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary[14]. The proposed regulation puts a high importance on both audit and transparency. For example, under Annex 7 the document states that: *"the body shall carry out periodic audits to make sure that the provider maintains and applies the quality management system and shall provide the provider with an audit report. In the context of those audits, the notified body may carry out additional tests of the AI systems for which an EU technical documentation assessment certificate was issued."*

The AI Act specifies that for high-risk AI systems, the design should prioritise sufficient transparency to enable users to interpret the system's output and utilise it appropriately. As noted, it is essential to establish an appropriate level and form of transparency to ensure compliance with respective obligations. In relation, ENISA acknowledges the existing techno-legal gap concerning transparency in AI systems and their importance for security. For example, it maintains that: *"The traceability and lineage of both data and AI components are not fully addressed. The traceability of processes is addressed by several standards related to quality. In that regard, ISO 9001 is the cornerstone of quality management. However, the traceability of data and AI components throughout their life cycles remains an issue that cuts across most threats and remains largely unaddressed."* The regulatory document emphasises that that documentation in itself is not a security requirement, and that for a security control, technical documentation is needed to ensure system transparency.

Blockchain technology offers unique features that can enhance both the transparency and auditability of AI systems, enabling stakeholders to hold them accountable for their actions. One of the key advantages of blockchain is its inherent transparency. By recording the entire lifecycle of an AI model on the blockchain (or proof of the lifecycle to minimise on-chain data), including the data sources used for training, the algorithms employed, and any subsequent updates or modifications, a verifiable trail is established. This comprehensive record enables auditors and regulators to trace the decision-making process of the AI system, ensuring that it adheres to ethical standards, legal requirements, and established guidelines. The transparency of blockchain-based audit trails can help identify potential biases in AI systems. Biases can arise from various sources, including biassed training data or discriminatory algorithmic design. With blockchain, relevant stakeholders including auditors can examine the inputs, processes, and outputs of an AI system and detect any potential biases or discriminatory patterns. This visibility fosters accountability and allows for necessary interventions to mitigate biases and ensure fair and equitable outcomes.

[14]See Section 3.5. under Fundamental rights of the AI Act.

Furthermore, blockchain's immutability ensures the integrity and tamper resistance of the audit trail. Once recorded on the blockchain, the information becomes practically unalterable, preventing unauthorised modifications or tampering. This feature ensures that the audit trail remains reliable and trustworthy, bolstering confidence in the accountability and transparency of AI systems. The use of blockchain technology also facilitates cross-organizational audits and accountability. Multiple stakeholders, including developers, data providers, regulators, and end-users, can access the blockchain-based audit trail and contribute to the auditing process. This collaborative approach enhances the effectiveness of audits, promotes shared responsibility, and strengthens the overall accountability framework surrounding AI systems. This is in line with the AI Act and can serve as an effective tool to enforce reliable and more effective audits. In addition, incorporating blockchain as a tool, could reduce the need of human oversight as noted by the Article 14 of the AI Act - since rules could be encoded into a blockchain system and smart contracts that guarantee a system's compliance.

Overall, by leveraging blockchain technology, AI systems can better enforce auditability requirements specified in the AI Act. The immutability, transparency, traceability, consensus mechanisms, smart contracts, and data security features of blockchain contribute to establishing a trustworthy and auditable framework for AI systems. This enables auditors to examine compliance, fairness, and accountability aspects of AI operations, promoting transparency and responsible AI development and deployment.

6.4.4 Identity and Access Management

As noted in section 2, identity and access management is a crucial aspect of ensuring the security of AI systems. Along the same lines, the AI Act specifies the need for access control policies[15] including a description of roles, groups, access rights, and procedures for granting and revoking access. Under Article 15, the AI Act aims to ensure that appropriate access control is established in high-risk AI systems to provide resilience against attempts by unauthorised parties to exploit the system. A more detailed description of access control is given under the Technical Guidelines for the implementation of minimum security measures for Digital Service Providers by ENISA [271]. The document also underlines the need of having a list of authorised users who can access certain security functions including keeping logs from privileged accounts' usage.

Blockchain technology presents an opportunity to enhance identity management and access control in a secure and decentralised manner. Traditional iden-

[15] Access control refers to the process of managing and regulating the permissions and privileges granted to specific users or entities interacting with an AI system.

tity management systems often rely on centralised authorities or intermediaries to verify and authenticate users. This centralised approach introduces vulnerabilities and single points of failure that can be exploited by malicious actors. In contrast, blockchain-based identity solutions, such as self-sovereign identity (SSI), offer a more secure and user-centered approach. With SSI, individuals have control over their personal information and digital identities. For example, a blockchain company Dock, utilises SSI technology to allow people to self-manage their digital identities without depending on third-party providers to store and manage the data [272]. The solution, however, still links the users with verifiers (e.g., employers, banks, universities, etc.) to attest the validity of a certain document (e.g., a student has graduated).

Blockchain enables the creation of unique, tamper resistant digital identities that are associated with cryptographic keys. These identities are stored on the blockchain and can be securely managed by the individual themselves[16]. This decentralised approach can eliminate some control that centralised identity providers currently have and reduces the risk of unauthorised access or data breaches. Moreover, in the context of AI systems, blockchain-based identity management can be leveraged to control access to AI models and data sources.

1. Users: Users can be selectively granted access permissions to specific AI models or datasets based on predefined rules and smart contracts. This allows for fine-grained access control, ensuring that only authorised individuals or entities can interact with the AI system. Users have the ability to maintain control over their personal data and can choose to disclose only the necessary information to the AI system. This reduces the reliance on third-party data custodians and minimises the exposure of sensitive personal data. Furthermore, the immutability and transparency of blockchain records provide a trustworthy audit trail of identity-related activities. Any changes or updates to identities, access permissions, or transactions can be recorded on the blockchain, enabling accountability and traceability. This can be particularly important in regulated environments or scenarios where compliance with data protection regulations is necessary.

2. Developers: Access control can also refer to the permissions and privileges granted to specific entities (e.g., developers) interacting with an AI system. It aims to protect extraction of sensitive data, prevent unauthorised access & code modification, and maintain the integrity and confidentiality of the system. In the context of AI and cybersecurity, access control involves implementing robust authentication and authorization mechanisms, establish-

[16]The potential drawback to this system is that a user can lose its key and may not be able to recuperate his access.

ing fine-grained access policies, and enforcing secure roles and privileges. Specific parameters can be incorporated to restrict access to critical systems by leveraging the capabilities of tamper-proof decentralised infrastructure such as blockchains, smart contracts, and oracles. Organisations can define access restrictions and conditions by associating private keys with specific actions or permissions within the AI system. For example, certain critical system operations or sensitive data access can be tied to specific private keys. The blockchain serves as the decentralised infrastructure that securely stores and manages these private keys. Private keys can be securely stored in digital wallets or key management systems, with access controls and encryption mechanisms to prevent unauthorised use or tampering. The blockchain will also record the ownership and transactions related to these private keys, ensuring transparency and accountability, further reinforcing the AI Act standards on transparency.

6.5 Technology: A complementary tool to achieve legal compliance

In general, the EU position has been in line with implementing 'Security-by-Design' mechanisms as a way to improve the overall cybersecurity of digital systems. Security-by-design is a concept in software engineering and product design that takes security considerations into account at the early stages of product development (ex-ante). This includes considering security risks and vulnerabilities at every stage of development, from architecture and design to implementation, deployment and testing [273].

One of the unique aspects of implementing blockchain for AI is that this technology allows for the introduction of both ex-ante and ex-post measures that can reinforce the overall cyber security of the system. In regard to our example on high-risk AI systems, by storing information on a decentralised and tamper-resistant blockchain, it becomes possible to establish a verifiable and auditable history of an AI system's development and behaviour. Overall, the idea behind verifiable and immutable time-stamps allows for ex-post regulatory measures such as auditing procedures. On the other hand, as an ex-ante measure, designing a smart contract based 'Access Control' system would require a predetermined set of characteristics to be transposed on-chain.

Furthermore, in [58] the authors maintain that for a proper enforcement of cyber measures (in accordance with the AI Act), there is a need for establishment of AI system architecture that would involve the creation of specific entities (namely: Entity for Record Keeping, Entity for Risk Mitigation, Entity for AI Processing,

Entity for AI verification, etc.). The authors argue that the 'Entity for Record Keeping' is needed to be in charge of registering and administering the 'loggings' of user interactions and their connection with data, storage and other parts of the system. Similarly, this entity would be in charge of assuring that data was not modified or altered in any way. As suggested, the 'AI System Management Entity' would be in charge of managing the interaction between the different entities, detecting any possible issues or undesired behaviour.

While we don't argue against the relevance of establishing suitable regulatory entities in order to reinforce certain measures in the AI Act, we argue that blockchain can serve as a useful tool to a) reinforce the effectiveness of a given entity's tasks and b) establish a governance mechanism for decision making between entities. For example, in both of the situations above, blockchain can be of help as it can provide a reliable and verifiable record of the data, detecting any possible alteration. Via this tool the 'Entity for Record Keeping' can have trusted information on the data provenance, usage, date and time, etc. In the second case, blockchain can serve as a useful governance mechanism between different entities. In other words, blockchain allows for robust governance by providing a distributed network where multiple entities participate in a consensus allowing for more transparent processes in decisions making. For example, if a malicious behaviour such as data poisoning by an unauthorised party is registered by one supervisory entity, the system can signal to others entities to apply further verification. Similarly, this reduces the 'single point' risk when one entity might be hacked/inaccessible. Likewise, via the usage of smart contracts the decisions of all entities would be accounted for and automated within the AI system architecture.

6.6 Limitations

It is important to note that while blockchain technology offers several advantages, it may not be a suitable solution for all AI-related cyber risks. The implementation of blockchain in AI systems requires careful consideration of factors like scalability, performance, and the specific requirements of the application. Additionally, blockchain technology itself is not immune to all cybersecurity threats and cyber vulnerabilities as we discussed in details in Chapters 2, 3, 4 and 5, and proper measures should be taken to secure the underlying infrastructure and smart contracts associated with the blockchain implementation.

6.7 Conclusion

In this chapter, we argue that blockchain technology offers unique set of properties that can be harnessed to establish transparency, security and enhanced verification in AI systems. As the European Union's regulatory focus intensifies on cybersecurity challenges related to AI, in tandem with the AI Act proposal, our objective is to illustrate how blockchain holds the potential to alleviate specific cybersecurity vulnerabilities associated with AI systems. We maintain that the incorporation of blockchain technology can enable specific AI-based systems to align with various provisions delineated in the AI Act. This alignment particularly pertains to aspects such as data, data governance, record-keeping, transparency assurance, and access control enforcement. We show how the decentralised and tamper resistant attributes of blockchain offer solutions to fulfil these requisites, serving as a promising basis for establishing more secure AI systems. The chapter also explores how blockchain can successfully address certain attack vectors related to AI systems, such as data poisoning in trained AI models and data sets.The overall goal of this analysis is to contribute to the progress of more secure AI implementations, not only within the EU but also globally. We seek to bridge the divide between legal and technical research by providing an interdisciplinary perspective of cybersecurity in the AI domain, and the applicability of blockchain based affordances in mitigating certain risks.

Chapter 7

BLOCKCHAIN FOR REC: ENHANCING PRIVACY AND INCENTIVES IN ENERGY TRADING

This chapter is based on the article: Ramos, S., & McMenamin, C. (2023). "Privacy-Preserving Energy Trading with Applications to Renewable Energy Communities." *8th International Conference on Renewable Energy and Conservation (ICREC)*

7.1 Introduction

Renewable energy communities (RECs) encounter a spectrum of challenges that span across technological, socio-economic, and regulatory dimensions. Their functionality is restricted by the availability of primary resources, such as solar and wind power. Moreover, these sources tend to exhibit variable renewable energy production, characterized by stochastic patterns [274]. Technical solutions such as advanced energy storage technologies (e.g. batteries) often involve high costs associated with implementing, maintaining, and depreciating such technologies. As noted by MIT Technology Review [275], fluctuating solar and wind power require lots of energy storage, and while lithium-ion batteries seem like the obvious choice they are far too expensive to play a major role [54]. In addition, the lithium industry for battery production has been highly criticized due to the exploitation of natural resources, over-usage of drinkable water in arid areas and irreversibly damaging the environment and communities in the exploited areas [276].

A successful REC hinges on active member involvement in consumption and

production, along with coordination and incentive alignment among participants. In addition, the socio-economic challenges in RECs often extend to achieving equitable access to renewable energy among the community members where participants benefit across diverse demographic and economic groups. A community owned production units and a collectively owned renewable energy is often considered a common good, facing problems such as efficient allocation. In economics, **common goods** are traditionally defined as rivalrous and non (or hardly) excludable goods, however an extended definition by [277] explains a common good characterized by a resource, a community and a set of rules presiding over the governance of the resource. Common goods often face the 'Tragedy of the Commons' phenomena which explains a situation of a common good resource (e.g., a lake with fresh water) where individuals with access to it act in their own interest and, in doing so, ultimately deplete the resource and negatively affect themselves and the rest of the users (and the community) [278].

In a similar direction, RECs often face free-riding challenges such as over-consumption and/or under-provision of Renewable Energy (RE), underlining the well known 'Tragedy of the Commons' phenomena. Peer-to-peer (P2P) trading is often suggested as a solution to tackle challenges like free-riding where members individually own production units and trade surplus energy in a market based approach. However, there is a possibility that these mechanisms may disproportionately favor members with greater resources, potentially leading to an imbalance within the community and, consequently, impacting the socio-economic fabric of a REC [279, 280]. Likewise, while P2P trading offers opportunities for individuals to directly exchange energy, it also raises questions about data privacy and confidentiality which need to be effectively addressed, particularly in line with the ongoing regulatory requirements [281, 282]. Further to this, RECs typically find themselves with a need to monitor and verify sustainable practices to avoid 'greenwashing', and secure future funding, permits, and tax discounts [283]. On the regulatory side, the EU policy regarding Renewable Energy has evolved its approach where the EU Commission foresees RECs and prosumers as essential part of the clean energy transition [284]. The resent increment of energy prices has further elevated the need as well as the demand for alternative souses of energy, where REC have come to be seen as a potential alternative, especially in small and medium size communities. Nevertheless, the ability to verifying the validity of renewable actions and trust the progress towards higher sustainability has be noted as one of the important challenges amongst regulators [51]. Likewise, there have been ongoing efforts to establish the universal and harmonized provisions for monitoring, reporting, and verification (MRV) in climate change mitigation projects [52].

Therefore, there is a clear need for a comprehensive and adaptable strategy, integrating technological innovation, effective coordination mechanisms, robust

member data protection, and a reliable verification tools. By amalgamating these elements, sustainable change can be effectively propelled forward. In this chapter, we present a blockchain-based solution that achieves all of these needs. Specifically, we propose a solution (see Section 7.4) that achieves the following four important objectives:

1. Allow for the coordination of all community members, and increase the overall welfare of the community vs. individually rational strategies. We provide members with an incentive compatible mechanism[1] to trade energy in a single shared community marketplace before trading with the public energy grid. This ensures members both maximize community usage of renewable energy, and retain of wealth within the community.

2. Enable privacy-preserving expression of supply and demand by default.

3. Generate and monitor green blockchain-based tokens which enable alignment of community goals with individual incentives and provide a monetizable medium with which we can ensure members follow our community welfare-optimizing protocol (see Sections 7.3.1 and 7.5).

4. Enable relevant external parties (e.g., governments, organizations, municipality) to verify the sustainable behavior and progress of RECs/REC members (which can be often times crucial for granting funding, allowing to occupy land, reducing taxes, etc).

7.2 Related Work

7.2.1 On RECs

According to the definition of the EU Directive 2018/2001, a Renewable Energy Community (REC) is a entity which is based on open and voluntary participation, where the primary purpose is to provide environmental, economic or social community benefits for its shareholders, members and the local areas where it operates, rather than solely maximizing financial profits [284, 285]. According to Article 22 of RED II, an REC is a community in which consumers can produce, consume, distribute, and trade renewable energy, and in which every member must be able to access and acquire renewable assets co-ownership. REC typically belong to a spatially bounded locality, such as neighborhood, village, town,

[1] through our use of green tokens coupled with pricing which is, at worst, the same price achieved by trading directly with the public energy grid

or municipality, although with a suitable planning these communities can expand gradually.

The definition of REC can vary depending on a particular taxonomy and country. For example, [286] introduced RECs as a special type of grassroots initiative that produce or invest in the production of renewable energy to cover their own energy needs. In [287], the authors argued that energy sustainable communities should be defined according to their involvement in the process of energy sustainability. In her thesis, the author gives a more complete definition of clean energy communities as *"social and organizational structures formed to achieve specific goals of its members primarily in the cleaner energy production, consumption, supply, and distribution, although this may also extend to water, waste, transportation, and other local resources"* [280]. Focusing on the Australian market, she distinguishes between different categories of clean energy communities based on their supply structure of Renewable energy (RE) such as Virtual Power Plans, Peer-to-Peer Trading, Microgrids, and Integrated Community Energy Systems.

This chapter does not aim to add on to the definition of RECs, nether to provide a comprehensive overview of all types of RECs, as this is a complex and extensive topic that warrants volumes of literature. Likewise, recognizing the inherent diversity within RECs, each marked by a unique organizational framework and specific challenges, this chapter's objective is not to offer an all-encompassing remedy for RECs. Rather, our focus centers on a targeted range of issues. For these, we intend to present viable solutions that can be refined and broadened to encompass a wider array of use case scenarios. Throughout the chapter, we employ the example of Culatra to elucidate and enhance reader comprehension. Culatra is a local renewable energy community at Culatra Island, located in the south of Portugal [54]. RECs such as Culatra, represent a promising approach to energy infrastructure that aims to help address some of the present inequalities in energy provision for different regions and consumer types, and deliver considerable social, economic and environmental benefits to the community involved.

7.2.2 Blockchain and RECs

The adoption of a blockchain technology within RECs holds significant potential to enhance their operational framework, unlocking benefits that cannot exist in centralized and/or uncoordinated settings. Blockchain, characterized by its decentralized and transparent nature, offers a novel approach to addressing several critical challenges faced by RECs. An EU report maintains that blockchain can truly engage prosumers in the energy market acting as enabler for the creation of energy communities [288]. According to the study, blockchain enhances the transparency and trust of the energy market system.

In [289, 290, 291] the authors develop blockchain-based solutions for some of

the many challenges faced by RECs. The protocol in [289] leverages blockchain-based smart contracts to establish a P2P market for energy where local producers trade with local consumers, although overlooks the need to ensure user data remains private throughout the process. In [290], the authors propose a blockchain to enhance energy prices for demand-side management using demand response. The authors suggest the usage of pseudo-digital identity to enhance members' privacy. The authors however do not go into further details explaining the design, implementation and the management of these identities. Likewise, a recent review of blockchain-based energy trading platforms [291] identifies member privacy while also ensuring verifiability of the exchange process as an important open problem. This is something we solve in our protocol through our use of homomorphic encryption. The review also mentions compatibility for low-resource smart devices, and scalability as important issues for blockchain-based energy trading. Low-resource individuals in our protocol (Section 7.4) are only required to verify their own data has been encrypted and decrypted correctly, as long as any one member in the community verifies the settlement price for each time-slot has been performed correctly. Furthermore, as this verification is done locally (not computed using shared on-chain computation resources), this does not affect the scalability of the system.

Related to P2P trading as a means of increasing community welfare in microgrids, [292, 293, 294] all introduce variations of P2P energy marketplaces enabling the exchange of energy between consumers and prosumers, leaning on the ability for users to set their own pricing mechanism. Compared to these, our solution is intended to align more with the socio-economic fabric of REC. We incentivize members to engage in energy trading as a unified batch through our use of green tokens, providing a clear optimum both for members and the community over any free-market approach. This is as a result of batch trading on its own maximizing community welfare through its optimal pricing guarantees [295], with green tokens dominating any potential benefit of free-market trading for the individual members. This not only promotes a sense of community collaboration, but also optimizes the efficiency of energy distribution within the REC, reinforcing its sustainable and interconnected nature. In [296], the authors argue for the implementation of smart controllers which estimate the probability of energy use in the next hour, in order to predict occupancy patterns and assist with demand management. The authors leverage blockchain-based network for buildings to exchange data of a specific parameter called the probability of the next hour. We allow for such control systems too, generalizing to a notion of predictions based on historical data to any predictive mechanism, including the use of user-input information (not just extrapolations from historical data).

In terms of tokenomics, [293] design a blockchain-based asset ownership system allowing consumers to securely obtain energy production shares within a po-

tential REC in Germany. In [297], Rozas et al. 2020 suggest how blockchain-based affordances including tokenomics can theoretically be used to fulfill and automate Ostrom's principles, as a way towards avoiding the Tragedy of the Commons. A study by Cila et al. 2020 extend the debate arguing specific design dilemmas when creating a blockchain system, following a fictitious example of an energy community [298]. These demonstrate some of the ways in which tokenized assets can play a role in the context of RECs by facilitating the representation and exchange of value within the community ecosystem. In our protocol, we leverage this value-representation of token to incentivize the correct behaviour of individually rational members in the community towards optimizing the overall welfare of the community.

7.3 Designing an energy marketplace for RECs

Creating a fair energy marketplace for RECs presents a multifaceted challenge. Often the main focus of these communities revolves around fostering socio-economic and environmental well-being rather than pursuing a pure profit-maximization strategies [280]. As noted by [299], there is often a trade-off between economic and social performances in RECs which should be addressed ex-ante the implementation and design.

In this chapter, one of our key motivations is to uphold the community socio-economic fabric and motivating sustainable behaviors among its members, while providing a protocol towards maximizing the welfare of the community as a whole. The main challenge of any energy marketplace is the alignment of supply and demand. A free-market approach is a straightforward approach to solve this, although such an approach can be considered contrary to an REC's socio-economic fabric [300]. According to [301], dynamic pricing also requires sophisticated control technology and considerable implementation and operational costs, and has not proven highly successful in RECs. Moreover, this approach risks generating ethical concerns if prices surge due to demand surpassing supply, potentially burdening vulnerable community members.

In a microgrid environment such as Culatra, where the microgrid is connected to the main grid, the community is typically given a price p_s/MWh to sell excess energy to the main grid, while receiving some price p_b/MWh to buy energy from the main grid, with $p_b > p_s$. From a recent analysis on Culatra, $p_s \approx 40/MWh$ [54], while current estimates for the buy price set $p_b \approx 100/MWh$ [302] (these numbers are used as indicative example). By creating a blockchain-based settlement process for matching supply and demand imbalances, we can use blockchain tokens to incentivize desirable collaborative behaviour. One (simple) way we can use the tokens/non-monetary incentives to incentivize cooperative behaviour is:

- When supply exceeds demand, trade everything (sum of local net supply) at p_s, and give "green" tokens to the sellers which can be used to claim community discounts and/or satisfy grant delivery conditions.

- When demand exceeds supply, trade everything (net demand) at p_b, and give the same "green" tokens to the buyers, again creating a dominant incentive to take part in the community settlement process.

In order to incentivize the community to act cooperatively and not individually, as well as to improve the supply and demand matching, we suggest that participating community members can submit their net energy usage (energy usage minus energy creation) at some point before each time slot using a homomorphic encryption scheme (explained in Section 7.4). Then, the auctioneer, a semi-trusted third party in charge of matching supply and demand, aggregates the individual net usages for each time slot. This aggregation takes the form of a single number representing the community's net usage for the respective time slot, without revealing individual usages. This net usage is then communicated with external sources, either purchasing energy from the main grid in the case of net demand, or utilizing surplus energy to generate revenue by selling to the main grid (or alternative use-cases [303]) in the case of net supply.

7.3.1 Green Tokens and Specific Use Cases

The drive for demand, value, and usage of green tokens is specific to the REC in which the tokens are deployed, and typically depends on local conditions and needs. The following are examples of how demand can be created for the green tokens introduced:

a) In line with [297] argument for effective decentralized governance of common goods, tokens can be used in REC to define community membership and voting rights.

B) Tokens can be employed to provide local discounts on goods and services, encouraging community members to patronize local businesses and contribute to the growth of the local economy. This localized incentive mechanism not only bolsters community cohesion but also reinforces the REC's commitment to enhancing local sustainability and resilience.

C) Green tokens can be used to satisfy national or international quotas for sustainable energy usage. By tying grants, such as land permits for occupying natural reserve land [304], to tangible assets, there is a clear value proposition for such tokens. This is in line with regulatory efforts to establish the universal and harmonized provisions for monitoring, reporting, and verification in climate change mitigation projects [52].

7.4 Protocol Description

This section outlines the blockchain protocol intended for a deployment in a potential REC community. In this section we first outline the model assumptions, and cryptographic primitives that are required for use in our protocol. We then merge these with the necessary blockchain functionalities, describing the entire protocol, as implemented here [305].

At a high-level, our protocol implements a publicly verifiable and privacy-preserving supply-demand matching protocol. Participating community members submit their net energy usages (energy usage minus energy creation) at some point before each time slot using a homomorphic encryption scheme. The auctioneer, a special semi-trusted entity in the community in charge of matching supply and demand, aggregates the individual net usages for each time slot, outputting the community's overall supply or demand for the respective time slot, without revealing individual usages. An accurate prediction of energy demand within a microgrid can be crucial for ensuring an appropriate balance between supply and consumption [280]. Incentivizing members to report accurate energy forecasts can be used to secure better pricing in advance of such spikes, in the same way that energy producers trade futures on energy prices to minimize variance in profits. Important usage information that is typically known in advance could take the form of holiday plans for community members (reduced energy usage) versus increased demand for community hotels (increased energy usage). This, in conjunction with the ability to report these profiles in a privacy preserving manner, has clear potential for an REC.

The net community usage is then communicated with external sources, either purchasing energy in the case of net demand, or utilizing surplus energy to generate revenue (selling to the grid, or alternative use-cases like Bitcoin mining [303]) in the case of net supply. Through our choice of encryption scheme, the individual contributions to the net supply/demand can be communicated and recorded publicly without any individual's information leakage. This is done in a way that only requires the encrypted total for each community member at each time slot to be stored. All of this, while ensuring each encrypted total is valid with respect to the community total.

With a public record of community renewable energy usage at each time slot, and encrypted summary statistics for each individual, these individuals can verify to local, national, or international entities that certain quotas are being met. If individuals are responsible for such proofs, these same individuals can be sure that sensitive information leaked by granular energy usage statistics is avoided.

7.4.1 Model Assumptions

1. A public-key infrastructure exists such that for any public key, and a message encrypted using that public key, only the owner of the private key corresponding to the private key can decrypt the message.

2. There exists an auctioneer in our system who is trusted to keep his own private key and decrypted plain-text messages private.

Importantly, our model does not require any trust that the auctioneer performs the settlement process correctly. Through our choice of homomorphic encryption system, every member in the system can verify that the auctioneer is settling the auction correctly, and neither creates nor destroys wealth within the community.

7.4.2 Homomorphic Encryption Scheme

For the purposes of our protocol, we require an encryption scheme which for encrypted usages $e(u_i)$ of each member $i \in [1, ..., n]$, we can verify that for some value v, $v = \sum_{i=1}^{n} u_i$ without revealing any of the u_is. The Paillier encryption scheme is such a protocol [306]. For full details on the system, and requirements for key generation see [307]. A Paillier private key can be described by a tuple (n, g, λ, μ), with corresponding public key (n, g). The encryption function e for $m \in [1, ..., n-1]$ the plaintext is described as:

$$e : m, r \rightarrow r^n g^m \textbf{ mod } n^2, \tag{7.1}$$

for a random nonce r with r, n co-prime. The decryption function d for a ciphertext c is:

$$d : c \rightarrow \lfloor \frac{c^\lambda \textbf{ mod } n^2}{n} \rfloor \cdot \mu \textbf{ mod } n. \tag{7.2}$$

For $c = e(m, r)$, $d()$ is such that $d(e(m, r)) = m$. Importantly for our purposes, the Paillier encryption also has the following homomorphic property:

$$d(e(u_1).e(u_2)) = d(e(u_1)) + d(e(u_2)) = u_1 + u_2. \tag{7.3}$$

In our system, each member i will post the tuple $(c_{i,r}, c_{i,m})$, an encryption of r_i and u_i respectively, to the blockchain using the auctioneer's public key (n_a, g_a). Let these ciphertexts be $c_{i,r} = e(r_i, R_i)$ for some randomly chosen R_i, and $c_{i,m} = e(u_i, r_i)$, using the same r_i in both ciphertexts. This allows the auctioneer exclusively to decrypt each of the plaintexts and corresponding nonce (u_i, r_i). By having the auctioneer post $r = \prod_{i=1}^{n} r_i$ and $v = \sum_{i=1}^{n} u_i$, anyone can then verify that the sum is correct by checking $e(v, r) = \prod_{i=1}^{n} c_{i,m}$. [2]

[2] In order to compute $r = \prod_{i=1}^{n} r_i$, necessary for verification that a proposed v is indeed the sum of the individual plaintexts, these nonces must be encrypted separately. This is because decryption of a plaintext does not reveal the nonce used in encryption.

7.4.3 Blockchain Protocol

Given these premises, we are equipped to implement our blockchain protocol. Each community member is represented by an address, with the set of addresses controlled by a public-key infrastructure. The blockchain protocol progresses in real-time. Unless otherwise specified, $e_i()$/$d_i()$ indicate Paillier encryption-decryption with member i's public-private key, while $e_a()$/$d_a()$ indicates Paillier encryption-decryption with the auctioneer's public-private key. Algorithm 1 describes the functions and data structures which are executed and stored on the blockchain. The protocol proceeds in sequential time slots, with each time slot requiring the following three steps:

1. **UPLOAD_ENC_USAGE()**: To be called by each member in the community for each time slot. The member decides on their net usage for the time slot u, some randomness r with which to encrypt that usage, and another randomness r' with which to encrypt the randomness r. These encryptions are done using the auctioneers public key, meaning only the auctioneer can decrypt the plaintext values. The encryption of r using r' allows the auctioneer to decrypt r, and as such compute the product of the nonce used to encrypt the usages. This product, along with the sum of the usages allows any blockchain observer to verify that the encryptions and decryptions were all done correctly. Through calling **UPLOAD_ENC_USAGE()**, the member uploads the encryptions of u using r, and r using r', which are then stored on the blockchain in `enc_Usages` and `enc_Rands` respectively. These values are to be used later by the auctioneer, and then by anyone wishing to verify the outcome of a particular auction.

2. **UPLOAD_DEC_USAGE()**: To be called by the auctioneer. After all members have called **UPLOAD_ENC_USAGE()** for a particular time slot, this blockchain function reveals the sum of the member usages for that time slot. Moreover, this function also reveals the product of the randomnesses used to encrypt each of these individual usages. For encrypted member usages $c_u^1, ..., c_u^n$ for a given time slot, with v the proposed net usage for the time slot, and r the proposed product of the randomnesses used, any blockchain member can verify that $\prod_{i=1}^{n} c_u^i = e_a(v, r)$. This ensures the decryption was done correctly.

3. **UPDATE_USER_TOKENS()**: To be called by the auctioneer to update the encrypted representation of a members total tokens within the blockchain system, stored in `enc_tokens`. Each member can verify that their own encryption has been performed correctly, while also verifying that the sum of the encryptions matches the implied total from the decrypted total usage

for the given time slot. As the encrypted token updates are done using $e_a()$, the blockchain performs a `require()` check before updating the token balances to ensure the token updates correspond to the net usage for that slot. Specifically, in line 14 the blockchain function checks that the decrypted net usage for the specified slot, `dec_Net_Usage[`$slot$`]`, times the price $price$, when encrypted with the specified randomness product $prod$ equals the product of the individual token updates, $\prod_{t \in T} t$. By the homomorphic property of the encryption scheme, this only holds true if the the token updates equal the net usage multiplied by the specified energy price. Assuming each member verifies their own token update is done correctly, a reasonable assumption given members are token maximizing, the community as a whole can be confident that all token updates are performed correctly.

Algorithm 1 Blockchain Protocol

```
1: mapping() enc_Usages
2: mapping() enc_Rands
3: mapping() dec_Net_Usage
4: mapping() dec_Rands_Product
5: mapping() enc_Tokens
6: mapping() enc_Token_Rands
7: function UPLOAD_ENC_USAGE (i=USER NUMBER, c_u=ENCRYPTED USAGE, c_r=ENCRYPTED
   RANDOMNESS, slot=TIME SLOT)
8:     enc_Usages[slot][i]=c_r
9:     enc_Usages[slot][i]=c_u
10: function UPLOAD_DEC_USAGE (v=TOTAL NET USAGE, r=RANDOMNESS PRODUCT USED, slot=TIME
    SLOT)
11:     dec_Net_Usage[slot]=v
12:     dec_Rands_Product[slot]=r
13: function UPDATE_USER_TOKENS (T=TOKEN UPDATES, R=ENCRYPTED RANDOMNESSES USED,
    slot=TIME SLOT, prod=PRODUCT OF RANDOMNESS, price= ENERGY PRICE USED)
14:     require(∏_{t∈T} t=e_a(price* dec_Net_Usage[slot], prod))
15:     for i ∈ [1, num_user] do
16:         enc_tokens_randomness[slot][i]=R[i]
17:         enc_tokens[i]=enc_tokens[i]*T[i]
```

7.5 Tokens and Value Exchange within an REC

This section introduces possible uses for such a green token (Section 7.3.1), mirroring the notion of carbon credits. We also describe how this notion can be enhanced by using the same privacy-preserving and verifiable functionalities of Section 7.4 to describe a marketplace for members to buy and sell these tokens without leaking sensitive information such as balances and trade history (Section 7.5).

The protocol described in Section 7.4 allows members to securely express supply and demand without revealing these preferences to other members. This supply and demand is converted into continuously updated and verifiable homomorphically encrypted financial balances for each member. The intention with such balances is to, at a minimum, track the amount owed to or by each community member. This core protocol implicitly records each individual's participation rates, self-sufficiency ratio, and self-consumption ratio. All of these variables can be explicitly recorded (in a privacy-preserving way if necessary), and merged to translate our high-level proposal of green tokens into a more tangible value proposition as described in Section 7.3.1.

Regardless of the exact use-case for the green tokens, there are many uses which create utility for users which can be translated to monetary value. To motivate the value proposition of these tokens, consider the use of green tokens for use in community improvement proposals and voting. In renewable energy communities such as Culatra, there are numerous shared costs related to infrastructure and development which must be prioritized. Green tokens received for participation in our proposed welfare-maximizing protocol of Section 7.4 are ideal for this purpose. Green tokens in such a system should then be distributed proportionally to volume traded, although in-line with the democratic needs of the community. Specifically, it is likely important to prevent monopolization of green tokens, so users may need to be pro-rated based on their expected volume/usage, while still incentivizing maximal volume to trade within the community protocol. Tokens can then be destroyed (anonymously, again using the same techniques as introduced in Section 7.4.2), and exchanged for votes. With competing utilities for one vote over another from each member's perspective [3], tokens now have a monetizable value with users having clear motivation to buy and sell. Specifically, members can express the value of such a green token vote in monetary terms.

To allow for the exchange of such tokens, consider a community progressing through time with members accruing various quantities of these green tokens while votes are periodically taking place. As discussed, there will be a natural desire for members to exchange tokens. With a blockchain technology, there are many ways to implement such an exchange in a decentralized manner [308, 309, 310]. These protocols match buyers with sellers, implementing variations of a frequent batch auction [295]. Batch auctions involving a trusted auctioneer and encrypted order information, as in [308, 309], are proven to settle orders at a price representative of the true underlying supply and demand. As the blockchain members can observe all of the auction inputs and outputs, we

[3] Members living away from a set of proposed development sites for new wind turbines may be indifferent to the development location compared to members closer to some sites than others due to noise pollution

can again leverage homomorphic encryption to ensure the auction is settled correctly. This stands as another example of blockchain-based techniques which can enhance these renewable energy communities.

7.6 Conclusion

In this chapter, we presented a blockchain based framework that not only enhances the coordination, privacy, and alignment of incentives within RECs but also empowers them to establish a trustworthy reputation in the eyes of relevant external stakeholders. In particular, we introduce a privacy-preserving energy trading protocol which enables REC members to securely communicate their energy supply and demand. Coupled with our use of tokenized incentives, users are encouraged to publish usage profiles and trade energy in a community-controlled public forum. This allows all users in the community to benefit from typically cheaper locally-produced renewable energy, while also allowing the community as a whole to more effectively to balance energy supply and demand. All of this is provided without compromising the confidentiality of sensitive data of REC members. Through these advancements, our blockchain-based protocol contributes to the advancement of sustainable energy adoption at the community level and paves the way for broader societal and environmental benefits.

Bibliography

[1] Gutierrez C. Blockchain Security: Choosing a Platform Is Only the First Step; 2017. Available from: https://www.altoros.com/blog/blockchain-security-choosing-a-platform-is-only-the-first-step/.

[2] Bank of France. Decentralised or Disintermediated Finance: What Regulatory Response? 2023;.

[3] Regnath E, Stainhorst S. SmaCoNat: Smart Contract in Natural Language. 2018;.

[4] Mindell R. Short History of Ledgers. Modern Treasury. 2022;.

[5] Kanade V. What Is ARPANET? Definition, Features, and Importance; 2023. Blog post. Available from: https://www.spiceworks.com/tech/networking/articles/what-is-arpanet/.

[6] Merino M. Que fue de Napster, la aplicacion P2P que cambio la industria musical en el 2000 (y con la que medio mundo descubrio el MP3); 2022. Available from: https://www.genbeta.com/a-fondo/que-fue-napster-aplicacion-p2p-que-cambio-industria-musical-2000-que-medio-mundo-descubrio-mp3.

[7] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2009;.

[8] Reijers W, Wuisman I, Mannan M, Filippi PD. Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies. Innovation Finance Accounting eJournal. 2018;.

[9] Dinh TTA, Wang J, Chen G, Liu R, Ooi BC, Tan KL. BLOCKBENCH: A Framework for Analyzing Private Blockchains. SIGMOD '17. New York, NY, USA: Association for Computing Machinery; 2017. p. 1085â1100. Available from: https://doi.org/10.1145/3035918.3064033.

[10] Vujicic D, JagodiÄ D, RandjiÄ S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In: 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH); 2018. p. 1–6.

[11] Lamport L, Shostak R, Pease M. In: The Byzantine Generals Problem. New York, NY, USA: Association for Computing Machinery; 2019. p. 203â226. Available from: https://doi.org/10.1145/3335772.3335936.

[12] Chatzigiannis P, Baldimtsi F, Griva I, Li J. Diversification Across Mining Pools: Optimal Mining Strategies under PoW; 2019.

[13] Zhang S, Lee JH. Analysis of the main consensus protocols of blockchain. Elsevier; 2019. Available from: https://www.sciencedirect.com/science/article/pii/S240595951930164X.

[14] Liu Z, Luong NC, Wang W, Niyato D, Wang P, Liang YC, et al. A survey on applications of game theory in blockchain. arXiv preprint arXiv:190210865. 2019;.

[15] Liu Z, Luong NC, Wang W, Niyato D, Wang P, Liang YC, et al. A Survey on Blockchain: A Game Theoretical Perspective. IEEE Access. 2019;7:47615–47643.

[16] Barreiro-Gomez J, Tembine H. Blockchain Token Economics: A Mean-Field-Type Game Perspective. IEEE Access. 2019;7:64603–64613.

[17] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets. European Commision; 2020. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC$_1 format = PDF$.

[18] Pavloff U, Amoussou-Guenou Y, Tucci-Piergiovanni S. Ethereum Proof-of-Stake under Scrutiny. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. SAC '23. New York, NY, USA: Association for Computing Machinery; 2023. p. 212â221. Available from: https://doi.org/10.1145/3555776.3577655.

[19] Ethereum. Proof of Stake (PoS); 2023. Document. Available from: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[20] Saad M, Spaulding J, Njilla L, Kamhoua CA, Shetty S, Nyang D, et al. Exploring the Attack Surface of Blockchain: A Systematic Overview. ArXiv. 2019;abs/1904.03487.

[21] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the Security and Performance of Proof of Work Blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. CCS â16. New York, NY, USA: Association for Computing Machinery; 2016. p. 3â16. Available from: https://doi.org/10.1145/2976749.2978341.

[22] Ramos S, Pianese F, Oliveras E, Leach T. A great disturbance in the crypto: Understanding cryptocurrency returns under attacks. Blockchain: Research and Applications. 2021;2(3):100021.

[23] Ramos S, Ellul J. The MEV Saga: Can Regulation Illuminate the Dark Forest? arXiv preprint arXiv:230503718. 2023;.

[24] Ethereum. Maximal Extractable Value (MEV); 2023. Available from: https://ethereum.org/en/developers/docs/mev/.

[25] Mevwatch; 2023. https://www.mevwatch.info/.

[26] Raphael A, Frost J, Vidal Pasto JM. Miners as intermediaries: extractable value and market manipulation in crypto and DeFi; 2022. Bank of International Settlements.

[27] EigenPhi Report;. https://eigenphi.io/.

[28] Ethereum. Introduction to Smart Contracts; 2023. Available from: https://ethereum.org/en/developers/docs/smart-contracts/.

[29] Wright A, De Filipi P. Decentralized Blockchain Technology and the rise of Lex Cryptographia. 2015;.

[30] Hewa T, Ylianttila M, Liyanage M. Survey on Blockchain-Based Smart Contracts: Applications, Opportunities, and Challenges. Journal of Network and Computer Applications. 2021 March;177:102857.

[31] Alharby M, Aldweesh A, Moorsel Av. Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research (2018). In: 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB); 2018. p. 1–6.

[32] Han J, Lee J, Li T. Dao governance. 2023;.

[33] Bug Affecting Ethereum Network Leads to Fork. Yahoo!;. Available from: https://finance.yahoo.com/news/bug-affecting-ethereum-network-leads-170500387.html.

[34] 300m in cryptocurrency' accidentally lost forever due to bug. Guardian News and Media; 2017. Available from: https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether.

[35] Missing Line in a Smart Contract Leads to $10M Hack; 2021. https://news.ycombinator.com/. YCombinatorNews.

[36] Huang Y, Bian Y, LiShow R, Shi P. Smart Contract Security: A Software Lifecycle Perspective. IEEE Access. 2019 October;.

[37] Fereira A. Regulating Smart Contracts: Legal revolution or simply evolution? Telecommunication Policy. 2021;.

[38] McMenamin C, Daza V, Fitzi M, O'Donoghue P. Fairtradex: A decentralised exchange preventing value extraction. 2022 November 11;p. 39–46. Available from: http://example.com/path/to/pdf.

[39] Beniiche A. A Study of Blockchain Oracles; 2020.

[40] Al-Breiki H, Rehman MHU, Salah K, Svetinovic D. Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. IEEE Access. 2020;8:85675–85685.

[41] Oracles by Ethereum;. Accessed on: [insert access date here]. Available from: https://ethereum.org/en/developers/docs/oracles/.

[42] Ghosemajumder S. You Canât Secure 100% of Your Data 100% of the Time. Harvard Business Review. 2017;.

[43] Li Y, Liu Q. A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments. Energy Reports. 2021;.

[44] Ramos S, Melon L, Ellul J. Exploring Blockchains Cyber Security Techno-Regulatory Gap. An Application to Crypto-Asset Regulation in the EU. In: Graduate Conference in Law and Technology, Sciences Po. vol. 10; 2022. .

[45] European Securities and Market Authority. Advice - Initial Coin Offerings and Crypto-Assets; 2019. Available from: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391$_c rypto_a dvice.pdf$.

[46] Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets 2020/2034(INL). Legislative Observatory. European Parliament; 2020. Available from: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2034

[47] Antonopoulos A; 2021. Harvard Law School Blockchain and FinTech Initiative Conference.

[48] Altschuler S. Should Centralized Exchange Regulations Apply to Cryptocurrency Protocols? Stanford Journal of Blockchain Law & Policy. 2022;.

[49] Ramos S, Mannan M. Watch the Gap: Making code more intelligible to users without sacrificing decentralization? In: IEEE 24th Conference on Business Informatics; Workshop towards Decentralized Governance Design. vol. 24; 2022. .

[50] Alanne K, Saari A. Distributed energy generation and sustainable development. Renewable and sustainable energy reviews. 2006;10(6):539–558.

[51] Reuters. EU watchdog to define 'greenwashing' as sustainable funds rocket; 2022.

[52] Singh N, Finnegan J, Levin K, Damassa T, Elsayed S, Mitra A, et al. Understanding Measurement, Reporting, and Verification of Climate Change Mitigation; 2016.

[53] Poux P, de Filippi P, Ramos S. Blockchains for the Governance of Common Goods. In: Proceedings of the 1st International Workshop on Distributed Infrastructure for Common Good; 2020. p. 7–12.

[54] Pacheco A, Monteiro J, Santos J, Sequeira C, Nunes J. Energy transition process and community engagement on geographic islands: The case of Culatra Island (Ria Formosa, Portugal). Renewable Energy. 2022;184:700–711.

[55] Rozas D, Tenorio-FornÃ©s A, DÃaz-Molina S, Hassan S. When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. SSRN Electronic Journal. 2018;Available from: https://www.ssrn.com/abstract=3272329.

[56] Shinde R, Patil S, Kotecha K, Ruikar K. Blockchain for Securing AI Applications and Open Innovations. Journal of Open Innovation: Technology, Market, and Complexity. 2021;7(3):189.

[57] Mamoshina P, Ojomoko L, Yanovich Y, Ostrovski A, Botezatu A, Prikhodko P, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget. 2017;9(5):5665–5690.

[58] Mueck MD, Elazari Bar On A, Du Boispean S. Upcoming European Regulations on Artificial Intelligence and Cybersecurity. 2023;.

[59] Ramos S, Ellul J. Blockchain for AI: Enhancing Compliance with the EU AI Act through Distributed Ledger Technology. A Cybersecurity Perspective. International Cybersecurity Law Review. 2023;.

[60] Borri N. Conditional tail-risk in cryptocurrency markets. Journal of Empirical Finance. 2019;50(C):1–19.

[61] Raymaekers W. Cryptocurrency Bitcoin: Disruption, challenges and opportunities; 2015. .

[62] Apostolaki M, Zohar A, Vanbever L. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. In: 2017 IEEE Symposium on Security and Privacy (SP); 2017. p. 375–392.

[63] Marella V, Upreti BR, Merikivi J. Understanding the Creation of Trust in Cryptocurrencies: Bitcoin. In: Bled eConference; 2019. .

[64] Zhang R, Preneel B. Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security. In: 2019 2019 IEEE Symposium on Security and Privacy (SP); 2019. p. 175–192. Available from: https://doi.ieeecomputersociety.org/10.1109/SP.2019.00086.

[65] Heilman E, Kendler A, Zohar A, Goldberg S. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In: 24th USENIX Security Symposium (USENIX Security 15). Washington, D.C.: USENIX Association; 2015. p. 129–144. Available from: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman.

[66] Bissias G, Levine BN, Ozisik AP, Andresen G. An Analysis of Attacks on Blockchain Consensus; 2016.

[67] Zhang SJ, Lee JH. Double-Spending With a Sybil Attack in the Bitcoin Decentralized Network. IEEE Transactions on Industrial Informatics. 2019;15:5715–5722.

[68] Jang J, no Lee H. Profitable Double-Spending Attacks. ArXiv. 2019;abs/1903.01711.

[69] Kroll JA, Davey IC, Felten EW. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries; 2013. .

[70] Chohan UW. The double spending problem and cryptocurrencies. Available at SSRN 3090174. 2017;.

[71] Lewenberg Y, Bachrach Y, Sompolinsky Y, Zohar A, Rosenschein JS. Bitcoin mining pools: A cooperative game theoretic analysis. In: Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems. Citeseer; 2015. p. 919–927.

[72] Bastiaan M. Preventing the 51-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin; 2015. .

[73] Eyal I, Sirer EG. Majority is Not Enough: Bitcoin Mining is Vulnerable. Commun ACM. 2018 Jun;61(7):95â102. Available from: https://doi.org/10.1145/3212998.

[74] Crypto51. PoW 51 Attack Cost; 2019. Available from: https://www.crypto51.app/.

[75] NiceHash. Leading Cryptocurrency Platform for Mining and Trading; 2019. Available from: https://www.nicehash.com/blog/post/nicehash-as-a-defence-against-51-attack.

[76] Islam N, Mantymaki M, Turunen M. Why do blockchains split? An actor-network perspective on Bitcoin splits. Technological Forecasting and Social Change. 2019;.

[77] DuPont Q. Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance. Routledge; 2019.

[78] Lin IC, Liao TC. A Survey of Blockchain Security Issues and Challenges. I J Network Security. 2017;19:653–659.

[79] Rajagopalan S. Blockchain and Buchanan: Code As Constitution; 2018. .

[80] Gandal N, Hamrick J, Moore T, Oberman T. Price manipulation in the Bitcoin ecosystem. Journal of Monetary Economics. 2018;95(C):86–96. Available from: https://EconPapers.repec.org/RePEc:eee:moneco:v:95:y:2018:i:c:p:86-96.

[81] Li T, Shin D, Wang B. Cryptocurrency Pump-and-Dump Schemes. SSRN Electronic Journal. 2018;.

[82] Huillet M. Ethereum Classic Cooperative Warns Public Against Apparent Hard Fork Scam. Cointelegraph; 2020. Available from: https://cointelegraph.com/news/ethereum-classic-cooperative-warns-public-against-apparent-hard-fork-scam.

[83] Young J. Bitcoin Platinum Created By South Korean Teenager As a Scam, Local Market Erupts. Cointelegraph; 2017. Available from: https://cointelegraph.com/news/bitcoin-platinum-created.

[84] Guri M. BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2018. p. 1308–1316.

[85] Peterson P. Event Studies: A Review of Issues and Methodology. Quarterly Journal of Business and Economics. 1989;28(3):36–66. Available from: http://www.jstor.org/stable/40472954.

[86] MacKinlay AC. Event Studies in Economics and Finance. Journal of Economic Literature. 1997;35(1):13–39. Available from: https://EconPapers.repec.org/RePEc:aea:jeclit:v:35:y:1997:i:1:p:13-39.

[87] Fama ea Eugene F. The Adjustment of Stock Prices to New Information. International Economic Review. 1969;10(1):1–21. Available from: https://EconPapers.repec.org/RePEc:ier:iecrev:v:10:y:1969:i:1:p:1-21.

[88] Yayla AA, Hu Q. The impact of information security events on the stock value of firms: the effect of contingency factors. Journal of Information Technology. 2011;26:60–77.

[89] Campbell K, Gordon LA, Loeb MP, Zhou L. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. 2003;.

[90] Tweneboah-Koduah S, Atsu F, Buchanan WJ. Impact of cyberattacks on stock performance: a comparative study. Inf Comput Secur. 2018;26:637–652.

[91] Telang R, Wattal S. Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - an Empirical Investigation. In: WEIS; 2005. .

[92] Cavusoglu H, Mishra BK, Raghunathan S. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce. 2004;9:104 – 70. Available from: https://api.semanticscholar.org/CorpusID:10753015.

[93] Uma M, Padmavathi G. A survey on various cyber attacks and their classification. Int J Netw Secur. 2013;15(5):390–396.

[94] Hung CC. Analysis of Information Security News Content and Abnormal Returns of Enterprises. Big Data and Cognitive Computing. 2019;3(2):24.

[95] Colivicchi I, Riccardo V, et al. Forecasting the impact of information security breaches on stock market returns and VaR backtest. Journal of Mathematical Finance. 2019;9:402–454.

[96] Carlsson C, Danielsson F, Svensson C. The effect of blockchain related corporate name changes on stock prices : An investigation into the creation of cumulative abnormal returns following a blockchain related corporate name change; 2018.

[97] Corbet S, Larkin C, Lucey B, Meegan A, Yarovaya L. Cryptocurrency reaction to FOMC announcements: Evidence of heterogeneity based on blockchain stack position. Journal of Financial Stability. 2020 February;46. Available from: https://eprints.soton.ac.uk/436932/.

[98] Shanaev S, Shuraeva A, Vasenin M, Kuznetsov M. Cryptocurrency Value and 51 Attacks: Evidence from Event Studies. SSRN Electronic Journal. 2018 01;.

[99] Abhishta A, Joosten R, Dragomiretskiy S, Nieuwenhuis LJ. Impact of successful ddos attacks on a major crypto-currency exchange. In: 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE; 2019. p. 379–384.

[100] Auer R, Claessens S. Cryptocurrency market reactions to regulatory news. C.E.P.R. Discussion Papers; 2020. 14602. Available from: https://ideas.repec.org/p/cpr/ceprdp/14602.html.

[101] Koutmos D. Return and volatility spillovers among cryptocurrencies. Economics Letters. 2018;173:122–127.

[102] Caporale GM, Kang WY, Spagnolo F, Spagnolo N. Cyber-attacks, spillovers and contagion in the cryptocurrency markets. Journal of International Financial Markets, Institutions and Money. 2021;74:101298.

[103] Bambrough B. Bitcoin Rival Suffers Devastating Attack. Forbes Magazine; 2020. Available from: https://www.forbes.com/sites/billybambrough/2020/01/28/bitcoin-rival-suffers-devastating-attack/.

[104] Civitarese J, Mendes L. Bad News, Technical Development and Cryptocurrencies Stability; 2018. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract$_id = 3154124$.

[105] Joo M, Nishikawa Y, Dandapani K. Announcement effects in the cryptocurrency market. Applied Economics. 2020 05;p. 1–15.

[106] Dyckman T, Philbrick D, Stephan J. A comparison of event study methodologies using daily stock returns: A simulation approach. Journal of accounting research. 1984;p. 1–30.

[107] Campbell JY, Lo AW, MacKinlay AC, Whitelaw RF. The econometrics of financial markets. Macroeconomic Dynamics. 1998;2(4):559–562.

[108] Brown SJ, Weinstein MI. Derived factors in event studies. Journal of Financial Economics. 1985;14(3):491–495. Available from: https://www.sciencedirect.com/science/article/pii/0304405X85900108.

[109] Brown SJ, Warner JB. Using daily stock returns: The case of event studies. Journal of financial economics. 1985;14(1):3–31.

[110] Brown SJ, Warner JB. Measuring security price performance. Journal of financial economics. 1980;8(3):205–258.

[111] Xu J, Livshits B. The Anatomy of a Cryptocurrency Pump-and-Dump Scheme. ArXiv. 2019;abs/1811.10109.

[112] Black C. Cryptocurrency Gold Rush on the Dark Web. Carbon Black, Inc.; 2018.

[113] Ellul J, Pace G, Revolidis I, Schneider G. When is good enough good enough? On software assurances. ERA Forum. 2023;23.

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

[115] Ellul J, Galea J, Ganado M, McCarthy S, Pace GJ. Regulating Blockchain, DLT and Smart Contracts: a technology regulatorâs perspective. ERA Forum. 2020;.

[116] Joint statement by the Council and the Commission on stablecoins. European Council; 2019. Available from: http://www.consilium.europa.eu/en/press/press-releases/2019/12/05/joint-statement-by-the-council-and-the-commission-on-stablecoins/.

[117] von der Leyen U. Mission letter. European Commision; 2019. Available from: https://ec.europa.eu/info/sites/default/files/mission-letter-valdis-dombrovskis-2019$_en.pdf$.

[118] 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;.

[119] 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. European Commision; 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595from=EN.

[120] Enria A. Regulating Crypto Finance: Taking Stock and Looking Ahead. Venice; 2023. Speech by Andrea Enria, Chair of the Supervisory Board of the ECB, at the Conference on MiCAR and its coordination with EU financial markets legislation, jointly organized by Ca' Foscari University of Venice and Banca d'Italia. Speech.

[121] du Surveillance de Secteur Financier C. DLT Pilot Regime; 2023.

[122] European Central Bank. Global and Local Drivers of Bitcoin Trading Vis-Ã -Vis Fiat Currencies. European Central Bank; 2023.

[123] Anonymous. Decentralized Finance Market Size, Share & Trends Analysis Report. Not specified. 2023;By Component (Blockchain Technology, Smart Contracts), By Application (Payments, Stablecoins), By Region, And Segment Forecasts, 2023 - 2030.

[124] Aydar M, Cetin SC, Ayvaz S, Aygun B. Private key encryption and recovery in blockchain. arXiv preprint arXiv:190704156. 2019;.

[125] Guri M. Beatcoin: Leaking private keys from air-gapped cryptocurrency wallets. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE; 2018. p. 1308–1316.

[126] Balaban D. Inside The World Of Crypto Exchange Hacks; 2023.

[127] Sharma R. Cryptocurrency Insurance Could Be a Big Industry in the Future. Investopedia; 2021. Available from: https://www.investopedia.com/news/cryptocurrency-insurance-could-be-big-industry-future/.

[128] Orcutt M. Once hailed as unhackable, blockchains are now getting hacked. MIT Technology Review; 2021. Available from: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

[129] Report on The Cost of Third-Party Cybersecurity Risk Management. Ponemon Institute LLC; 2019. Available from: https://cdn2.hubspot.net/hubfs/2378677/Content-Assets/CyberGRX%20Ponemon%20Report.pdf.

[130] Bambrough B. Bitcoin Rival Suffers Devastating Attack. Forbes Magazine; 2020. Available from: https://www.forbes.com/sites/billybambrough/2020/01/28/bitcoin-rival-suffers-devastating-attack/7a462dafcb73.

[131] Nesbitt M. Ethereum Classic (ETC) is currently being 51% attacked. The Coinbase Blog; 2019. Available from: https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de.

[132] Kok S, Abdullah A, Jhanjhi N, Supramaniam M. Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers. 2019;8(4):79.

[133] Choi M, Levy Y, Hovav A. The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In: Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP); 2013. .

[134] Legal And Regulatory Framework Of Blockchains And Smart Contracts. EU Blockchain Observatory Forum; 2019. Available from: https://www.eublockchainforum.eu/sites/default/files/reports/reportlegalv1.0.pdf.

[135] Haque R, Seira R, Plummer B, Rosario N. Blockchain Development and Fiduciary Duty. Raina S Haque et al, Blockchain Development and Fiduciary Duty. 2019;2.

[136] Pazaitis A, De Filippi P, Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. Technological Forecasting and Social Change. 2017;125:105–115.

[137] Chiu J, Koeppl T. Incentive compatibility on the blockchain. In: Social Design. Springer; 2019. p. 323–335.

[138] Nissenbaum H. Securing trust online: Wisdom or oxymoron. BUL Rev. 2001;81:635.

[139] Gambetta D. Can We Trust Trust? Diego Gambetta. 2000 08;.

[140] Schneier B. Liars and outliers: enabling the trust that society needs to thrive. John Wiley & Sons; 2012.

[141] Walch A. Call Blockchain Developers What They Are: Fiduciaries. American Banker, Aug. 2016;9.

[142] Ganado M, Ellul J, Pace GJ, Tendon S, Wilson B. Mapping the Future of Legal Personality. 2020;.

[143] Law PoPiETaWFUSo Raina S Haque, LLP AaC Rodrigo Seira Silva-Herzog, Law JDCaWFUSo Brent A Plummer, Law APaCKSo Nelson M Rosario. Blockchain Development and Fiduciary Duty. Stanford Journal of Blockchain Law & Policy. 2019 6;Https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty. Available from: https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty.

[144] FILIPPI PD. Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream. Cyberspace Law eJournal. 2019;.

[145] Eyal I, Sirer EG. Majority is Not Enough: Bitcoin Mining is Vulnerable. Commun ACM. 2018 Jun;61(7):95â102. Available from: https://doi.org/10.1145/3212998.

[146] Townsend M, Hillis B, Rooke H, Tan B. English court to decide extent of blockchain developersâ legal duties to users; 2022.

[147] Frommelt E. Liability Challenges in the Blockchain Ecosystem. Business Law Journal. 2021;.

[148] Nye Jr JS. Deterrence and dissuasion in cyberspace. International security. 2016;41(3):44–71.

[149] The Board of the International Organization of Securities Commissions. Policy Recommendations for Decentralized Finance (DeFi); 2023.

[150] Lin LX. Deconstructing Decentralized Exchanges. Stanford Journal of Blockchain Law Policy. 2019 jan 5;Https://stanford-jblp.pubpub.org/pub/deconstructing-dex.

[151] Altschuler S. Should Centralized Exchange Regulations Apply to Cryptocurrency Protocols? Stanford Journal of Blockchain Law & Policy. 2022;5(1):92–113.

[152] Coindesk. Decentralized Exchange Volumes Hit Record Above $50BinJanuary.2021;$.

[153] Pourpouneh M, Nielsen K, Ross O. Automated Market Makers. 2020;.

[154] Chen J, Wang Y, Zhou Y, Ding W, Tang Y, Wang X, et al. Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild. In: 2023 IEEE 8th European Symposium on Security and Privacy (EuroSP); 2023. p. 332–351.

[155] Yano M, Dai C, Masuda K, Kishimoto Y, editors. Blockchain and Crypto Currency. Springer; 2020. Available from: https://EconPapers.repec.org/RePEc:spr:ecliap:978-981-15-3376-1.

[156] Hansen P. The EU's new MiCA framework for crypto-assets - the one regulation to rule them all; 2023.

[157] The International Organization of Securities Commissions. Policy Recommendations for Decentralized Finance (DeFi) Consultation Report; 2023. Available from: www.iosco.org.

[158] Augustin N, Eckhardt A, de Jong AW. Understanding Decentralized Autonomous Organizations from the Inside. Electron Markets. 2023;33:38.

[159] Ltd EYG. How to navigate tax and legal complexity associated with DAOs. EY Global; 2023. Available from: https://www.ey.com/en$_gl/tax/how-to-navigate-tax-and-legal-complexity-associated-with-daos::text=There$

[160] CoinDesk. CoinDesk Turns 10: 2016 - How The DAO Hack Changed Ethereum and Crypto. CoinDesk; 2023. Available from: URL of the Report if available.

[161] Hellström E. Fair Voting System for Permissionless Decentralized Autonomous Organizations; 2022.

[162] CoinDesk. The Liability of DAOs and Their Founders Has Been Put to the Test in Court. CoinDesk; 2023. Available from: URL of the Report if available.

[163] Systems Auditors Guidelines. Malta Digital Innovation Authority;. Available from: https://mdia.gov.mt/sa-guidelines/.

[164] Malta Financial Service Authority; 2019. Available from: https://www.mfsa.mt/wp-content/uploads/2019/06/Cybersecurity-Guidance-Notes.pdf.

[165] Ganado M. Blockchain Versus the Law. 2019;Available from: https://ganado.com/wp-content/uploads/2019/11/Ganado.pdf.

[166] Mazzora B, Penna N. Constant Function Market Making, Social Welfare and Maximal Extractable Value; 2022.

[167] Sinclair S. Global securities regulator calls out MEV in DeFi, highlighting âunlawfulâ nature; 2023.

[168] The Board of the International Organization of Securities Commissions. Policy Recommendations for Decentralized Finance (DeFi) Consultation Report; 2023.

[169] Barczentewicz M. MEV on Ethereum: A Policy Analysis; 2023. International Center for Law and Economics.

[170] Barczentewicz M, Sarch AF, Vasan N. Battle of the Crypto Bots: Automated Transaction Copying in Decentralized Finance. University of Pennsylvania Journal of Business Law. 2023;26.

[171] Robinson M, Konstantopoulos G. Ethereum is a Dark Forest; 2020.

[172] Philip D, Steven G, Tyler K, Yunqi L. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges; 2019.

[173] Flashbots; 2023. https://boost.flashbots.net/.

[174] Sun X. This Is MEV; 2022. DEVCON BOGOTA.

[175] Markham J. Front-Running - Insider Trading Under the Commodity Exchange Act. Catholic University Law Review. 1989;.

[176] Jaffe J. Special Information and Insider Trading. The Journal of Business. 1974;.

[177] Final Rule: Selective Disclosure and Insider Trading; 1999. 17 CFR Parts 240, 243, and 249, Securities and Exchange Commission.

[178] del Pozzo A, Tucci-Piergiovanni S, Gurcan O. On the Bitcoin Limitations to Deliver Fairness to Users. In: 25th International Conference on Cooperative Information Systems (CoopIS 2017): On The Move Federated Conferences and Workshops 2017. Rhodos, Greece; 2017. Ffcea-01807032f.

[179] Lessig L. Code. Version 2.0 ed. New York: Basic Books; 2006. OCLC: ocm77638613.

[180] Heimbach L, Kiffer L, Torres CF, Wattenhofer R. Ethereum's Proposer-Builder Separation: Promises and Realities. 2023;.

[181] Cointelegraph; 2022. https://cointelegraph.com/news/ofac-compliant-blocks-on-ethereumhits-three-month-low-of-47.

[182] Metrika. Exploring the Impact of OFAC Compliance on MEV Relays: An Investigation. 2023;.

[183] University C. Columbia CryptoEconomics Workshop; 2022.

[184] Szabo N. Formalizing and securing relationships on public networks. First Monday. 1997;.

[185] De Filippi P, Mannan M, Reijers W. Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society. 2020 Aug;62:101284. Available from: http://www.sciencedirect.com/science/article/pii/S0160791X20303067.

[186] Luhmann N. Familiarity, Confidence and Trust: Problems and Alternatives. 2000;.

[187] Hyperledger; 2022. https://www.hyperledger.org/use/fabric.

[188] Tulsidias T. Smart contracts from a legal perspective. Facultad de Derecho, University of Alicante; 2018.

[189] Raskin M. The law and legality of smart contracts. 2017;.

[190] Neuburger J. Arizona Passes Groundbreaking Blockchain and Smart Contract Law â State Blockchain Laws on the Rise. New Media. 2017;.

[191] Nevada Passes Pro-blockchain Law; 2017. https://www.lexology.com/library/detail.aspx?g=829fb8ea-8299-44b0-9bcc-472f06ba22dd.

[192] Papantoniou A. Smart Contracts in the New Era of Contract Law. Digital Law Journal. 2018;.

[193] Woebbeking M. The Impact of Smart Contracts on Traditional Concepts of Contract Law. 2019;.

[194] Eisenberg M. The Limits of Cognition and the Limits of Contract. Stanford Law Review. 1995;.

[195] Schwartz A, Scott R. Contract Theory and the Limits of Contract Law. Columbia Law School. 2003;.

[196] Ferreira A. Regulating smart contracts: Legal revolution or simply evolution? Telecommunications Policy. 2021;45:102081.

[197] Schrepel T. Smart Contracts and the Digital Single Market Through the Lens of a âLaw + Technologyâ Approach. European Commission. 2021;.

[198] Ley 22/2007, de 11 de julio, sobre comercializacion a distancia de servicios financieros destinados a los consumidores; 2007. https://www.boe.es/buscar/act.php?id=BOE-A-2007-12905.

[199] Werbach K, Cornell N. Contracts ex machina. Duke LJ. 2017;.

[200] Lessig L. MIT lecture on Smart Contracts and Dapps; 2020. Interview.

[201] Stuart L. An Introduction to Smart Contracts and Their Potential and Inherent Limitations. 2018;.

[202] Grimmelmann J. Regulation by Software. 114 Yale LJ. 2005;.

[203] Christiaans R, Hulstijn R. Control Automation to Reduce Costs of Control. International Journal of Information System Modeling and Design. 2013;.

[204] Schrepel T. Collusion by blockchain and smart contracts. Harvard Journal of Law and Technology. 2019;33.

[205] De Graaf T. From old to new: From internet to smart contracts and from people to smart contracts. Computer Law & Security Review. 2019;.

[206] settlemint; 2022. https://www.settlemint.com/for-it-leaders.

[207] Simbachain; 2022. https://simbachain.com.

[208] openlaw; 2022. https://docs.openlaw.io.

[209] mywish; 2022. https://mywish.io.

[210] Clack C. Languages for Smart and Computable Contracts. Centre for Blockchain Technologies Department of Computer Science UCL. 2021;.

[211] Marlowe; 2022. https://docs.cardano.org/marlowe/learn-about-marlowe.

[212] De Filipi P. Blockchain Technology and Decentralized Governance: The Pitfalls of a Trustless Dream. 2020;.

[213] Schneier B. Schneier on Security; 2008. Blog post. Available from: https://www.schneier.com/blog/.

[214] Coghlan J. EU backs Data Act with clause to shut off smart contracts; 2023.

[215] Coindesk. EUâs Controversial Smart Contract Kill-Switch Rules Finalized by Negotiators. 2023;.

[216] De Filippi P, Mannan M, Reijers W. The alegality of blockchain technology. Policy and Society. 2022;.

[217] Shi X. Do Core Developers Owe Fiduciary Duty to Users of Blockchain Platforms?;.

[218] Roumpos D. Liability of the Smart Contract Developer: A Comparative Analysis in the Light of US and EU Law; 2020.

[219] Clack C, Bakshi V, Braine L. Smart Contract Templates: Foundations, design landscape and research directions. 2017;.

[220] oneNDA; 2022. https://onenda.com.

[221] Standardized Agreements, Bidding Documents and Guidance Manuals; 2021. https://ppp.worldbank.org/public-private-partnership/standardized-agreements-bidding-documents-and-guidance-manuals.

[222] Borgogno O. Smart Contracts as the (New) Power of the Powerless? The Stakes for Consumers. European Review of Private Law. 2018;.

[223] Hiriart Y, Martimort D, Pouyet J. The public management of risk: Separating ex ante and ex post monitors. 2009;.

[224] Shadab H. Smart Contracts. Coin Center. 2014;.

[225] Diver L. Digisprudence: the design of legitimate code. Law, Innovation & Technology. 2022;.

[226] Schneider N. Decentralization: an incomplete ambition. Journal of Cultural Economy. 2019;12.

[227] Erenkrantz J, Taylor R. Supporting Distributed and Decentralized Projects: Drawing Lessons from the Open Source Community;.

[228] European Commission's High-Level Expert Group on Artificial Intelligence. Definition of AI; 2018. Available from: https://ec.europa.eu/futurium/en/system/files/ged/aihlegdefinitionofai18december1.pdf.

[229] IDC Worldwide Semiannual Artificial Intelligence Tracker; 2022. https://www.idc.com/.

[230] Yampolskiy RV, Spellchecker MS. Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures. 2016;.

[231] Comiter M. Attacking Artificial Intelligence: AIâs Security Vulnerability and What Policymakers Can Do About It; 2019. Belfer Center for Science and International Affairs, Harvard Kennedy School.

[232] ENISA Research and Innovation Brief, Artificial Intelligence and Cybersecurity Research; 2023.

[233] EU's Cybersecurity Strategy for the Digital Decade;. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[234] Lohn A. Hacking AI: A Primer for Policymakers on Machine Learning Cybersecurity. 2020 December;.

[235] Ellul J. Should we regulate Artificial Intelligence or some uses of software? Discover Artificial Intelligence. 2022;2(1).

[236] Liang B, Li HC, Su MQ, et al. Detecting Adversarial Image Examples in Deep Networks with Adaptive Noise Reduction. 2017;Available from: https://arxiv.org/abs/1705.08378.

[237] Li J. Cyber security meets artificial intelligence: a survey. Frontiers Inf Technol Electronic Eng. 2018;19:1462–1474. Available from: https://doi.org/10.1631/FITEE.1800573.

[238] Abeshu A, Chilamkurti N. Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag. 2018;56(2):169–175. Available from: https://doi.org/10.1109/MCOM.2018.1700332.

[239] Kaloudi N, Li J. The AI-Based Cyber Threat Landscape: A Survey. ACM Comput Surv. 2021 January;53(1):Article 20, 34 pages. Available from: https://doi.org/10.1145/3372823.

[240] Meng X, Shan Z, Liu FD, et al. MCSMGS: Malware Classification Model Based on Deep Learning. In: Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery; 2017. p. 272–275.

[241] Xin Y, Kong LS, Liu Z, et al. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access. 2018;6:35365–35381.

[242] Andrasko J, Mesarcik M, Hamulak O. The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. AI & Soc. 2021;36:623–636. Available from: https://doi.org/10.1007/s00146-020-01125-5.

[243] Biasin E, Kamenjasevic E. Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. Int Cybersecur Law Rev. 2022;3:163–180. Available from: https://doi.org/10.1365/s43439-022-00054-x.

[244] Short AR, Leligou HC, Papoutsidakis M, Theocharis E. Using Blockchain Technologies to Improve Security in Federated Learning Systems. In: 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). Madrid, Spain; 2020. p. 1183–1188.

[245] Taddeo M, Floridi L. How AI can be a force for good. Science. 2018;361:751–752.

[246] Mahmud H, Islam AKMN, Ahmed SI, Smolan K. What influences algorithmic decision-making? A systematic literature review on algorithm aversion. Technological Forecasting and Social Change. 2022 Feb;175:121390.

[247] Dietterich TG. Steps Toward Robust Artificial Intelligence. AI Magazine. 2017;38(3):3–24.

[248] Ahmed IM, Kashmola M, Ahmed IM. Threats on Machine Learning Technique by Data Poisoning Attack: A Survey. In: Advances in Cyber Security; 2021. .

[249] Tolpegin V, Truex S, Gursoy ME, Liu L. Data Poisoning Attacks Against Federated Learning Systems;. Georgia Institute of Technology, Atlanta GA 30332, USA.

[250] Yerlikaya FA, Bahtiyar S. Data poisoning attacks against machine learning algorithms. Expert Systems with Applications. 2022;208:118101.

[251] Ramirez MA, et al. Poisoning attacks and defences on artificial intelligence: A survey. arXiv preprint arXiv:220210276. 2022;.

[252] Wang Y, et al. Adversarial Attacks and Defences in Machine Learning-Powered Networks: A Contemporary Survey. 2023;.

[253] Unknown. Evasion Attacks on Machine Learning or Adversarial Examples; Unknown. Towards Data Science. Available from: https://towardsdatascience.com/evasion-attacks-on-machine-learning-or-adversarial-examples-12f2283e06a1.

[254] Tufail S, Batool S, Sarwat AI. False Data Injection Impact Analysis In AI-Based Smart Grid. In: SoutheastCon 2021; 2021. p. 01–07.

[255] Amin M, Al-Obeidat F, Tubaishat A, Shah B, Anwar S, Tanveer TA. Cyber security and beyond: Detecting malware and concept drift in AI-based sensor data streams using statistical techniques. Computers and Electrical Engineering. 2023;108:108702.

[256] Isaac ERHP, Reno J. AI Product Security: A Primer for Developers. 2023;.

[257] European Commission. Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence and amending certain Union Legislative Acts (Artificial Intelligence Act); 2021. COM(2021) 206.

[258] Regulatory Framework for Artificial Intelligence; Unknown. European Commission Digital Strategy. Available from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[259] European Parliament Adopts Its Negotiating Position on the EU AI Act; 2023. Gibson, Dunn & Crutcher LLP. Available from: https://www.gibsondunn.com/wp-content/uploads/2023/06/european-parliament-adopts-its-negotiating-position-on-the-eu-ai-act.pdf.

[260] Cybersecurity of AI and Standardisation; 2023. European Union Agency for Cybersecurity (ENISA). Available from: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation.

[261] Zhang C, Wu C, Wang X. Overview of Blockchain Consensus Mechanism. In: Proceedings of the 2020 2nd International Conference on Big Data Engineering. BDE 2020. New York, NY, USA: Association for Computing Machinery; 2020. p. 7â12. Available from: https://doi.org/10.1145/3404512.3404522.

[262] Bernal Bernabe J, Canovas JL, Hernandez-Ramos JL, Torres Moreno R, Skarmeta A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access. 2019;7:164908–164940.

[263] Dusk Network Tackles Financial Privacy Concerns With Daybreak; 2023. Cointelegraph. Available from: https://cointelegraph.com/press-releases/dusk-network-tackles-financial-privacy-concerns-with-daybreak.

[264] Galal HS, Youssef AM. Publicly Verifiable and Secrecy Preserving Periodic Auctions. 2021 September 17;.

[265] Lindell Y. Secure Multiparty Computation. Commun ACM. 2021 January;64(1):86–96.

[266] Chiang JHy, David B, Gama M, Lebeda CJ. Correlated-Output-Differential-Privacy and Applications to Dark Pools. 2023;.

[267] Nassar M, Salah K, Rehman MHU, Svetinovic D. Blockchain for Explainable and Trustworthy Artificial Intelligence. First published on 17 October 2019;.

[268] IPFS; 2023. InterPlanetary File System (IPFS). Available from: https://ipfs.tech/.

[269] Neumann V, Davidge G, Harding M, Cunningham J, Davies N, Devaney S, et al. Examining Public Views on Decentralised Health Data Sharing. PLoS One. 2023;18(3):e0282257.

[270] Markovic M, Naja I, Edwards P, Pang W. The Accountability Fabric: A Suite of Semantic Tools For Managing AI System Accountability and Audit. 2021;.

[271] European Union Agency for Cybersecurity (ENISA). Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers; 2017.

[272] Self-Sovereign Identity; 2023. Dock. Available from: https://www.dock.io/post/self-sovereign-identity.

[273] European Union Agency for Cybersecurity (ENISA). Artificial Intelligence and Cybersecurity Research; 2023.

[274] Algarvio H. The Role of Local Citizen Energy Communities in the Road to Carbon-Neutral Power Systems: Outcomes from a Case Study in Portugal. Smart Cities. 2021;4(2):840–863.

[275] Technology Review. The $2.5 Trillion Reason We Can't Rely on Batteries to Clean Up the Grid; 2018.

[276] Simpkins LG. The Side Effects of Lithium Mining. 2021;.

[277] Ostrom E. Collective action and the evolution of social norms. Journal of economic perspectives. 2000;14(3):137–158.

[278] Hardin G. The Tragedy of the Commons. Science. 1968 Dec;162(3859):1243–1248. Available from: http://science.sciencemag.org/content/162/3859/1243.

[279] Junlakarn S, Kokchang P, Audomvongseree K. Drivers and Challenges of Peer-to-Peer Energy Trading Development in Thailand. Energies. 2022;15:1229.

[280] Gui E. Investment Planning and Institution Design for Community Microgrids as a Socio-technical Energy System; 2019.

[281] de Almeida L, Klausmann N. Peer-to-Peer Energy Communities: Legal Definitions and Access to Markets. Journal Name. 2021;.

[282] Schneiders A, Shipworth D. Community Energy Groups: Can They Shield Consumers from the Risks of Using Blockchain for Peer-to-Peer Energy Trading? Journal Name. 2021;.

[283] European Commission. European Commission Press Corner: European Green Deal: Commission proposes transformation of energy system to make it fit for 55target. 2023;.

[284] European Union. Directive 2018/2001 of the European Parliament and of the Council. 2018 12;.

[285] Sudhoff R, Schreck S, Thiem S, Niessen S. Operating Renewable Energy Communities to Reduce Power Peaks in the Distribution Grid: An Analysis on Grid-Friendliness, Different Shares of Participants, and Economic Benefits. Energies. 2022;15:5468.

[286] Doci G, Vasileiadou E, Petersen AC. Exploring the transition potential of renewable energy communities. Futures. 2015;66:85–95.

[287] Schweizer-Ries P. Energy sustainable communities: Environmental and psychological investigations. Energy Policy. 2008;36:4126–4135.

[288] Commission E. Blockchain in Energy Communities; 2017.

[289] Wang X, Yang W, Noor S, Chen C, Guo M, van Dam KH. Blockchain-based smart contract for energy demand management. Energy Reports. 2019;.

[290] Wen S, Xiong W, Tan J, Chen S, Li Q. Blockchain enhanced price incentive demand response for building user energy network in sustainable society. Energy Reports. 2021;7:2704–2712.

[291] Guo Y, Wan Z, Cheng X. When blockchain meets smart grids: A comprehensive survey. High-Confidence Computing. 2022;2(2):100059.

[292] Mengelkamp E, GÃ¤rttner J, Rock K, Kessler S, Orsini L, Weinhardt C. Designing microgrid energy markets: A case study - The Brooklyn Microgrid. Applied Energy. 2018;210:870–880.

[293] Durillon B, Davigny A, Kazmierczak S, Barry H, Saudemont C, Robyns B. Decentralized neighbourhood energy management considering residential profiles and welfare for grid load smoothing. Sustainable Cities and Society. 2020;63:102464.

[294] Noor S, Yang W, Guo M, van Dam KH, Wang X. Energy Demand Side Management within Micro-grid Networks Enhanced by Blockchain. Applied Energy. 2018;226:47–60.

[295] Budish E, Cramton P, Shim J. The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response *. The Quarterly Journal of Economics. 2015 07;130(4):1547–1621.

[296] Kolahan A, Maadi SR, Teymouri Z, Schenone C. Blockchain-based solution for energy demand-side management of residential buildings. Energy Reports. 2021;7:1813–1824.

[297] Rozas D, Tenorio-Fornes A, Diaz-Molina S, Hassan S. When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance. SAGE Open. 2021;11(1).

[298] Cila N, Ferri G, de Waal M, Gloerich I, Karpinski T. The Blockchain and the Commons: Dilemmas in the Design of Local Platforms. 2020;.

[299] Cutore E, Volpe R, Sgroi R, Fichera A. Energy management and sustainability assessment of renewable energy communities: The Italian context. Energy Conversion and Management. 2023;.

[300] Gan L, Jiang P, Lev B, Zhou X. Balancing of supply and demand of renewable energy power system: A review and bibliometric analysis. Sustainable Futures. 2020;.

[301] Siano P. Demand response and smart grids-A survey. Renewable and Sustainable Energy Reviews. 2014;30:461–478.

[302] OMIE. Spanish and Portugese Energy Prices; 2023. Accessed: 14/08/2023. https://www.omie.es/pt.

[303] Scilling. Digital Mining; 2023. Accessed: 14/08/2023. https://www.scillingmining.com/.

[304] Rees P. Culatra Island Home-Owners to be Granted 30-Year Residence Licences. Journal Name. 2017 October;.

[305] Github. GitHub; 2023. https://github.com/The-CTra1n/RE-Communities.

[306] Paillier P. Paillier Encryption and Signature Schemes.;.

[307] Will MA, Ko RKL. Chapter 5 - A guide to homomorphic encryption. In: Ko R, Choo KKR, editors. The Cloud Security Ecosystem. Boston: Syngress; 2015. p. 101–127.

[308] Penumbra;. Accessed: 23/07/2023. https://penumbra.zone/.

[309] McMenamin C, Daza V, Fitzi M, O'Donoghue P. FairTraDEX: A Decentralised Exchange Preventing Value Extraction. In: Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security. DeFi'22. New York, NY, USA: Association for Computing Machinery; 2022. p. 39â46.

[310] CoW Protocol;. Accessed: 11/08/2023. https://docs.cow.fi/.