UNIVERSITY OF PIRAEUS

School of Finance and Statistics
Department of Finance and Banking Administration
Postgraduate Study Program in "Finance and Banking" with specialty in "Finance and Banking Administration".

"SMART CONTRACTS & CRYPTOCURRENCIES"

A Legal Perspective

The Case of Greece as a Member of the EU

Georgios Petalas (MXPH2017)

SUPERVISOR

Professor Mr. Nikolaos Kourogenis

Evaluation Committee:

Professor Mr. Nikolaos Kourogenis

Assistant Professor Mr. M. Anthropelos

Assistant Professor Mr. N. Englezos

JANUARY 2023

ABSTRACT

This dissertation aims to explore the field of cryptocurrencies and smart contracts mainly from a legal perspective. The developing regulatory framework and the challenges thereof is discussed, particularly in relation to Ethereum as compared to Bitcoin. The theoretical part of the dissertation examines basic definitions, outlines the profile and function of the cryptocurrency and blockchain environment, as well as addresses the fundamental legal issues arising from smart contracts. In the empirical part of the dissertation, the perplexing and sometimes, insufficient legal framework both in the EU and in Greece is be brought forward as a practical case study. The current legal and regulatory framework is nascent, presenting significant legal gaps regarding cryptocurrencies and smart contrast in theory and practice. However, there are indeed viable proposals for further research and application.

Keywords: Cryptocurrency, Smart Contracts, Bitcoin, Ethereum, Blockchain, Greek Legal System, Antitrust Law

ΣΥΝΤΟΜΗ ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία αποσκοπεί στη διερεύνηση του πεδίου των κρυπτονομισμάτων και των έξυπνων συμβάσεων (Smart Contracts) κυρίως από νομική άποψη. Συζητείται το αναπτυσσόμενο ρυθμιστικό πλαίσιο και οι προκλήσεις που αυτό συνεπάγεται, ιδίως σε σχέση με το Ethereum σε σύγκριση με το Bitcoin. Στο θεωρητικό μέρος της διατριβής εξετάζονται οι βασικοί ορισμοί, σκιαγραφείται το προφίλ και η λειτουργία του περιβάλλοντος των κρυπτονομισμάτων και της blockchain, καθώς και αναλύονται τα θεμελιώδη νομικά ζητήματα που προκύπτουν από τις έξυπνες συμβάσεις. Στο εμπειρικό μέρος της διατριβής, το αινιγματικό και ενίοτε, ανεπαρκές νομικό πλαίσιο τόσο στην ΕΕ όσο και στην Ελλάδα αναδεικνύεται ως πρακτική μελέτη περίπτωσης. Το ισχύον νομικό και ρυθμιστικό πλαίσιο είναι εκκολαπτόμενο, παρουσιάζοντας σημαντικά νομικά κενά σχετικά με τα κρυπτονομίσματα και τις έξυπνες συμβάσεις στη θεωρία και την πράξη. Ωστόσο, υπάρχουν πράγματι βιώσιμες προτάσεις για περαιτέρω έρευνα και εφαρμογή.

Λέξεις-κλειδιά: Κρυπτονομίσματα, Έξυπνες Συμβάσεις (Smart Contracts), Bitcoin, Ethereum, Blockchain, Ελληνικό Νομικό Σύστημα, Αντιμονοπωλιακό Δίκαιο

AKNOWLEDGEMENTS

I would like to sincerely thank my professor Nikolaos Kourogenis for the abundant and constructive guidance, he provided me with throughout the accomplishment of this dissertation. I would also like to thank my family, especially my twin brother for his financial support of my postgraduate studies.

TABLE OF CONTENTS

1. INTRODUCTION

The cryptocurrency notion is not new. Several years ago, cryptocurrencies were created and offered to engage in financial transactions without exclusively relying on banks or governments.

The idea for cryptocurrency first emerged in 1983, when American cryptographer David Chaum published a conference paper outlining an early form of anonymous cryptographic electronic money. The concept was for a currency that could be sent untraceably and in a manner that did not require centralized entities (i.e., banks). In 1995, Chaum built on his early ideas and developed a proto-cryptocurrency called Digicash. It required user software to withdraw funds from a bank and required specific encrypted keys before said funds could be sent to a recipient (Chohan, 2022).

Bit Gold, often deemed a direct precursor to Bitcoin, was designed in 1998 by Nick Szabo. It required a participant to dedicate computer power to solving cryptographic puzzles, and those who solved the puzzle received a reward. Combined with Chaum' s work, it results in something that comes very close to resembling Bitcoin (Chohan, 2022).

But Szabo could not solve the infamous double-spending problem (digital data can be copied and pasted) without the use of a central authority. As such, it was not until a decade later when a mysterious person or group, using the pseudonym Satoshi Nakamoto, set the history of Bitcoin and later cryptocurrencies in motion, by publishing a white paper called *Bitcoin – A Peer to Peer Electronic Cash System. (Burniske ansd Tatar, 2018)*

The very first cryptocurrency created is known as Bitcoin. On October 31, 2008, Satoshi Nakamoto published the Bitcoin white paper, describing the functionality of the Bitcoin blockchain network. Satoshi formally began work on the bitcoin project on August 18th, 2008, when they purchased Bitcoin.org. (Burniske and Tatar, 2018)

The history of Bitcoin was underway. Satoshi Nakamoto mined the first block of the Bitcoin network on January 3, 2009. They embedded a headline from The Times newspaper in this initial block, making a permanent reference to the economic conditions — involving bank bailouts and a centralized financial system — that Bitcoin was partly a reaction against (Chohan, 2022).

This first block — which resulted in 50 bitcoins being mined — is now referred to as the Genesis Block. Bitcoin had virtually no value at this time, as well as for the first few months of its existence. Six months after bitcoin became tradeable, in April 2010, the value of one BTC was just under 14 cents. By early November, the price surged to 36 cents before settling at around 29 cents (Chohan, 2022).

Soon, other cryptocurrencies were offered, as well as specialized platforms with one of the most prominent being Ethereum. It is noteworthy that cryptocurrency network is owned by nobody in specific, much like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin users around the world. While developers are improving the software, they can’t force a change in the Bitcoin or other Cryptocurrency protocol because all users are free to choose what software and version they use. For those reasons, as well as a means of investment portfolio diversification or even hedging, cryptocurrencies grew abruptly in popularity. The cons of lack of regulatory framework, the multiple scam accusations, blended with the pros of the anonymity, traceability and increasing security of transactions in the context of blockchain applications and the rise of decentralized finance, resulted in another prominent characteristic of cryptocurrencies: volatility. And while the volatility of cryptocurrencies is both attractive and potentially devastating, the underlying technology behind them all, blockchain, has the power to change many sectors of our society. Whether it s providing accessible and affordable financial exchange options, securing one s funds so that no one but them can access them, or providing accurate data for your insurance quote, blockchain technology has the potential to be used in almost every area of the economy (Tikhomirov, 2017).

As the market becomes more stable with increased knowledge, and with the introduction of new areas such as stablecoins and decentralized finance (DeFi), it is expected for cryptocurrency and its potential from an investment and technological perspective to augment. This is regardless of whether it
is Bitcoin or another blockchain project that stokes one’s interest (Tikhomirov, 2017).

However, notwithstanding the above advancements, the legal part of this remarkable financial evolutionary process lags behind in terms of development. The regulatory framework regarding the interaction of end users, entities and authorities with cryptocurrencies are not amply demarcated. The most protuberant example of legal gap revolves around smart contracts, which, automatedly, via a custom algorithm, execute the code thereof, completing transactions on behalf of the end users. As this could be a preliminary form of artificial intelligence, the legal perspectives of personality, capacity and responsibility should be outlined. Significant efforts are being made at EU level, but have only started recently, without any concrete results (European Commission, 2022).

Therefore, this dissertation aims to explore the field of cryptocurrencies and smart contracts mainly from a legal perspective. The developing regulatory framework and the challenges thereof will be discussed, particularly in relation to Ethereum as compared to Bitcoin. The theoretical part of the dissertation will examine basic definitions, outline the profile and function of the cryptocurrency and blockchain environment, as well as address the fundamental legal issues arising from smart contracts. In the empirical part of the dissertation, the perplexing and sometimes, insufficient legal framework both in the EU and in Greece will be brought forward as a practical case study. Individuals and companies interested in developing crypto-related activities in Greece recognise that this sector is mostly unregulated, although some rules of law do apply to crypto users. According to the views of the Hellenic Capital Market Commission, cryptocurrencies are not currency, but rather portfolio assets. At the moment, the Greek authorities have transposed in the national legislation the EU s AMLD5 (Anti-Money Laundering Directive) (Haffke et al., 2020).

Thus, a lot of questions remain to be answered. Is the current legal and regulatory framework sufficient? What are the legal gaps regarding cryptocurrencies and smart contrast in theory and practice? Lastly, are there any viable proposals for further research and application? The following chapters constitute an attempt of providing sound answers.

2. LITERATURE REVIEW

2.1. Significant Definitions

2.1.1. Cryptocurrency

An effective dialogue on cryptocurrencies requires as a first step developing a common taxonomy at EU level. The Commission currently provides a working definition of virtual currencies as: "*a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*" (European Commission, 2016 in Solodan, 2019). This broad categorisation of virtual currencies can be further broken down into various subcategories. Virtual currencies can for instance be convertible, meaning they can be directly exchanged for "real" currency by virtual currency exchangers, or non-convertible, meaning they cannot be exchanged for real currency. Furthermore, virtual currencies can be centralised, meaning they have a single administrating authority, or decentralised. Other bodies consider cryptocurrencies as a subset of virtual currencies that are used in a decentralised manner, using for example Blockchain technology. A proposed definition for cryptocurrency is: "*Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography. i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy*" (Financial Action Task Force, 2014 in Solodan, 2019). Though neither of these definitions are as of yet legally binding, they provide a framework for engaging with technical and policy-related issues surrounding cryptocurrencies from a cybersecurity perspective. As with other fiat currencies, the value of cryptocurrencies is driven by supply and demand. Where the supply of a cryptocurrency is capped, and demand exceeds supply, the value of the cryptocurrency will rise (Solodan, 2019).

As cryptocurrencies are increasingly employed for both legitimate and illicit purposes, there is a need for a debate on the cybersecurity concerns that may arise surrounding their use. A number of administrations are well advanced in their plans to authorise the use of cryptocurrencies. Cost reductions, improved risk management, and automated regulatory compliance include benefits of cryptocurrencies utilisation. owever, with the growing use of cryptocurrencies, greater attention needs to be given to the cybersecurity associated with their use, as well as the regulatory aspects, in order to protect the users and society from illegal activities, including money laundering and terrorism financing (Solodan, 2019).

2.1.2. Blockchain

Blockchain is a decentralised technology. As decentralisation is one of the main characteristics of blockchain technology and a considerable number of (legal) questions are related thereto, we assume that the guidelines can also be applied to other Distributed Ledger Technologies. However, we acknowledge that there may be areas where this is not feasible due to technological changes. In such cases, specific principles or rules will have to be adopted. Even if this report often refers to the blockchain or the blockchain technology, it is well understood that there is not only one blockchain, but many variations thereof. From a legal perspective, the distinction between private and public blockchain is essential. A private blockchain is a blockchain in which only certain persons can participate. Before participation in the blockchain, the respective (personal) participation requirements are usually checked by the (central) gatekeeper. The users of a private blockchain are often identifiable (mostly by the gatekeeper, sometimes also by other users of the blockchain). Further, the nodes operating the blockchain are usually known. Thus, the operation of the blockchain can be interfered with. A public blockchain is a blockchain which can be joined at any time by downloading the publicly available client (provided the technical requirements are met). There is neither a check of requirements by a gatekeeper nor authentication of the individual participants of the blockchain (Panova, 2019; Anush et al., 2021).

A further distinction can be made between permissioned and permissionless blockchains. This subdivision is aimed in particular at the issue of authorisations. In the case of permissioned blockchains, only certain a) various types of smart contracts can be distinguished. the smart contract can be: (1) mere code and no legal agreement exists (the situation is a mere transaction in the technical sense of the word); (2) a tool to execute a legal agreement; the legal agreement exists off-chain; (3) a legally binding declaration of will, such as an offer or acceptance or constitute a legal agreement itself; (4) merged with the legal agreement and therefore exists simultaneously both on-chain and off-chain; in the latter situation, it ought to be determined whether the agreement should be treated as on-chain or off-chain. b) if the smart contract is merged with the legal agreement, it ought to be determined by the parties whether the agreement should be treated as on-chain or off-chain. c) the principles focus on smart contracts as a legally binding declaration (such as an offer or acceptance) and on smart contracts as a legal agreement. People are allowed to execute transactions on the blockchain, whereas, in the case of permissionless blockchains, anyone is allowed to execute transactions on the blockchain. In general, a blockchain can be classified as either a private or public blockchain as well as permissioned or permissionless. There are therefore four main types, namely: (1) public permissioned blockchains; (2) public permissionless blockchains; (3) private permissioned blockchains; and (4) private permissionless blockchains. The parties to blockchain transactions can be businesses, governments and/or consumers. The legal status, and consequently the bargaining positions and knowledge levels, varies considerably both between and within these groups. In many respects, small- and medium-sized enterprises (SMEs) have a far weaker position than, for example, large international business enterprises or governments and government agencies. This applies even more so to consumers, whose position in DLT transactions is extremely weak (Anush et al., 2021). Consumer protection must at least be at the same level on-chain as it is off-chain, given the asymmetrical knowledge, information and bargaining position between consumers and businesses as well as consumers and governments. This also applies to other weaker parties, such as tenants and employees (Panova, 2019).

2.1.3. Decentralized Finance

Decentralized finance (or "DeFi") is a financial ecosystem based on blockchain technology. It lets users buy and sell assets and financial services as a form of investment or financing without middlemen (Salami, 2020). To understand how DeFi works, we must first delve into what s behind it. DeFi uses blockchain, which connects users without a central server and can transfer data and assets securely, under the users own watch. Transactions are regulated under smart contracts, computer programs that also use blockchain and run automatically when the parameters the parties set in advance are met. They use blockchain to store and transfer digital assets and smart contracts to make sure the parties keep their end of the bargain. A recent phenomenon, DeFI s potential and use will largely depend on user needs and regulation. People and businesses invest and get funding with DeFi apps that bridge supply and demand, using blockchain to make sure transactions remain secure. Since DeFi apps have an open code, anyone with Internet can use it, create and offer services (like lending), and combine existing services. DeFi software and systems are available to the public free of charge and can even be copied, enhanced or adapted to user needs. To access DeFi apps, one needs a virtual wallet to store tokens — the hard currency in blockchain, bought with euros, dollars and other legal tender. DeFi app users looking for a return on investment in tokens can program a smart contract to sell cryptocurrency at a certain price. And users who want to buy tokens can prepare a smart contract to automatically acquire them when they reach the desired value. In both cases, transactions are automatic and there is no intermediary. It is a decentralized financial ecosystem, it's not regulated. Under the traditional financial system, personal details can be checked to review loan applicants' indebtedness and other aspects. In blockchain, however, a public key that holds no personal information is the identifier. This can make preventing fraud and other financial crimes tricky. Security is also an important factor. On DeFi platforms, users safeguard their own assets via access keys and authentication to sign in to apps. Because no entity can provide or restate their personal details if they are stolen, users could lose all their assets (Salami, 2020).

2.1.4. Smart Contracts

Smart Contracts are self-executing computer programmes (Drummer and Neumann, 2020): Smart Contracts are a much-discussed topic in legal literature, which is partially caused by their name. When lawyers think of contracts, they immediately think of legally binding agreements, although this is not necessarily what coders mean. From a purely technical perspective, Smart Contracts are programme codes that represent "if-then" conditions. From a legal perspective, the question is whether these programme codes can be contracts under civil law. This question cannot be answered by presenting a hard and fast rule. A careful case-by case analysis will be needed, given the differences in types of blockchains, parties and interests involved. Nevertheless, certain fairly general guidelines can be given, but no hard and fast rules. Such rules have the advantage that they provide certainty ex ante, clarity already when the contract is at a stage of formation, but may be over- or under-inclusive in their practical impact and, therefore, may result in an unfair outcome. A case-by-case analysis has the advantage that it provides flexibility to courts and arbitrators, so fairness ex post, after formation of the contract and in the stage that it is performed, but results in uncertainty. Given that the technologies on which these Principles focus are new and still in continuous development, a balance has to be struck between ex ante certainty and ex post fairness (De Filippi et al., 2021). Guidelines, appear to be the most suitable means of achieving the most important guideline being, that Smart Contracts can also be binding under civil law. The guidelines take the traditional requirements for a validly binding agreement as their starting point. A contract comes into existence when the declarations of intent of two parties match. In other words, a contract is concluded if the offer and acceptance are congruent. Offer and acceptance here are given the meaning as generally accepted in traditional contract law. A legally valid offer must be sufficiently specific in terms of content and the offeror must express sufficient intent to be bound (De Filippi et al., 2021). However, a mere invitation to make an offer is different from an offer; this is always the case when no sufficient intention to be bound is expressed for an offer. A valid acceptance must be in agreement with the offer; the acceptance must therefore not deviate from the offer. Although a case-by-case approach is advocated in these guidelines, the following scenarios can still be identified:

The smart contract can be mere code and no legal agreement exists (the situation is a mere Transaction in the technical sense of the word). As illustrated, Smart Contracts are "if-then" terms. Therefore, there may also be cases in which Smart Contracts merely perform status changes on the blockchain that lead to de facto changes without any further legal effect (De Filippi et al., 2021). Such Smart Contracts are not contracts in the civil law sense, but merely technical phenomena (Drummer and Neumann, 2020).

The smart contract can be a tool to execute the legal agreement; ***the legal agreement exists off-chain.*** In this case, a legally binding contract is concluded outside the blockchain system (off-chain). In this off-chain contract, the rights and obligations of the contracting parties are defined and it is already agreed that blockchain technology, or more precisely Smart Contracts, will be used to execute the contract. The Smart Contracts used in this case are merely acts of performance or settlement tools. However, these Smart Contracts are not binding contracts under civil law.30 Certainly, in this context, there may be challenging legal issues (such as under what circumstances blockchain technology can be used to fulfil contracts, who bears the risk of poor performance of a Smart Contracts, etc). However, these issues can be resolved using the general principles of civil law (Drummer and Neumann, 2020).

The smart contract can be a legally binding declaration of will, such as an offer or acceptance or constitute a legal agreement itself. When analysing the formation stage leading towards a contract, it could very well happen that only a part of that stage is concluded by making use of Smart Contracts (De Filippi et al., 2021). The Smart Contract (and again the use of the word contract shows how unfortunate that term here is from a legal perspective) could be the offer, which is accepted off-chain (for example, because of written or verbal communication), or the on-chain acceptance of an offer that itself is off-chain. In the latter situation, an offer is made off-chain eg in the form of source code; acceptance takes place on-chain when the other party compiles the source code into byte code and deploys it to the blockchain. Note, however, that if the first party now fails to interact with the bytecode (eg by transferring cryptocurrency to the address at which the bytecode is deployed), this is a breach of contract, although this may sound almost counterintuitive. To make clear that these Principles, particularly when focusing on consumer protection, also apply when the Smart Contract cannot be qualified as a legal agreement, but consists of elements which result in such an agreement, it must be clear that the guidelines also apply then (Drummer and Neumann, 2020).

In light of the above, the question arises as to whether Smart Contracts, ie the programme code, can constitute legally binding declarations. Ultimately, the underlying legal question is whether declarations of intent can be expressed by a programme code. It is submitted that – as an outflow of private autonomy – a Smart Contract should be an eligible way to express the will of a party (Zou et al., 2019). However, this should certainly not lead to a reduction of the protection of market participants or consumers, i.e., all remedies (e.g., moral unlawfulness remedies, consumer protection rules) also apply in the context of Smart Contracts. A Smart

Contract stored on a blockchain can also generally fulfil the requirements of an offer, namely the definiteness of the content and the intention to bind: i. given the *if X, then Y-condition* of the Smart Contract, it must already be clear when the Smart Contract is deployed which performance is owed if the Smart Contract is triggered, e.g., by payment of a cryptocurrency amount (De Filippi et al., 2021). As a result, the Smart Contract will generally be determined in terms of its content; and ii. binding intention is also generally given by the storage on the blockchain, since, after storage on the blockchain, a Smart Contract can no longer be changed due to the characteristics of the blockchain. Thus, a Smart Contract can constitute an offer in the legal sense. Such an offer may be accepted by implication. Potential objection as to compilation of source to bytecode necessary: from a technical perspective, Smart Contracts are a set of instructions in the form of bytecode. Thus, before executing a Smart Contract on a blockchain network, the – potentially human readable – source code has to be compiled into machine-readable bytecode (Zou et al., 2019). The misconception could arise that only because of the need to compile source code into bytecode could the source code not represent the content of a – potentially – legally relevant Smart Contract: this is not the case, because although the translation of the contract terms from source into bytecode is necessary, the source code still determines the bytecode and thus also the key elements of the Smart Contract. Insofar as errors occur in the translation of source into bytecode (for example, because the compiler is defective), these translation errors must be resolved in accordance with general civil law provisions. In practical terms, this would mean that if person A wants to make an offer on the blockchain using a Smart Contract and programmes a Smart Contract in source code for this purpose, defining the key elements of the offer, person A generally only wants to be bound by this offer. If the offer is now misrepresented due to a faulty compilation of the source code in bytecode, whether person A should be bound to the (faulty) offer expressed in bytecode must be reviewed according to general civil law regulations. To conclude, a Smart Contract can be regarded as (part of) a legally binding agreement, provided that the prerequisites for the conclusion of a contract in the respective legal system (e.g. offer and acceptance) are fulfilled (Zou et al., 2019). This conclusion is two-fold (De Filippi et al., 2021). First, when analysing the relationship between negotiating parties, the use of source code or bytecode does not by itself prevent any conclusion that they created a legally binding agreement. Second, following the well-established rules on contract formation, a declaration of will could very well be expressed in coded format. It cannot be denied that, in practice, numerous and difficult to resolve problems may come up. For example, consider the situation where two commercial parties have a history of implementing their off-chain legal agreement using bytecode on a blockchain, without reference to any source code and one party deploys the same, familiar bytecode with the intention that the other party would be able to accept it as legally binding simply by interacting with the bytecode e.g., by transferring cryptocurrency to the address at which the bytecode is deployed. In this case, although their history might lead a court to imply terms by custom and practice (the terms expressed in the source code exchanged on previous occasions), it could reasonably be argued that both parties communicated their legally binding intentions solely through bytecode (Drummer and Neumann, 2020).

The smart contract is merged with the legal agreement and therefore exists simultaneously both on-chain and off-chain; in the latter situation, it ought to be determined whether the agreement should be treated as on-chain or off-chain. in principle 9, it is laid down that, in the case of a conflict between the off-chain and the on-chain version of the contract, the off-chain text prevails. Still, the contract is of a hybrid nature, which may, from a legal viewpoint, affect its formation, content, performance and enforcement. This is particularly relevant in cases of so-called Ricardian contracts, developed by Ian Grigg in 2000 as contracts which are both readable on paper and readable by computer programmes (Drummer and Neumann, 2020).

2.1.5. Ethereum

Smart contracts can be developed in different blockchain-based platforms. Many of them offer distinctive features and support high-level programming languages for deploying smart contracts (Chen et al., 2021). The most important and popular one is, undoubtedly, Ethereum. While most people know Ethereum thanks to its token (Ethereum, Ether or ERC-20), many might not be aware of that it is the world's leading smart contract platform, and the best choice for several developers. Ethereum is a smart contract ecosystem created by Vitalik Buterin and other co-founders in 2013 (Jani, 2017). It is a Proof of Work blockchain network hosting the Ethereum Virtual Machine (EVM), which is a "Turing-complete system". The Ethereum platform is also a hotspot for some DeFi (Decentralized Finance) applications. A key benefit of this platform is the degree of standardization and the support offered. Once a set of clear guidelines for developers was published, Ethereum have made smart contract development easier and less risky (Chen et al., 2021). Moreover, apart from having the biggest market capitalization among all the smart contract platforms, Ethereum is completely dedicated to improving the way smart contracts are created and run (Jani, 2017).

2.2. The Applications, Pros & Cons of Smart Contracts

There are distinct practical applications where smart contracts can be applied (Chen et., 2021).

2.2.1. Internet of Things and Smart Property

There are billions of nodes sharing data among each other through the Internet. Smart contracts can allow those nodes to share or access digital properties without a trusted third party.

2.2.2. Music rights management

A possible use case is to record the music s ownership rights. A smart contract can enforce payments for music owners if a song is used for commercial purposes. It also ensures that those payments are being distributed between the music s owners.

2.2.3. E-commerce

Another potential use case is to facilitate the trade between untrusted parties, without the need for a middleman. This would result in a reduction of the trading costs. Smart contracts can release the payment to the seller, once the buyer is satisfied with the good or service they received.

2.2.4. Insurance

Smart contracts can offer advantages in speeding up the claims of insurance s processes. An example could be the life insurance. Their policy terms would be encoded into a smart contract. In case of passing away, the death certificate would be provided as the input trigger for the smart contract in order to release the payment to the named beneficiaries.

2.2.5. Supply Chain and Logistics

The use of smart contracts is revolutionizing the supply chain and logistics sector as well. Blockchain can provide a permanent record of the transit of goods among multiple handlers. Payments can be executed automatically upon the receipt of delivery, and inventory levels automatically updated in real-time.

2.2.6. Rights for Digital Token Holders

Asset tokenization may mean individual token-holders have rights. These rights can be, here again, coded into a smart contract. If firm s stocks are tokenized, shareholders have voting rights. And, through smart contracts, the person s voting right is granted when every ballot is opened up. They also allow people to cast their vote and to vote from remote.

2.2.7. Pros & Cons

Smart contracts have the substantial potential to bring radical changes in the way international business are executed by speeding up transactions, reducing paperwork and causing cost-efficiency (Jani, 2017).

On the other hand, there also exist some drawbacks in developing smart contracts. Starting from the positive features, we can highlight:

• Disintermediation: through which contractual parties can enter into agreements with no dependence on a middleman.

• Efficiency, Accuracy and Rapidity: once a condition is met, the contract is automatically executed. Since smart contracts are digital and automated, there is no paperwork to process, and no time spent finding errors manually.

• Trust and Transparency: without a third party involved, and since encrypted transaction records are shared across the nodes, there is no need to question whether information has been altered on purpose for personal reasons.

• Security: since blockchain transaction records are encrypted, they are very hard to hack. Hackers would have to alter the entire chain to change a single record, because each record is connected to the previous and the following ones on a distributed ledger.

As to the risks:

• Confidentiality: although enterprises desire transparency, they hesitate to use a blockchain and to put their contractual information on it. Ethereum does not have an option for private smart contracts. Therefore, businesses will have to select their blockchain platform based on their needs.

• Accuracy: since a smart contract is a computer program, each term and condition of the contract needs to be coded, and there is possibility of misinterpretation or omission by the programmer. The more we use smart contracts, the more we could encounter loopholes in the code.

- Unreliable Inputs: for traditional contracts, the parties can proceed to a judicial court for redressal. But this is not possible with smart contracts, where legal validity is still largely debated.
- Bugs in the Code: they could lead to disputes and procedural complications concerning the identification of errors, and the parties responsible for those. There could be unforeseen repercussions.

2.3. The Legal Issues of Smart Contracts in the Context of Blockchain

As of today, in order to enable cryptocurrency markets to raise, both businesses and lawmakers must collaborate together for creating new engagement rules. Regulators and policymakers should yield clear guidelines and set basic principles to attract investors, ensure costumer protection and guarantee citizens' rights. One of the main issues is doubtless related to competitive practices and fair competition within the European law. A cryptocurrency network, e.g., through Bitcoin (Jani, 2017) should enhance efficiency and lower boundaries for new competitors to access digital marketplaces.

2.3.1. The "Law is Code" Principle

Given the aforementioned features of the blockchain, the mainstream adoption of this technology may require a shift in the way we perceive the role of law. We might need to re-think the mechanisms we use to regulate individuals and society, in order to better grasp the emergence of this new set of technological rules (Drummer and Neumann, 2020). Thanks to digital technology, code has been established as the dominant form for regulating the people s behaviour on the Internet. Programs can enforce rules more efficiently than legal code, but there are several limitations as well. This is mainly because transposing the flexibility and the ambiguity of legal rules into a programming language interpreted by a machine is not an easy task. With the emergence of blockchain (along with smart contracts), code has assumed a stronger role in regulating the actions of the Internet users (Raskin, 2016). Therefore, we have officially passed from the traditional notion of “code is law” (code having the effect of law) to the new conception of “law is code” (law defined as code). Law and tech can influence each other in many ways. They interact by means of a complex system of dependencies and interdependencies (Raskin, 2016).

Through the progressive growth of ICT, their relationship has significantly evolved. Over the Internet, regulations are done by private means within an environment that (due to its transnationality) seems to go beyond the jurisdiction of each state. The deployment of Internet network and the development of information technologies have generated a new status for humans, in which rules are set by software code. Software applications are different from hardware devices (De Graaf, 2019). Code can be produced using just a computer and can be easily distributed via any network connection, while building physical artefacts requires raw materials and production facilities. For this reason, the barriers to entry are much lower than in other contexts for software developers (De Graaf, 2019). This explains the exponential expansion of software applications in the past couple of decades. Yet, as opposed to the physical world in which the costs of reproduction are often high, in the digital world it is virtually null (Argelich-Comelles, 2020). Even the cost of distributing information is close to zero. Moreover, since software code is (by nature) digital, it can be modified or replicated from everybody; and any piece of program can be reproduced all around the world regardless of national boundaries. Thus, it is difficult for a country to avoid or prevent the importation and exportation of computer code. However, every device manufacturer or online operator is subject to the laws of her/his nation by disclosure obligations and monitoring requirements (De Graaf, 2019). The idea that "Code is Law" has now become a popular conception. Recently, there has been a tendency by both public institutions and private actors to replace current laws (which can only be enforced ex-post through state intervention) by technical regulations (which can be enforced ex ante through code). While it is true that code is increasingly assuming some of the typical functions of law, it is also true that law is progressively starting to assume the characteristics of code (Raskin, 2016). To this end, blockchain technology reinforces the trend to rely on code rather than on law; especially for regulating transactions. Combined with smart contracts, a blockchain promotes a new way of thinking about law. As a result, legislators could draft contractual rules in a manner closer to the technical ones. Blockchain is not only a neutral technology, but also a technical artefact with a specific architecture. Besides, since blockchains bypass the need for a central system and smart contracts can be executed and run on a distributed network, they are all transnational and reduce the risk of prosecution for legal proceedings. Latest discussions are focused on the optimization and efficiency of smart contracts. With respect to traditional contracts, their security level is superior and transaction costs are very low (Argelich-Comelles, 2020). Today, more and more interactions are mediated through technology, and we are delegating to tech the interpretation and application of law. But, as we increasingly rely on technological means for enforcing legal rules, we face the risk that law progressively assume the characteristics of code (Raskin, 2016). And, with the appearance of blockchain, this issue has become reality. Code can be used for enforcing existing legal provisions and also for defining them. We are currently experiencing a radical change in the way we intend the law. Nevertheless, laws should not be entirely and exclusively defined through technological processes, as tech cannot replace the democratic debate which must take place in the legislative branch. The principal risk is that, while the legal system provides a series of policies and procedures for society to collectively agree upon certain rights or obligations and whose legitimacy can be put into question, technical rules can be unilaterally imposed by software developers. Furthermore, in the context of smart contracts, since their enforcement is done through the technological framework itself, it becomes possible for private parties to bypass the legal safeguards required by the law. Thus, once a smart contract is executed, it will be enforced regardless of whether or not it is qualified as a valid contract under the law (Argelich-Comelles, 2020). Anyway, we cannot forget that blockchain-based applications are meant to operate in the real world, which is regulated by traditional rules of law. As to smart contracts, in order for them to be as effective as their typical counterparts, they must be actionable in the real world as well. Several legal rules are intended to be generic enough for being applicable to various situations. By definition, they must have a high level of abstraction for being able to encompass as many cases as possible. This is why legal rules need to be interpreted by a judge, and they have been drafted to and for humans. Therefore, in order to give meaning to the law, accounting for the initial intention of the legislator (along with human interpretation) is pivotal (De Graaf, 2019).

2.3.2. Lex Cryptographia

The widespread deployment of the blockchain technology has led to a new subset of law, the so called "Lex Cryptographia". In particular, it consists of a set of rules administered through self-executing smart contracts and decentralized autonomous organizations (DAOs) (Woebbeking, 2019). Since blockchains are becoming widely adopted, centralized systems and authorities could lose their ability to watch over the individuals' activities. As a result, there will be an increasing need to focus on how to regulate and shape the establishment of these emerging decentralized technologies (Woebbeking, 2019).

Legal theory has always sought to harmonize the struggle among nations, markets and individuals; trying to find the right balance between the interests of the public sphere and those of the private one. With the abrupt advent of decentralized applications and autonomous agents, there is no doubt that the traditional conceptions of the Internet regulations have to be reviewed. By means of an appropriate mix of these different levers of power, legal theorists have persuasively discussed that our use of the Internet could be tamed (Schrepel, 2019). Countries habitually approve laws in order to ban online services and for employing coercive power to shut down illegal services (like, for example, online gambling). Governments (along with private interests) progressively manipulate markets by pressuring search engines, advertising networks and other financial intermediaries (Woebbeking, 2019).

The emersion of Lex Cryptographia may oblige us to reevaluate the interactions between them (Becker, 2022). Current technologies can be used to institute new rules for organizations and, potentially, for governmental entities. Automatically enforced through self-executing code, smart contracts might edit some of the basic principles of property law, effectively turning property rights into a subset of contract law. Judicial enforcement of law could also be displaced by blockchain technology, and smart contracts could be made to rely on a certain degree of human judgment during their execution (Schrepel, 2019). For instance, in order to determine whether or not predefined conditions have been met, contractual clauses could be made dependent on the judgment of one or more external parties (known as "Oracles") (Schillig, 2021). One of these parties could be the judiciary, but it could be represented by independent arbitrators as well. Subsequently, these decentralized judiciaries can narrow the role of centralized judicial bodies. As of now, the rise of Lex Cryptographia can offer people access to alternative currencies, global markets, automated and trustless transactions systems, self-enforcing smart contracts, smart property and cryptographically activated assets (Schillig, 2021). Combined, all these elements could be used to promote individual freedoms and user autonomy. Hence, people could be granted equal access to basic digital institutions and infrastructure, regardless of their nationality. Through the experimentation of emergent blockchain-based applications, decentralized institutions and governance models could be designed and structured iteratively, rather than being imposed by centralized legal statutes (Schillig, 2021). This aspect could significantly contribute to that disintermediation process which is characterizing the online environment. In spite of the blockchains benefits, many of the emerging applications also come with some drawbacks (Schrepel, 2019). Given the transnational nature of blockchain technologies, malicious individuals can exploit them for illicit transactions. This factor, along with the pseudonymity provided by blockchain, can make complicated for law enforcement agencies to identify and prosecute these kinds of users (Becker, 2022).

As more and more communities form their own values, individuals' behaviour will become harder to regulate through external forces imposed by third parties (such as national laws) (Schrepel, 2019). And if the law becomes less efficient in its capacity to administer, governments will be forced to regulate by intervening into markets or by revising the code design. Within a decentralized context, states and governments would need to adopt a different approach to shape markets. As of today, marketplaces backed by DAOs will not allow government intervention (Schrepel, 2019). Laws which try to prevent anticompetitive practices, become more difficult to enforce. Besides, the open nature of blockchain-based applications lets anyone to reproduce or adjust most of them, for satisfying the interests of the different communities. In this regard, states can always adopt coercive measures in order to force users to update their clients (Schrepel, 2019). Yet, regulating a blockchain-based architecture can be a tricky task, since there is the concrete risk of undercutting the powerful interconnectivity of the Internet and the typical notions of free expression. For this reason, if we want to preserve the upsides provided by the blockchain technology while reducing to the minimum their possible drawbacks, we have to start thinking about a new law archetype. This new legal model should be able to balance the power of the Blockchain in such manners to promote economic growth, free speech, and the protection of individual rights and liberties (Becker, 2022).

2.4. The End of Antitrust Law?

Because blockchain is decentralized, anonymous, and immutable, questions arise regarding the ability to detect anticompetitive practices and their perpetrators. We show that some practices are de facto more likely to be implemented (Schrepel and Buterin, 2020).

Next, s current antitrust laws and how antitrust authorities should tackle these issues is a debate topic. On the one hand, regulators must avoid using their unfamiliarity with a new technology to justify over-regulating a potentially beneficial advancement or employing what this article calls the blockchain excuse for regulation. On the other hand, antitrust enforcement must adapt to stay relevant, and this article suggests that regulators adopt a new methodology of regulatory infiltration using a law is code approach (Schrepel and Buterin, 2020).

Third, even if this new regulatory scheme is adopted, some ultimate questions demand resolution. Nevertheless, the decentralized nature of blockchain forces us to consider the legitimacy of antitrust law, which rests on centralized legal structures and enforcement that are inconsistent with blockchain s trustless nature; although, antitrust is still needed. This is the blockchain antitrust paradox (Schrepel and Buterin, 2020).

3. METHODOLOGY

This dissertation is merely a product of meticulous desk study; a hybrid desk study that includes secondary data from scholarly publications and official governmental statutory law papers or opinions and research.

As no absolute control can be exercised on the way of data collection and conclusions extractions in secondary data, in order to safeguard the quality of the research, strictly scientific and governmental sources were chosen, i.e., from subscription-based portals, scientific books, governmental portals and recent, opinions of regulatory bodies. Any other internet source, whose validity and quality and age of content could not be guaranteed, was excepted from the literature review as well as from the case study.

4. DATA ANALYSIS SECTION A: THE EU REGULATORY FRAMEWORK ON SMART CONTRACTS TECHNOLOGY AND PARAMETERS

4.1. GDPR, Blockchain & The EU Single Market

Over the past few years, blockchain s potential for the EU s Digital Single Market has been at the center of many debates. By its nature, indeed, this technology seems to be unable to comply with the European data protection law. This paragraph aims to analyze the relationship between the blockchain technology and the GDPR (General Data Protection Regulation), pointing out the present tensions and the possible future solutions (Matsson, 2022).

The GDPR is based on the 1995 Data Protection Directive and became binding in the year 2018. On the one hand, it facilitates the free movement of personal data within the area of the European Union. On the other side, it institutes a legal framework for the protection of certain fundamental rights, which builds a set of obligations for data controllers (the bodies that determine the means of data processing). The aforementioned clashes between blockchain and GDPR depend on two preeminent elements. Firstly, the GPDR is based upon the principle for which, with respect to any personal data, there is (at least) one person (either natural or legal) whose data subjects can address to accomplish their rights. However, blockchains are designed to reach decentralization for replacing a single player with more actors. And this renders burdensome the allocation of accountability and responsibility in relation to the not-so-clear concept of “joint controllership” under the current regulation. For this reason, a further complication arises due to the loss of legal certainty concerning the definition of entities qualify as "joint controllers". Secondly, the GDPR is based upon the presumption that data can be modified or deleted whether necessary in order to comply with the legal requirements provided, for instance, by articles 16 (for which data must be amended) and (for which data, in some cases, must be cancelled) of the regulation. Such data modifications are made onerous by the blockchain not only in order to achieve trust in their network, but also for assuring data integrity. Nevertheless, the general uncertainty regarding blockchain technologies is boosted by the already existing uncertainties related to the current European data protection law (Matsson, 2022).

There is an ongoing debate with respect to when (hashed or encrypted) data stored on a distributed ledger can be qualified as personal data for the purpose of GDPR. Another example is referred to data minimization and purpose limitation. While GDPR requires that personal data must be processed just for means and purposes specified in advance, these two principles are arduous to apply to a blockchain technology, since DLTs are append-only databases which continuously grow as new data are added. Additionally, such data are replicated on several computers. Therefore, it is problematic from the data minimization s viewpoint, and it is unclear how the personal data processing s mean should be applied to the blockchain as well. The most debated aspect in relation to blockchain technologies is perhaps the "right to erasure" (also known as the "right to be forgotten"), since data modification complicated if not even impossible. Again, this is hard to conform with the requirements provide for by articles 16 and 17 of the GDPR (Ture, 2021).

4.2. Legal Nature of Blockchain and Bitcoin Transactions in the EU

Legal nature of blockchain transactions: this Principle was at the heart of several rounds of discussion among the Reporters and within the whole Project Team (European Commission, 2022; Garcia Teruel and Simón Moreno, 2021). The final conclusion was that the approach taken in Principle 5 is, indeed, accurate and reflects existing law, not only in B2B and B2G, but also in B2C relations. For commercial, financial and government relations, no doubts existed, given international practice, but the issue of how to ascertain existing and future consumer protection in particular was a point of grave concern. However, by formulating Principles specifically aimed at protecting consumers, the Project Team agreed that consumer protection could be more than adequately safeguarded. The discussions as to whether transactions or elements thereof can amount to an offer, acceptance or any other contractual declaration, centred around the European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)) and Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights. In this resolution, the European Parliament requests the European Commission: "*to in particular update its existing guidance document on Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights in order to clarify whether it considers smart contracts to fall within the exemption in point (l) of Article 3(3) of that Directive, and, if so, under which circumstances, and to clarify the issue of the right to withdrawal*." (European Commission, 2022; Garcia Teruel and Simón Moreno, 2021) Article 3(3)(l) of the Consumer Rights Directive reads as follows: "*This Directive shall not apply to contracts: […] (l) concluded by means of automatic vending machines or automated commercial premises*; (European Commission, 2022; Garcia Teruel and

Simón Moreno, 2021). The exception, however, does not refer to what is achieved with a Smart Contract, being a self-executing computer programme, but refers to instant contracting through a device such as vending or parking ticket machines. This is confirmed by the Guidance Document on the Consumer Rights Directive, which provides the following example: *This exception would apply to contracts concluded on automated commercial premises such as: Automated gas stations without the physical presence of the trader s representative for the conclusion of the contract*." The main question regarding the legal status, if any, of Smart Contracts is whether a Smart Contract can, as such (so without an already existing, underlying and preceding legally binding relationship) create a legally binding contract (European Commission, 2022; Tsindeliani and Egorova, 2020).

4.3. Smart Legal Contracts

A Smart legal contract is basic European framework for contract formation can be found in the Draft Common Frame of Reference (DCFR) (Dwivendi et al., 2021). The Reporters, therefore, took the DCFR as their overall accepted starting point for answering the question of whether a Smart Contract can be a legally binding contract. The reporters also took as their starting point that both subjects involved (natural and legal persons) and the object (what is agreed upon?) must be clear and that an automated process by itself, without creating clarity regarding subjects and object, cannot produce legally binding acts. The answer to the question above concerning the legal status of a Smart Contract might be different depending upon whether a consumer (B2C, G2C) or a professional party (B2B, B2G or G2G) is involved. The position of a consumer, entitled to pre-contractual information and post-contractual service given the consumer s unequal bargaining strength against a professional party, is different from businesses negotiating at arm s length. It is beyond any doubt that consumer protection is needed the more contract formation takes place by using algorithms, which, from a consumer s viewpoint, create a *black box* (Dwivendi et al., 2021; European Commission, 2022), making it impossible to fully understand the technical side of the transaction. Consumer protection which takes the specific algorithmic nature of a transaction into account can be secured in two ways: either by denying that a contractual relationship as such has come into existence, given that algorithms are as such neither readable nor understandable except by software developers and computer programmers, or by accepting that while a contract was concluded, the consumer is still entitled to protection, for example, a right to annul a clause or a right of withdrawal. The form of such right to annul or right to withdraw will, however, require adaptation given the technological environment in which this right must be made effective, compared to a right to annul or withdraw regarding contracts concluded through more traditional means, such as in writing. In both approaches, existing EU consumer law must be held against the light of how a Smart Contract functions. At the same time, it should be realised that it should not matter for the binding nature of a contract whether or not an e-commerce transaction takes place online, using Smart Contracts. The Smart Contract is the back side of the transaction and it is not in doubt that a contract can be concluded using software, such as buying goods in a web shop online or by exchanging e-mails. Analysing the various technical stages of a Smart Contract (source code, bytecode, blockchain) when a decision has to be made as to attaching legal consequences to what happens online was considered irrelevant. The question whether the law should focus on the formation process (e.g., is there an intention to create binding legal relations?) as such, or should rather focus on the fact that source code, and certainly bytecode, cannot be read and understood by human beings, particularly not a consumer can, of course, be asked.

However, this problem is not new and is not specific for the use of Smart Contracts. It has generally been accepted that e-commerce transactions are valid (Dwivendi et al., 2021; European Commission, 2022).

4.4. Triggering of Transactions

The triggering of a transaction, particularly a Smart Contract, on a blockchain has three aspects: the code which creates and, in fact, is the blockchain and that controls what is seen as a transaction, what that transaction may contain, when it is performed and what the outcome of that performance is; the Smart Contract, which is also computer code functioning within the blockchain, and what the parties off-chain intend to achieve with their contract (European Commission, 2022). In the case of a public blockchain, the participants have no influence as such on the code that governs the blockchain. When the blockchain is private, the code can be programmed in such a way that what future contracting parties want as to how the blockchain functions is taken into account (Borgogno, 2019). This also applies to Smart Contracts, but to a lesser degree given that the Smart Contract functions within an already coded environment. Parties will have to take the coded environment into account if they want to use such environment as a tool for their contractual arrangements. They can, of course, try to code their pre-existing off-chain contract and mould the Smart Contract according to their wishes, but even then, especially in the case of a public blockchain, the enforcement of such encoded law would fully depend on the code governing the blockchain and any Smart Contracts which are already part of that code. Contracts in the more traditional sense of the word, where the contracting parties are known and which are not fully dependent on code, but could be a mixture of code and human writing, can more easily be created if the blockchain is private. In that case, the participants who can take part in the consensus process are restricted and known (Borgogno, 2019).

4.5. Transparency of intention to create legal relations

The intention to create legal relations, expressed in the process of offer and acceptance, must be transparent to both parties (Green and Sanitt, 2019). Such transparency can be facilitated by ensuring that the offer and acceptance reach the other party (to avoid the occurrence of transactions of which the other party is unaware and did not signal any consent) or is accessible off-chain. This also solves any problems regarding the evidence of such transactions. If no explicit agreement between the parties involved exists, dispositive law applies. This raises the question of which law then governs, a question of private international law. This is still a very unclear and heavily debated area where the Principles only take a careful position (European Commission, 2022). However, choice of law and choice of forum should be possible, allowing parties to decide for themselves which dispositive law applies, of course within the confines of public (international) law and public policy (ordre public) (European Commission, 2022). It should also be taken into account whether the parties are both businesses or whether one of the parties is a consumer. In the latter case, consumer protection must be safeguarded, irrespective of the fact that the transaction takes place in a coded environment (Green and Sanitt, 2019).

4.6. Public blockchains

when parties use a public blockchain, it is just as important as in the case of private blockchains that declarations of intent may only trigger legal consequences if: (i) the recipient has actually received them; or (ii) the transactions are either securely stored in the blockchain (i.e., cannot vanish in an orphan block) or securely stored off-chain. Within a coded environment, receiving a declaration of intent will mean having access to it, to which should be added having information about such access. A so-called orphan block is a block that is recognised by the blockchain (when two blocks are validly mined simultaneously) but was not accepted. How blockchains deal with orphan blocks may differ from blockchain to blockchain. In the absence of such agreement, dispositive law is applicable, whereby this can easily result in default of one party (eg in case declarations of intent vanish due to orphan blocks). The difficulty here is that this will all depend on the code, which for the parties will be a given fact. Whenever a consumer is a party to such a contract, the position of the consumer must at least be equal to their position in an off-chain transaction. This could imply that, when such protection cannot be offered on-chain because of the code which governs the transactions, the rights of the consumer must be restored through an off-chain contract (Yang et al., 2020; European Commission, 2022).

4.7. Functional equivalence and technological neutrality

The EU ELI Principles are based on the need for functional equivalence and technological neutrality (European Commission, 2022). These aspects, although closely related, are not the same. Functional equivalence means that solutions which are legally binding under already existing (off-chain) law should also be legally binding when new technology is being used. A question, for example, is whether a blockchain transaction, given its immutability and time stamp, could be seen as the functional equivalent of an authentic document. If the answer is in the affirmative, this does not immediately imply that civil servants or (civil law) notaries no longer have a role to play (De Filippi et al., 2022). Often, civil servants, (civil law) notaries or financial institutions are involved in cases where not only the authenticity of parties has to be established, but also other protective purposes are pursued (e.g., civil law notaries often have to fulfil certain legal obligations to explain and financial institutions have duties under their Know Your Customer obligations). Also, with blockchain technology, there could be the problem that the private key to an identity could be stolen or hacked, whereas, in such cases, the authenticity of the holder of the private key to the identity would no longer be valid. Such risk of identity theft could be lower when civil law notaries are involved (although here, too, there is the risk of people forging IDs or similar) (European Commission, 2022). Blockchain technology can be a perfect tool to provide evidence and secure archiving, but the input still may have to be done by a person whose integrity and knowledge is beyond doubt. In other words: disintermediation may happen, but not necessarily so, even when blockchain technology is seen as functionally equivalent to an authentic document. A solution is technology neutral if it applies to and regulates relationships irrespective of the technology used (De Filippi et al., 2022). Blockchain technology as we know it today may (and perhaps will) develop further and a solution would then be technologically neutral if these new developments are also covered by existing law. Such law may then achieve functional equivalence, but as a result of technology neutral law (European Commission, 2022).

4.8. Consumer & Weaker Party Protection

Consumer protection is at the forefront of European law, as part of a broader framework to protect fundamental rights of European citizens (European Commission, 2022). That framework also applies to the rights of European citizens, and hence consumers, in our rapidly developing and fast-growing digital economy, as expressed in the recently published European Declaration on Digital Rights and Principles for the Digital Decade. A preliminary question is how to define consumer in a digital setting. The Principles are based on existing, and more traditional, concepts of consumer and B2C transactions and thus are founded on the existing European Union acquis communautaire. Even if the definition of consumer may vary from one Directive to the other, the most recent definitions all tend to be similar: *any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person s trade, business, craft, or profession* (Article 2[6] Directive 2019/779/EU). Nevertheless, it should not be forgotten that, in an algorithmic environment, the aim and scope of the Principles might have to go beyond the classical concepts of consumer protection and might, for example, also apply to Peer-to-Peer (P2P) transactions.

P2P may reveal different structures, such as a consumer (designated then as prosumer) acting with another consumer. In this situation, the consumer is not so much being protected against a party with a stronger bargaining position, but rather against the technological tool (for example, a P2P transaction or platform) used, even though the counterparty may also very well be a consumer; or one party may be a small- or medium-sized enterprise (SME) and the counterparty a larger business.

Another aspect here is the question how to approach businesses which may pose as a consumer? (European Commission, 2022) A reply could be that identifying the status of a contracting party (consumers versus businesses) is not only difficult in a blockchain context, but also in other, more traditional, contexts and therefore not a specific problem caused by an IT setting. At the same time, it must be admitted that it certainly is a problem in the platform economy (European Commission, 2022). The Modernisation Directive addresses that issue by inserting in Article 7(4) of the Unfair Commercial Practices Directive that a provider of an online marketplace must be informed by a third party whether that third party acts as a trader or non-trader. Inspiration could also be drawn from the protection of consumers involved in investment transactions (European Commission, 2022). The Markets in Financial Instruments Directive (MiFID II) qualifies clients according to their different levels of experience, knowledge and expertise and categorises them as either non-professional or retail clients, professional clients or eligible counterparties (European Commission, 2022). A professional client is a client who possesses the experience, knowledge and expertise to make its own investment decisions and properly assess the risks that it incurs. The protection level is the highest for retail clients, is intermediate for professional clients (such as investment firms) and the lowest for eligible counterparties (for example governments).

In these Principles, EU primarily focuses on consumers (thus non-professional or retail clients), more in line with the Proposal for Markets in Crypto-assets Regulation. In Article 3(28) of this proposed Regulation, a consumer is defined, as can generally be found in the EU acquis communautaire, as meaning *any natural person who is acting for purposes which are outside his trade, business, craft or profession*. It was considered to introduce new terminology here. Such an approach can be found in the revised Package Travel Directive, which introduces the new legal category of traveller, but that Directive, according to its considerations, after all, still aims to protect consumers. It seems that internal consistency with the proposed Markets in Crypto-assets Regulation is, at least for the moment, the better workable approach.

However, although the primary focus of these Principles is on consumers, it should also be realised that micro-, small- or medium-sized enterprises (SMEs), next to tenants and employees, might be in the same dependent position as a consumer. With regard to SMEs, this becomes very clear when looking at the recently presented proposal for a Data Act (European Commission, 2022). The proposal in its Article 13 provides protection of these enterprises against unfair contractual terms in agreements between enterprises unilaterally imposing their own terms and conditions on their weaker business counterparts concerning the access to and use of data or the liability and remedies for the breach or the termination of data-related obligations. Article 13 then follows a structure, well-known from consumer law, which, after first defining in an open-ended norm what unfair means (European Commission, 2022), then makes unfairness more explicit by adding a blacklist and a grey list of unfair clauses. However, the Principles in this Part II only deal with consumers, as already referred to in the Explanatory Notes under Principle 12 on weaker parties. It has to be analysed whether the approach taken herein could also be applied to weaker parties in general. Micro-, small- and medium-sized enterprises, for example, might be in the same dependent position as consumers, both regarding their bargaining power as well as their knowledge (European Commission, 2022).

5. DATA ANALYSIS SECTION B: THE CASE OF GREECE

5.1. Current Background

The Greek blockchain market today mainly evolves around cryptocurrencies. Although there are no official statistics, it appears that a significant number of people, comparable to other European markets, exchange fiat currency with cryptocurrencies, mainly via cryptocurrency exchanges operating globally over the internet, but also through a network of physical cryptocurrency ATMs. Some retailers accept payments in cryptocurrencies, but actual use of crypto as a means of payment is extremely limited. While blockchain technology exists in the public and academic domain, there have not yet been any large-scale applications. The Hellenic Blockchain Hub (a non-profit organisation of executives from the public and private sector aimed at the dissemination of knowledge on blockchain and DLT technology and supported by various businesses and academic institutes, including the Hellenic Federation of Enterprises) has entered into memoranda of co-operation with various organisations, recently including the Supreme Council for Personnel Selection (ASEP). The use of cryptocurrencies and other digital assets is expected to expand over the coming months, following global trends, including NFTs and potential market participants offering innovative services to attempt entering the Greek market. Regulatory certainty will definitely facilitate such efforts and support innovation in blockchain applications in general. The recent introduction of a special digital wallet provider and cryptocurrency exchange registry by the Hellenic Capital Markets Commission (HCMC) is an important step towards regulatory transparency in the Greek blockchain market, but more certainly needs to be done, especially with respect to the proper regulation of digital assets themselves. As an EU Member State, Greece will follow any EU initiatives, including the EU Commission proposals for a new EU law on crypto assets (Hellenic Blockchain Hub, 2022).

Greece is home to an emerging blockchain ecosystem, populated by well- established businesses and organisations, start-ups, as well as of official and unofficial communities of practice which constitute the primary facilitator of education and discussion in the field, due to the lack of relevant state-backed or industry initiatives.
However, the ecosystem is in its infancy. The focus in the use of blockchain has been placed mainly by FinTech and RegTech Startups, but there have been also blockchain based tech Start Ups in the fields of Energy and ClimateTech Moreover, Greek blockchain software engineers have been active in the international ecosystem, attracting Greek establishments of international blockchain companies in Greece (such as Mysten Labs) (Hellenic Blockchain Hub, 2022).

Founders of Greek blockchain companies are typically entrepreneurs or researchers with strong academic backgrounds and international experience. Due to the relatively small size of the domestic market for blockchain, companies at large develop solutions that correspond to the needs of international customers and markets.
More precisely, there are:

- Blockchain & Web3 companies, based in Greece or with Greek establishment (founded by Greeks) with applications, among others, in:
    A. Fintech (Nayms, Wire)
    B. EnergyTech (Gridustry)
    C. ClimaTech (Weather prediction (WeatherXM)

- Few NFT Marketplaces and a community of NFT investors while a major cultural institution such as the Onassis Foundation has been actively exploring the NFT ecosystem, promoting use of NFTs in artistic creations (Hellenic Blockchain Hub, 2022).
- Active adoption of Blockchain in Fintech used by credit institutions and other financial organizations, with significant cases having requested regulatory advisory support by the Bank of Greece s (BoG) Fintech Hub the *FinTech Innovation Hub* (*according to BoG s FinTech Innovations Hub s Annual Report_2021, – where Blockchain is defined as Distributed Ledger Technology – the prevailing issues in enquiries were specifically referred to innovative technologies concerned Distributed Ledger Technology (DLT) (36%).* (Bank Of Greece, 2022)
- An active blockchain community, the Hellenic Blockchain Hub (founded in 2018). Hellenic Blockchain Hub is a non-profit network of executives from the public and private sector aimed at (a) the dissemination of knowledge on the blockchain – DLT technology, (b) the promotion of blockchain technologies in important sectors of the economy and society, (c) the creation of a permanent mechanism for consultation with the Greek State and European institutions on institutional interventions or synergies,(d) networking and synergies with collective bodies and policy makers, and equivalent Greek and foreign bodies, (f) the utilization of research and development (Hellenic Blockchain Hub, 2022).
- Greek Fintech Hub: Six key Greek bodies are taking part in an initiative aiming at showcasing the fintech landscape in Greece: National Bank of Greece together with Endeavor Greece, the Onassis Foundation, the Hellenic Chamber of Hotels, the National & Kapodistrian University of Athens, and the Athens University of Economics & Business. And together with these institutions, the

European Crowd Dialog initiative. A series of actions have been designed to strengthen entrepreneurship in Fintech, finance innovative businesses in the sector, link Fintech with research in universities and research centres, and inform and network with important networks and initiatives abroad (Greek Fintech Hub, 2022).

- Blockchain research is carried out by several members of the Greek academia and research community (Greek Fintech Hub, 2022).

5.2. ESG Regulations Compliance

So far neither the regulatory authorities (such as Capital Market Commission and Athens Stock Exchange nor the business practice acknowledge or refer to blockchain technology applicable in relations to ESG. In the Athens Stock Exchange 2022 ESG Reporting Guide there is not such reference to Blockchain. There is theoretical interest and possible proposals which are still at research level, but there is neither a strategy on how to adopt the technology considering ESG issues, nor tangible results in daily use. As the technology is in its infancy and given the potential negative environmental impact, regulatory frameworks and guidelines are necessary to foster environmental sustainability. As of now, there is not yet any outcome, proposal, direction, or regulation to this regard (Athens Stock Exchange, 2022).

5.3. Legislation and Regulatory Bodies

In July 2022, *Law 4961/2022 on Emerging Information and Communication Technologies, enhancement of Digital Transformation and other provisions (the Law on Emerging Technologies)* was published in the Governmental Gazette. Article 31 of the New Law provides a definition on Blockchain and DLT Technologies, whereas Chapter E (Articles 47 – 51) contains provisions regarding the *Application of Distributed Ledger Technologies* (D.L.T). More precisely, Articles 47-48 contain provisions regarding the validity of a record on the Blockchain or other DLT Technology, the enforceability of a Blockchain or DLT Technology transaction *per se*, as well as the allocation of the burden of proof regarding (the existence of) records or transactions performed on the Blockchain or other DLT Technologies (Bank of Greece, 2022; Greek Fintech Hub, 2022).

With the enactment of the New Law on Emerging Technologies (Law No 4961/2022), it is acknowledged that a framework regulating the use of Blockchain and DLT Technologies will ensure legal certainty and enhance trust, foster innovation for projects based on Blockchain and other DLT Technologies and will attract more investors. Emphasis has been placed in policymaking by Government bodies, such as the Ministry of Tourism, on the Blockchain Ethical Design Framework, to safeguard social values (Bank of Greece, 2022; Greek Fintech Hub, 2022).

The abovementioned provisions of the New Law (Bank of Greece, 2022; Greek Fintech Hub, 2022):

(a) make reference to Greek Civil Law provisions regarding the invalidity of transactions,

(b) acknowledge that a Blockchain (or other DLT Technology) record could be part of a main contract conducted by other means,

(c) provide that in case that a Blockchain record is declared invalid, the Court could rule for restitutio in integrum by way of either amending the record on the Blockchain or by way of compensation, and
(d) allocate the burden of proof among the parties, by indicating that the party relying on or invoking the existence of a recording or a transaction, bears the responsibility of submitting the relevant data and information to the court; following the transformation of the programming language or code into a readable format, evidence can be submitted in court proceedings, subject to a report of a cryptography expert.

Articles 49-51 of the Law, refer to smart contracts.

Law 4557/2018 *on preventing and combatting money laundering and terrorist financing" as amended by Law 4734/2020 (the AML Law)*, provides a definition on virtual currencies and sets obligations on providers engaged in exchange services between virtual currencies and fiat currencies as well as to the custodian wallet providers (Bank of Greece, 2022).

There is no other legislation or regulatory framework in Greece specifically relating to Blockchain or other DLT Technologies. Nevertheless, several existing laws and regulations are applicable to products/ services and activities/ operations based on or use Blockchain or other DLT Technologies (Bank of Greece, 2022).

In December 2020, the Ministry of Digital Governance issued *The Digital Transformation Strategy 2020-2025 of Greece, the so-called Digital Bible*, which is the main strategic document, that sets priorities and goals for the digital transformation of the country. The Digital Bible includes provisions for the usage of Blockchain and DLT

Technologies in the Public Sector, as a tool for digital transformation, emphasising on their use in the digitization of public contracts, storage of digital fingerprints of public documents, for public document and certificates verification, for health data management, for the supply chain etc (Greek Fintech Hub, 2022).

The Hellenic Capital Market Commission acknowledges the challenge of crypto assets and adopts the European Securities & Markets Authority (ESMA) 2022 Risk Analysis on *Crypto-assets and their risks for financial stability*. At the same time, it provides warnings to the investors (public) in relation to several cryptocurrencies vendors and underlines the risks involved in this non- regulated activity (Greek Fintech Hub, 2022).

The Bank of Greece (BoG) acknowledges the use of blockchain technologies as part of fintech adopted by Greek financial institutions (as noted in the Bank of Greece s (BoG) Fintech Hub Annual Report).

The National Cyber Security Policy recognises Cryptojacking as a cybersecurity issue and provides for measures to prevent and or tackle cryptocurrency fraud (Greek Fintech Hub, 2022).

As far as centralized regulatory encouragement is concerned, all the above are spurred from the fact that Greece is a signatory to the European Blockchain Partnership (Greek Fintech Hub, 2022).

Bank of Greece has set up a Regulatory Sandbox (the BoG’s Regulatory Sandbox), (established and operating by virtue of the Executive Committee Act

189/1/14.05.2021), which constitutes a mechanism that enables participants to carry out small scale testing of innovations, in a controlled regulatory environment, within specified parameters and timeframes under the BoG s supervision and in direct cooperation with the BoG. BoG acknowledges that Tokenisation, Blockchain and Distributed Ledger Technology (DLT), as well as Smart Contracts are innovative technologies and solutions which may be used by prospective Applicants within their propositions (Bank of Greece, 2022).

Despite all the above, there has been no official guidance on the use of Blockchain Technology up until nowadays in Greece. So far, there have been only some preliminary definitions as well as warnings (Athens Stock Exchange, 2022).

There is no Law in Greece to explicitly ban the use and trade of cryptocurrencies, however, we do not have as of now, one piece of legislation dedicated to the financial regulatory treatment of cryptocurrencies. Art. 3(24) of the national Law 4557/2018 *on preventing and combatting money laundering and terrorist financing* as amended by Law 4734/2020 (the AML Law), in the definition on virtual currencies, underlines that virtual currencies "*constitutes the digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by both physical and legal persons as a means of exchange which can be transferred, stored or distributed electronically*" (Athens Stock Exchange, 2022).

On two occasions, in 2014 and in 2018, the Bank of Greece (BoG) issued announcements warning the public of the potential risks associated with digital currencies. On the same note, on three occasions, in 2017, 2018 and 2021, the

Hellenic Capital Market Commission (HCMC) communicated to the general public the warnings of ESMA on ICOs, ESMA/EBA/EIOPA on virtual currencies and ESMA on non-regulated crypto assets, highlighting the potential risks associated with them. The Hellenic Capital Market Commission in its recent announcement to the general public (dated on 13.10.2022), underlined that does not regulate crypto assets market, nor the investment on crypto assets (Bank of Greece.

It shall be noted that Law 4514/2018 (that has implemented Directive 2014/65/EU on markets in financial instruments (MiFID II), requires entities that provide investment services or the carrying out of investment activities to obtain a license from the Hellenic Capital Market Commission or the corresponding supervisory authority of another EU Member State. Provision of investment services without such a license, constitutes an offence, which carries severe criminal and administrative sanctions. The HCMC draws the attention of investors to the assessment of companies (with which they intend to cooperate or are cooperating) with regard to their authorisation and supervision regime.

Yet, with respect of the crypto/ blockchain financing and according to guidance from the European Securities and Markets Authority (ESMA), firms give careful consideration as to whether their activities constitute regulated activities. If their activities constitute a regulated activity, firms must comply with the relevant legislation and any failure to comply with the applicable rules would constitute a breach.

The MiCA & DORA regulation proposals which aim at establishing a European-wide definition of crypto assets, and crypto asset service provider and which will set a

European passport and a crypto asset issuer regime, will provide the necessary legal certainty to the participants of the crypto-ecosystem (CASPs, investors, issuers, etc.).

5.4. Taxation

There is not as of today a special tax regime in the Greek Tax Legislation that governs the profits that taxpayers acquire from crypto currencies capital gains, or generally of the trade/ investment of cryptocurrencies. Those profits, however, constitute income subject to taxation and all provisions regarding tax evasion subject to Law 4174/2013 (art. 66 et seq) apply to any undeclared income from cryptocurrency transactions gains (publicrevenue.gr, 2013).

The Independent Authority for Public Revenue (AADE) of the Hellenic Republic, in its operational plan for 2019, takes a first approach by treating the institutionalisation of the taxation of cryptocurrencies as a portfolio investment. Given the intention of the AADE and in the absence of specific legislative provisions, the AADE considers the above income to be capital gains and will be taxed in accordance with Article 43 of the Income Tax Code a rate of 15%. It is worth noting that these incomes are also subject to solidarity levy since there is no explicit exemption for them in the tax legislation (gov.gr – taxation, 2022).

As far as the tax regime applicable to the issuers of cryptocurrencies is concerned, there are no tax and accounting guidelines, but only the Memorandum 104/27.02.2018 by the Accounting Standards Board (Σ.ΛΟ.Τ), according to which the issuers income out of the trade of cryptocurrencies, constitutes income deriving out of commercial activity and therefore is subject to taxation (gov.gr – taxation, 2022).

Finally, with regard to the use of cryptocurrencies as a mean of payment no additional tax is imposed (decision C-264/14 ECJ) (gov.gr – taxation, 2022).

5.5. ICOs

There has not been an ICO in Greece as of today.

Yet, with respect of the crypto/ blockchain financing and according to guidance from the European Securities and Markets Authority (ESMA), firms give careful consideration as to whether their activities constitute regulated activities. Namely, where the coins or tokens qualify as financial instruments it is likely that the firms involved in ICOs (or similar) conduct regulated investment activities, such as placing, dealing in, or advising on financial instruments or managing and marketing collective investment schemes. Moreover, they may be involved in offering transferable securities to the public. In such case, they need to contact the national competent authorities (Anthimos, 2022).

Under the light of the AML Law, an ICO may be considered as a service relating to crypto assets and the entity proceeding with such an ICO may be subject to registration and organizational compliance as a Crypto Assets Service Provider (CASP).

In more detail, there is no legal provision in the Greek regulatory regime that pose a ban on the ICOs. In principle, ICOs are unregulated in the sense that there is not overarching laws imposing legal and/or regulatory requirements on the activity of launching or running an ICO. When launching an ICO, depending on its structure (i.e nature and categorization of the tokens) the following shall be taken under consideration on a case- by- case basis (Kourbetis, 2020; Anthimos, 2022):

- Where the coins or tokens qualify as financial instruments, it is likely that the firms involved in ICOs conduct regulated investment activities, such as placing, trading in or advising on financial instruments or managing or marketing collective investments schemes, in which case the MiFID II applies.
- Where the ICO structure resembles or involves the offering of transferable securities to the public, the Prospectus Directive (EU) 2017/1129 (implemented in national legal system with Law 4706/2020) may apply, which requires publication of a prospectus (subject to exemptions) with the necessary information and material for investors to conduct an informed assessment.
- Where the ICO qualifies as an alternative Investment fund, then the Alternative Investment Fund Managers Directive (AIFMD) (EU) 2011/61 (implemented in national legal system with Law 4209/2013), imposing operational and organisational rules and transparency requirement, may apply.
- Utility tokens, i.e., tokens intended to provide access to a digital application or service using a blockchain, may in principle fall outside of current financial and securities regulation. Attention shall be given to utility tokens that cannot be used as such at the point in time of issuance, it must be considered a security.
- Compliance with AML Laws shall always be ensured as it is important to identify whether the issue of the token is an obliged entity that need be Registered with the HCMC.

- Tax Laws shall be taken under consideration applicable to issuers and investors.
- Contract Laws, Consumer Laws, Data Protection Laws, IP Laws, Competition Laws as well as Civil Law referred to the sale of goods, or Property Laws are applicable

5.6. Transfer of Titles and Freedom of Contract

Greek Civil Law (art.361) provides for the freedom of contract, therefore parties to a transaction are free to agree on transfer of title (provided that such arrangements do not conflict with any mandatory rules of law). There is no framework regarding the transfer of title to or the granting on security over tokens and virtual assets specifically. As long as there is no certificate or title attached to a token, a transfer is subject to assignment of the rights attached to a token. Issues may arise in relation to the transfer of claims against a particular issuer represented in a digital asset, in which case it shall be assessed whether a transfer of such a claim can be fulfilled by a mere blockchain or other DLT transaction. In addition, the transfer of certain type of assets, such as real estate, shares etc. shall be subject to a notary deed according to Greek Laws, therefore a token transfer of those kind of assets does not fulfil the conditions of a valid transfer (Kourbetis, 2020).

5.7. Smart Contracts in the Greek Legal System

A definition for smart contracts was recently introduced for the first time in Greece (Law 4961/2022 on Emerging Technologies) providing that a smart contract is a "*set of coded computer functions concluded and executed through Distributed Ledger Technology in automated electronic format with the use of instructions on the performance of actions, omissions or tolerance, which are based on the existence or absence of specific conditions, according to terms directly recorded in computer code, programmed commands or a programming language*" (Kourbetis, 2020).

The new Law contains provisions on the elements that qualify a data record in the blockchain or other DLT as a smart contract, the conclusion, validity and evidentiary effect of smart contracts and their enforcement both by the parties involved and the courts. In a nutshell, smart contracts in Greece (Papantoniou, 2020):

- are legally binding terms agreed upon among the parties recorded as data and/or transactions in the blockchain or other DLT-based applications (terms can be determined by the parties and coded into the computer program or they can be selected / approved by the parties from a pre-selected set of terms).
- Their validity and enforceability are subject to the interpretation of the law and the courts, which, essentially, indicate that a smart contract is valid so long as it meets the criteria set out in the Civil Code and the Code for Civil Procedure, which are the cornerstones for contract law in Greece.
- Where signature is required for the conclusion of a contract, the Law also provides for their signing via electronic signatures.
- Smart contracts can be part of other (traditional) contracts, drafted according to the law.

Given, however, the very recent entry into force of the new Law, academic literature and jurisprudence are not yet rich regarding the enforceability of smart contracts, as compared with traditional ones. Some of the interpretation issues that the legislator and the courts will need to shed light on, include provisions relating to the means of restitution available to the parties. For example, the Law provides for restitutio in integrum in case a smart contract (and the corresponding transactions) is declared invalid or unenforceable. Enforcing this provision is, however, highly challenging, given the nature of the blockchain (and the whole essence of DLT-based technology) which requires that the chain of blocks is *unbreakable* and untampered with, to ensure the continuity and validity of the rest of the recordings (let alone the environmental impact of repeated registrations and de-registrations, that require an excessive number of resources and energy) (Kourbetis, 2022).

Moreover, all on – chain concluded contracts are regarded as contracts conducted by distance means, therefore distance contract consumer protection legislation will be applicable where one of the parties acts under its capacity as a consumer. To this regard issues related to unfair terms, cooling off period, right to withdrawal etc. will face the challenge of enforcement (Kourbetis, 2020).

Furthermore, Smart Contracts and decentralised finance protocols are not that common in Greece as of today, -only few Start-ups are experimenting their use (i.e., gxblocks). The inclusion of Smart Contracts in the Greek legislative regime will create the basis for their use in our jurisdiction. Considering that decentralized finance protocols are not organized under a specific jurisdiction’s legal regime, it is not always evident to determine whether any such cases exist in Greece (Kourbets, 2020).

No key initiatives concerning the use of smart contracts, such as decentralised financial protocols, have been launched as of today (Anthimos, 2022).

5.8. Judicial Consideration

As of today, there is only one court decision regarding Bitcoin (Decision No 88/2021 of the Court of Appeal Western Central Greece which uphold the Decision No193/2018 of the Court of First Instance).The Appeal Court in year 2021, in upholding the first instance decision as per above, it held that, within the framework of the New York International Convention of 1958, which Greece has ratified since 1961, the recognition and declaration of enforceability of an American arbitration award awarding damages in bitcoin, violates the public policy of our country. The main rationale of the decision is that cryptocurrencies, (such as bitcoin), favour tax evasion and facilitate financial crime, causing uncertainty in commercial transactions, while at the same time, they bring harmful consequences to the detriment of the national economy. The Court of Appeal concludes its reasoning with the following considerations: The recognition of a foreign arbitral award that treats bitcoin as a decentralized monetary unit of peer to peer and orders the payment of a specific amount in bitcoin, is contrary to public policy, and in particular, to the fundamental rules and currently prevailing principles of the Greek legal order at the social, economic and political level. Finally, encouraging such transactions, as well as supporting their equation with those taking place in officially recognized currency units, would have the consequence of disrupting the prevailing economic conditions of the country, given the sudden and unpredictable fluctuation of the value of bitcoin (Anthimos, 2022).

The Court of Appeal in its judgement did not follow the developments in the cryptocurrencies between 2018 (decision of Court of First Instance) and its judgment in 2021 and it is most likely that the judgment will be considered obsolete in the coming years (Anthimos, 2022).

5.9. Other Applicable Legal and Regulatory Bodies

As mentioned earlier, a whole set of laws shall be under consideration by corporations operating blockchains or building applications (products/ services on blockchains. In particular, and indicatively (Papantoniou, 2020):

- Data Protection Laws: The application and enforcement of GDPR is a challenge for blockchain vendors. It is not easy to identify the Data Controller, who is the obliged entity to comply with the said Regulation, due to the diversity of actors involved in a blockchain and its decentralized nature. It is not feasible in many cases to demonstrate the privacy by design of a blockchain application, impossible to fulfil the right to erasure or to revoke a consent or safeguard the purpose limitation principle as blockchain by its nature processes all data recorded in the blocks perpetually.

- IP Laws: for instance, in the domain of the NFTs, trademark protections shall be extended to cover the digital assets represented by NFTs, or licensing issues defining ownership in the NFTs.
- Consumer Protection Laws, for instance to the extent a party to a smart contract acts under its capacity as a consumer.
- Advertising Laws, to the extent crypto assets are considered financial products.
- Property Laws in cases for example where blockchain products constitute financial instruments such as securities or when they concern real estate in which case specific property law requirements regarding the transfer of ownership, shall be taken under evaluation.

6. DISCUSSION & PROPOSALS FOR FURTHER RESEARCH

6.1. The Greek Environment

Considering all the above, with special regard to Greece, despite its developing crypto-ecosystem, cryptocurrency trading and smart contracts are not that common as of today, compared to other jurisdictions. There are not any notable cryptocurrencies vendors that are engaged to any of the activities connected to the cryptocurrencies. Nor has there been any licensed entity. There is a number of Start-ups participating in the BoG s Innovations FinTech Hub, some of which are intended to explore the related technologies. Mainstream financial institutions have not adopted any cryptocurrency solution; however, they are called to adopt to the new developments in any manner.

The Greek blockchain and cryptocurrency ecosystems will benefit at large from the DLT Pilot Regime Regulation (DLT PRR), which, together with the proposal for a bespoke regime for crypto assets (such as the Regulation for Markets in Crypto Assets (MiCA) which will provide the necessary legal certainty to the participants of the crypto-ecosystem (CASPs, investors, issuers, etc.), will provide appropriate levels of consumer and investor protection, legal certainty for crypto-assets, will enable innovative firms to make use of blockchain, distributed ledger technology (DLT) and crypto-assets while at the same time will ensure financial stability.

Till the adoption of all specific legislation that is currently under way, and which will shed light to legal uncertainties (i.e., MiCA, DORA, DLTR etc.), to ensure compliance with the applicable laws and regulations, a case-by-case assessment is of paramount importance to evaluate the nature and characteristics of a given product/ service has been designed on the basis of blockchain or related technologies.

A final point to consider, is the legal measures to take under consideration, in order to safeguard enforceability of an arbitration decision as per the usual T&Cs in the cryptocurrency trade platforms and determine the competent courts/ jurisdiction.

6.2. Global Measures of Importance for Future Research

Notwithstanding the legal insufficiencies about cryptocurrencies and Smart Contracts, one should not forget that the whole blockchain and the activities and products therein are largely based on technological development, which, on turn, shall aim for enhanced transactional security at a worldwide level.

In this context, the following proposals for future research are made:

(1) Key generation and key management addressing their use, strength, storage, loss and theft;

(2) Privacy/encryption related challenges to provide lawful access to transactions;

(3) Code review of Blockchain applications to include Software Development Lifecycles and penetration testing;

(4) Smart contract management by monitoring the behaviour of contracts and mitigating the risk of vulnerable contracts.

Taking the above into account, the legal systems at a worldwide level shall be eased further to commove with developments, as markets will operate with greater inherent safety and security and consequent stability, despite of their decentralisation.

7. CONCLUSIONS

This dissertation aimed to explore the field of cryptocurrencies and smart contracts mainly from a legal perspective. The developing regulatory framework and the challenges thereof was discussed, particularly in relation to Ethereum as compared to Bitcoin. The theoretical part of the dissertation examined basic definitions, outlined the profile and function of the cryptocurrency and blockchain environment, as well as address the fundamental legal issues arising from smart contracts. In the empirical part of the dissertation, the perplexing and sometimes, insufficient legal framework both in the EU and in Greece will be brought forward as a practical case study. Individuals and companies interested in developing crypto-related activities in Greece recognise that this sector is mostly unregulated, although some rules of law do apply to crypto users. According to the views of the Hellenic Capital Market Commission, cryptocurrencies are not currency, but rather portfolio assets. At the moment, the Greek authorities have transposed in the national legislation the EU s AMLD5 (Anti-Money Laundering Directive) (Haffke et al., 2020).

Still, a lot of questions remain to be answered. The current legal and regulatory framework is nascent, presenting significant legal gaps regarding cryptocurrencies and smart contrast in theory and practice. However, there are indeed viable proposals for further research and application.

8. BIBLIOGRAPHY

Athens Stock Exchange. 2022. ESG Reporting Guide 2022. [online]. Available at: https://www.athexgroup.gr/documents/10180/6599246/ESG+Reporting+Guide+2022-2202.pdf Last Access: 30/12/2022

Anthimos, A. 2022. Bitcoin and public policy in the field of international commercial arbitration. [online]. Available at: https://conflictoflaws.net/2022/bitcoin-and-public-policy-in-the-field-of-international-commercial-arbitration/ Last Access: 30/12/2022

Anush, B., Inna, G., Petrovich, D.O. and Tetyana, B., 2021. Comparative and informative characteristic of the legal regulation of the blockchain and cryptocurrency: state and prospects. Annals of the Romanian Society for Cell Biology, pp.5014-5028.

Argelich-Comelles, C., 2020. Smart Contracts O Code Is Law: Soluciones Legales Para La Robotización Contractual (Smart Contracts or Code Is Law: Legal Remedies for Contractual Robotization). InDret, 2.

Baker, H.K., Nikbakht, E. and Smith, S.S. eds., 2021. The Emerald Handbook of Blockchain for Business. Emerald Publishing Limited.

Bank Of Greece. 2022. Fintech Innovation Hub Annual Report 2021. [online]. Available at: https://www.bankofgreece.gr/en/main-tasks/supervision/fintech-innovation-hub Last Access: 30/12/2022

Becker, K. 2022. Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries. Law and Critique, 33(2), 113-130.

Borgogno, O., 2019. Usefulness and dangers of smart contracts in consumer and commercial transactions. A modified version is forthcoming in “Smart Contracts and Blockchain Technology: Role of Contract Law", L. DiMatteo, M. Cannarsa & C. Poncibo eds (Cambridge University Press, 2019).

Burniske, C. and Tatar, J., 2018. Cryptoassets: The innovative investor s guide to bitcoin and beyond. New York: McGraw-Hill Education.

Chen, J., Xia, X., Lo, D., Grundy, J. and Yang, X., 2021. Maintenance-related concerns for post-deployed Ethereum smart contract development: issues, techniques, and future challenges. Empirical Software Engineering, 26(6), pp.1-44.

Chohan, U.W., 2022. A history of bitcoin. Available at SSRN 3047875.

De Filippi, P., Mannan, M., & Reijers, W. (2022). The alegality of blockchain technology. Policy and Society, 41(3), 358-372.

De Filippi, P., Wray, C. and Sileno, G., 2021. Smart contracts. Internet Policy Review, 10(2).

De Graaf, T.J., 2019. From old to new: From internet to smart contracts and from people to smart contracts. Computer law & security review, 35(5), p.105322.

Drummer, D. and Neumann, D., 2020. Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. Journal of information technology, 35(4), pp.337-360.

Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A. and Draheim, D., 2021. Legally enforceable smart-contract languages: A systematic literature review. ACM Computing Surveys (CSUR), 54(5), pp.1-34.

European Commission. 2022. Commentary on ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection

Garcia-Teruel, R.M. and Simón-Moreno, H., 2021. The digital tokenization of property rights. A comparative perspective. Computer Law & Security Review, 41, p.105543.

Greek Fintech Hub. 2022. Homepage. [online]. Available at: https://www.fintechhub.gr/ Last Access: 30/12/2022

Green, Sarah, and Adam Sanitt. 2019. "The Contents of Commercial Contracts: Smart Contracts." The Contents of Commercial Contracts: Terms Affecting Freedoms, Forthcoming .

Haffke, L., Fromberger, M. and Zimmermann, P., 2020. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. Journal of Banking Regulation, 21(2), pp.125-138.

Hellenic Blockchain Hub. 2022. Homepage. News. [online]. Available at: https://www.blockchain.org.gr/ Last Access: 30/12/2022

Hellenic Republic – Government Website. 2022. Taxation. [online]. Available at: https://www.gov.gr/en/sdg/work-and-retirement/taxation/personal-income-taxes/personal-income-tax-rates Last Access: 30/12/2022

Jani, S., 2017. An overview of ethereum & its comparison with bitcoin. Int. J. Sci. Eng. Res, 10(8), pp.1-6.

Kourbetis Stavros, 2020. Smart Contracts: Private contractual practices under the light of digital technologies (Smart Contracts: Οι ιδιωτικές συμβατικές πρακτικές υπό το πρίσμα των ψηφιακών τεχνολογιών), Efarmoges Astikou Dikaiou kai Politikis Dikonomias

Matsson, D., 2022. GDPR, Blockchain & Personal data-The rights of the individual v. the integrity of Blockchain.

Panova, O. O., Yu O. Leheza, A. V. Ivanytsia, V. V. Marchenko, and V. G. Oliukha. 2019. "International models of legal regulation and ethics of cryptocurrency use: Country review."

Papantoniou Alexandros (2020), Smart contracts in the new era of contract law, Digital Law Journal, 1 (4), 8 – 24, https://doi.org/10.38044/2686-9136-2020-1-4-8-24, available online at https://www.digitallawjournal.org/jour/article/view/30.

PublicRevenew.gr. 2013. Law 4174/2013. [online]. Available at: http://www.publicrevenue.gr/elib/view?d=/gr/act/2013/4174 Last Access: 30/12/2022

Raskin, M. 2016. The law and legality of smart contracts. Geo. L. Tech. Rev., 1, 305.

Salami, I., 2020. Decentralised finance: the case for a holistic approach to regulating the crypto industry. Journal of International Banking and Financial Law, 35(7), pp.496-499.

Schillig, M., 2021. Lex Cryptographia, Cloud Crypto Land or What?–Blockchain Technology on the Legal Hype Cycle. Cloud Crypto Land or What.

Schrepel, T. and Buterin, V., 2020. Blockchain Code as Antitrust. Berkeley Technology Law Journal.

Schrepel, T., 2019. Anarchy, State, and Blockchain Utopia: Rule of Law versus Lex Cryptographia. General Principles and Digitalisation (Hart Publishing, 2020).

Solodan, K., 2019. Legal regulation of cryptocurrency taxation in European countries. Eur. JL & Pub. Admin., 6, p.64.

Tikhomirov, S., 2017, October. Ethereum: state of knowledge and research perspectives. In International Symposium on Foundations and Practice of Security (pp. 206-221). Springer, Cham.

Tsindeliani, I. and Egorova, M., 2020. Cryptocurrency as object of regulation by public and private law. J. Advanced Res. L. & Econ., 11, p.1060.

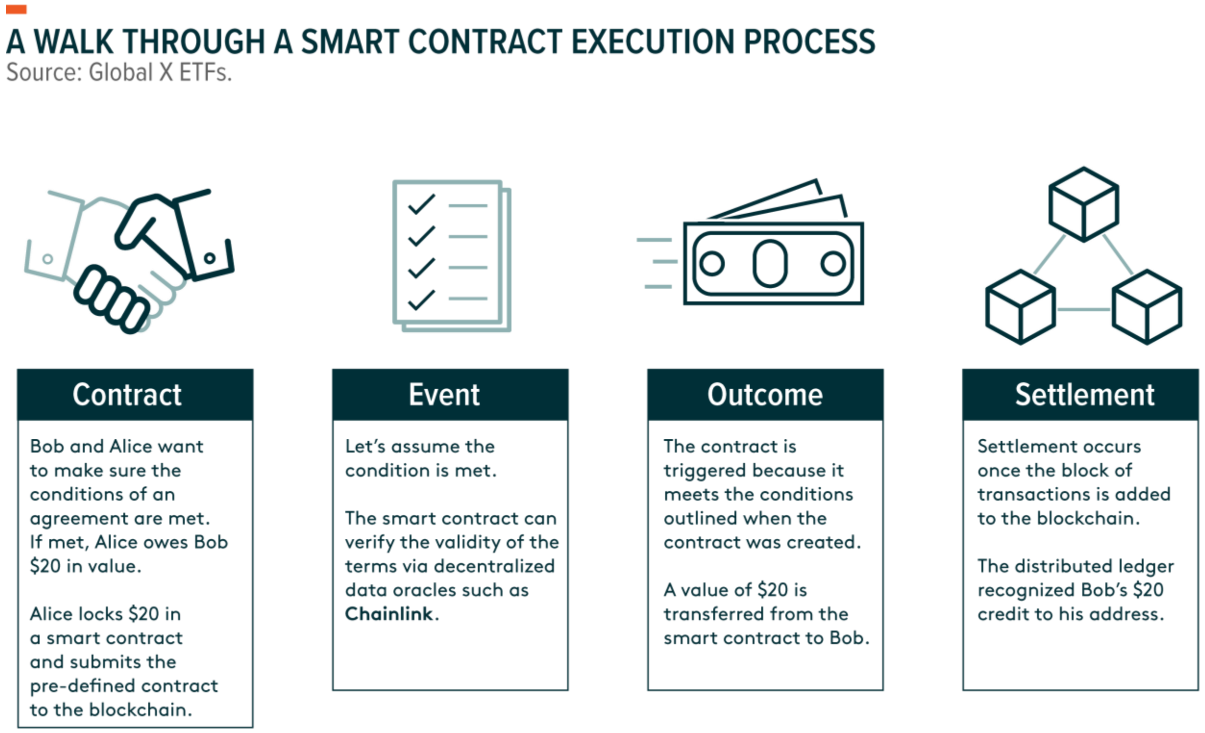
Ture, T., 2021. GDPR, Blockchain and the Right to be Forgotten.

Woebbeking, M.K., 2019. The impact of smart contracts on traditional concepts of contract law. J. Intell. Prop. Info. Tech. & Elec. Com. L., 10, p.105.

Yang, R., Wakefield, R., Lyu, S., Jayasuriya, S., Han, F., Yi, X., Yang, X., Amarasinghe, G. and Chen, S., 2020. Public and private blockchain in construction business process and information integration. Automation in construction, 118, p.103276.

Zou, W., Lo, D., Kochhar, P.S., Le, X.B.D., Xia, X., Feng, Y., Chen, Z. and Xu, B., 2019. Smart contract development: Challenges and opportunities. IEEE Transactions on Software Engineering, 47(10), pp.2084-2106.

9. APPENDIX



A WALK THROUGH A SMART CONTRACT EXECUTION PROCESS

Source: Global X ETFs.

Contract

Bob and Alice want to make sure the conditions of an agreement are met. If met, Alice owes Bob $20 in value.

Alice locks $20 in a smart contract and submits the pre-defined contract to the blockchain.

Event

Let's assume the condition is met.

The smart contract can verify the validity of the terms via decentralized data oracles such as **Chainlink**.

Outcome

The contract is triggered because it meets the conditions outlined when the contract was created.

A value of $20 is transferred from the smart contract to Bob.

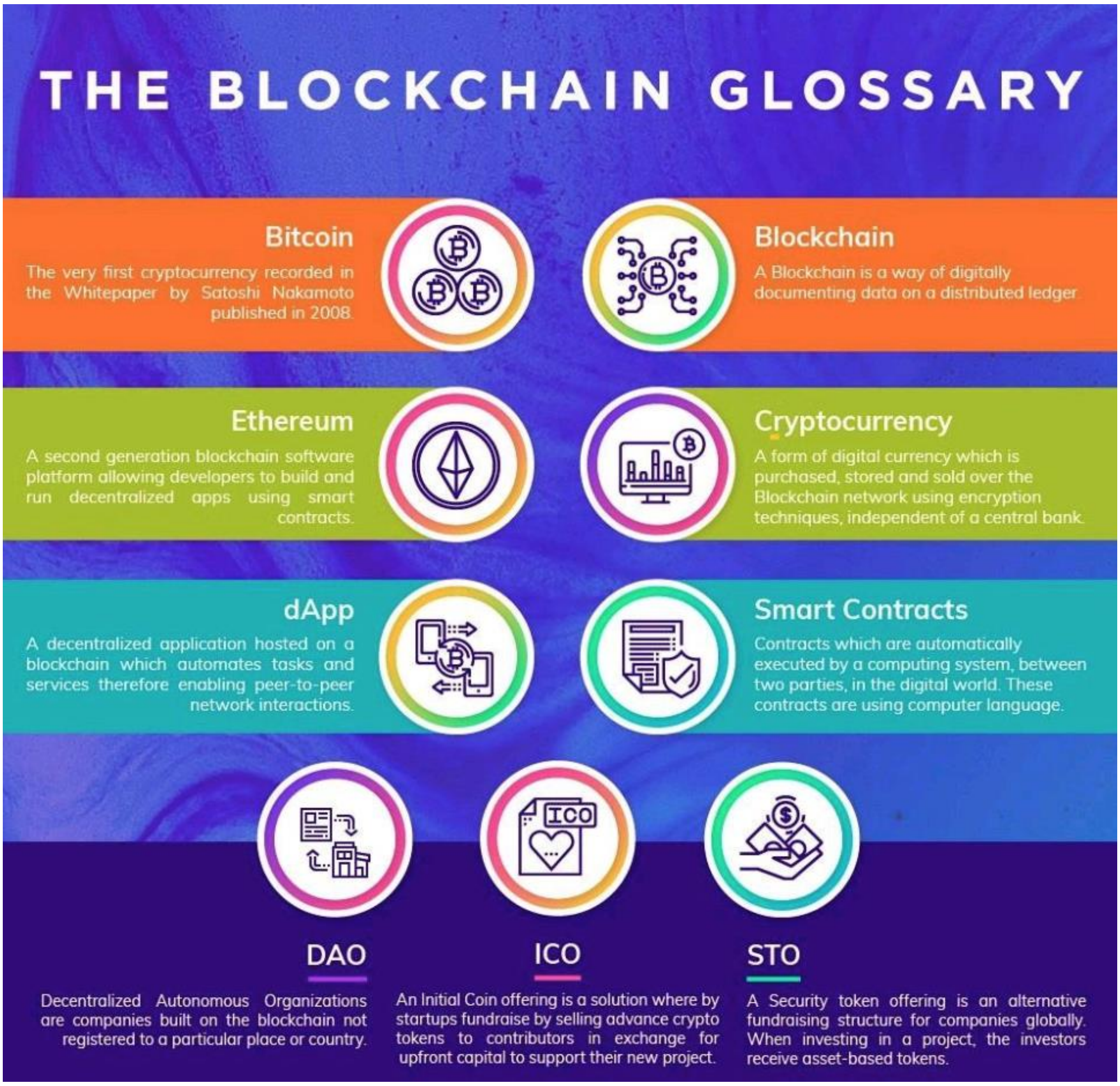
Settlement

Settlement occurs once the block of transactions is added to the blockchain.

The distributed ledger recognized Bob's $20 credit to his address.

Appendix Graph 1: Smart Contract Execution Process

Source: Baker, H.K., Nikbakht, E. and Smith, S.S. eds., 2021. The Emerald Handbook of Blockchain for Business. Emerald Publishing Limited. Adapted by the Author (2023).



THE BLOCKCHAIN GLOSSARY

Bitcoin

The very first cryptocurrency recorded in the Whitepaper by Satoshi Nakamoto published in 2008.

Blockchain

A Blockchain is a way of digitally documenting data on a distributed ledger.

Ethereum

A second generation blockchain software platform allowing developers to build and run decentralized apps using smart contracts.

Cryptocurrency

A form of digital currency which is purchased, stored and sold over the Blockchain network using encryption techniques, independent of a central bank.

dApp

A decentralized application hosted on a blockchain which automates tasks and services therefore enabling peer-to-peer network interactions.

Smart Contracts

Contracts which are automatically executed by a computing system, between two parties, in the digital world. These contracts are using computer language.

DAO

Decentralized Autonomous Organizations are companies built on the blockchain not registered to a particular place or country.

ICO

An Initial Coin offering is a solution where by startups fundraise by selling advance crypto tokens to contributors in exchange for upfront capital to support their new project.

STO

A Security token offering is an alternative fundraising structure for companies globally. When investing in a project, the investors receive asset-based tokens.

Appendix Graph 2: Glossary Infographic. Source: Baker, H.K., Nikbakht, E. and Smith, S.S. eds., 2021. The Emerald Handbook of Blockchain for Business. Emerald Publishing Limited. Adapted by the Author (2023).

A Glossary of Blockchain Terms*

Airdrop	An airdrop is a distribution of a cryptocurrency token or coin, usually for free, to numerous wallet addresses for marketing purposes.
Atomic swap	An atomic swap is a smart contract technology enabling the exchange of one cryptocurrency for another without using centralized intermediaries.
Bitcoin	Bitcoin is a type of digital currency that runs on the peer-to-peer (P2P) network without the need for central authority or intermediaries.
Block	A block is a collection of transactions that has not yet been recorded in any prior blocks.
Blockchain	A blockchain is a decentralized public ledger that uses cryptography to record transactions among a network's participating agents. It permits transactions to be gathered into blocks and recorded cryptographically into chain blocks in chronological order, and allows all users in the network to access the ledger. A central authority does not own, control, or manage this distributed database.
Blockchain application	A blockchain application is a P2P system for validating, time stamping, and permanently storing transactions and agreements on a shared ledger that is distributed to all participating nodes.
Byzantine fault tolerance (BFT)	BFT is the property of a system that can resist the class of failures derived from the Byzantine Generals' Problem, which is a logical dilemma that illustrates how a group of Byzantine generals may have communication problems when trying to agree on their next move. Thus, a BFT system can continue to operate even if some of the nodes fail or act maliciously.
Central bank digital currency (CBDC)	A CBDC is fiat money of a particular nation or region, issued and regulated by a country's monetary authority. Thus, CBDC is money that a government establishes and backs through its central bank in a virtual form.

*H. Kent Baker and Hak J. Kim compiled this glossary.

(Continued)

Cold wallet	A cold wallet is a component of hardware or other type of physical device that enables investors to access crypto-asset holdings.
Consensus protocol (algorithm or mechanism)	Consensus protocol is the set of rules and mechanisms implemented in a blockchain to consolidate the preferences and decisions of users and to manage decision-making of the network. It determines how users reach consensus on that blockchain in achieving the necessary agreement on a single data value or a single state of the network among distributed processes.
Consortium blockchain	A consortium blockchain is a system that is "semiprivate" with a controlled user group, but works across different organizations. The protocol layer is under the control of a consortium of firms that must govern according to legal frameworks and agreements external to the blockchain code. A consortium blockchain is a hybrid between the "low trust" offered by public blockchains and the "single highly trusted entity" model of private blockchains. Thus, a consortium blockchain is permissioned, semidecentralized, and has a multiparty consensus.
Crosschain	A crosschain is the interoperability between two relatively independent blockchains. It enables blockchains to speak to one another because they are built in a standardized way.
Cryptocurrency	A cryptocurrency is a digital or virtual currency that uses encryption techniques to regulate the generation of units of currency and verify the transfer of funds. It operates independently of a central bank. Many cryptocurrencies such as bitcoin are decentralized networks based on blockchain technology.
Cryptocurrency agnostic	Cryptocurrency agnostic means that projects are built to work with a multitude of tokens, cryptos, and altcoins, which allow users from different ecosystems to participate, further expanding building capacity across existing and new cryptocurrency projects.
Cryptoeconomics	Cryptoeconomics is using incentives and cryptography to design new kinds of systems, applications, and networks. It also studies economic interaction in adversarial environments.
Cryptographic hashing	Cryptographic hashing is the procedure of repeatedly inserting a random string of digits into hashing formula until finding a desirable output. It produces a single fixed length output. Some examples of hash function algorithms are MD5, MD4, or SHA-256.

(Continued)

Cypherpunk	A cypherpunk is someone who believes in privacy-enhancing technology.
Cryptography	Cryptography is a mathematical algorithm used to encrypt and decrypt information. In blockchain, it is used for creating wallets, signing transactions, and verifying the block.
Crypto tokens	A crypto token, also called a cryptocurrency or crypto asset, is a special kind of virtual currency token residing on its own blockchain and representing an asset or utility.
Decentralized application (dApp)	A decentralized application is a computer application that runs on a distributed computing system.
Decentralized autonomous organization (DAO)	A DAO is a virtual organization embodied in computer code and executed on a distributed ledger or blockchain.
Decentralized network	A decentralized network refers to a network in which anyone can transact on the ledger. The network is decentralized in the sense that no centralized entity governs the network.
Delegated Proof of Stake (DPoS)	DPoS is a consensus protocol that provides dependable verification and approval of transactions in a blockchain.
Distributed hash table (DHT)	DHT is a key-value store where the keys are hashes and widely used to coordinate and maintain metadata about P2P systems. Key-value pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.
Distributed ledger	A distributed ledger is a database that is shared across multiple sites or geographies accessible by multiple people. It allows transactions to open to the participants publicly. The participant at each node of the network can access the records shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants.
Double spending	Double spending is the result of successfully spending digital currency more than once. Blockchain protects against double spending by verifying each transaction in the network. It ensures that the inputs for the transaction had not previously already been spent.
Encryption	Encryption refers to the process of converting data to an unrecognizable or "encrypted" form. A common use of encryption is to protect sensitive information, so that only authorized parties can view it.

(Continued)

	Blockchain encryption prevents sensitive information from getting into the wrong hands and being misused or forged. Thus, only authorized parties can view the information. Although various blockchains use different cryptography algorithms, the Bitcoin blockchain uses the SHA-256 algorithm, which produces a 32-byte hash that has proven resistant to hacking attempts to date.
Genesis block	Genesis block is the name of a blockchain's first block. It is the prototype of all other blocks in the blockchain as the common ancestor of them. If any block is followed the chain backward in time, it eventually leads to the genesis block.
Hard fork	A hard fork occurs when a cryptocurrency on a distributed ledger undergoes a protocol change resulting in a permanent diversion from the legacy or existing distributed ledger. This radical change to the protocol of a blockchain network makes previously invalid blocks/transactions valid or vice versa. Thus, a hard fork is a backward incompatible upgrade to the blockchain network.
Hashing	Hashing is a mathematical function that miners perform on blocks to make the network secure. It is a transaction's unique identifier.
Hash rate	Hash rate is the computational power that miners contribute to secure the network in exchange for block rewards and transaction fees.
Hot wallet	A hot wallet is an online portal that allows investors or merchants to access crypto holdings via an online platform or application.
Hybrid blockchain	A hybrid blockchain is a mix of public and private blockchains. It can host an application or service on an independent permissioned blockchain while leveraging a public blockchain for security and settlement.
Hybrid PoW (Proof of Work)/ PoS (Proof of Stake)	A hybrid PoW/PoS consensus mechanism uses elements of both PoW and PoS models when determining transaction validation rights.
Hyperledger	Hyperledger is an open source blockchain project designed to promote collective advancement of blockchain projects as opposed to disparate proprietary systems.
Immutability	Immutability is the inability of a block to be deleted or modified once it is in the blockchain.

(Continued)

Initial coin offering (ICO)	An ICO is a mechanism used to raise external funding through the emission of tokens in exchange for cryptocurrencies. It is often a form of crowdfunding, but a private ICO that does not seek public investment is also possible.
Interoperability	Interoperability refers to the exchange of data and information compatibly across varied complex systems.
InterPlanetary File System (IPFS)	IPFS is a protocol and P2P network for storing and sharing data in a distributed file system.
Lightning network	A lightning network is a series of off-chain payment channels where two people can conduct a very fast low-cost transaction or series of transactions, which are later settled on-chain. It adds another layer to Bitcoin's blockchain enabling users to create payment channels between any two parties on that extra layer.
Merkle (hash) tree and root	A Merkle tree or hash tree is a tree-like structure that organizes large amounts of data using hashes. It consists of raw data, leaves, and a root. In blockchain, a Merkle tree serves to encode data and to verify it as blockchain signatures (hashing) more efficiently and securely. A Merkle root is the hash of all the hashes of all the transactions that are part of a block in a blockchain network.
Miner	A miner is a node on the network that is actively involved in the consensus process used to verify transactions before these transactions are batched in blocks. Miners participate in performing the block verification process by determining whether each transaction is legitimate. Miners are incentivized to participate in this process with the ability to earn compensation from either confirming blocks as they are added to the blockchain or processing transactions.
Mining	Mining is the process of adding new transaction records to a block and verifying a block created by other miners. It allows nodes to reach a secure, tamper-resistant consensus. Miners collect transaction fees and are rewarded for their services.
Node	A node is any kind of device such as a computer, laptop, or server that connects to the blockchain network. It stores, spreads, and preserves the blockchain data. All nodes on a blockchain network are connected and constantly exchange the latest data with each other.

(Continued)

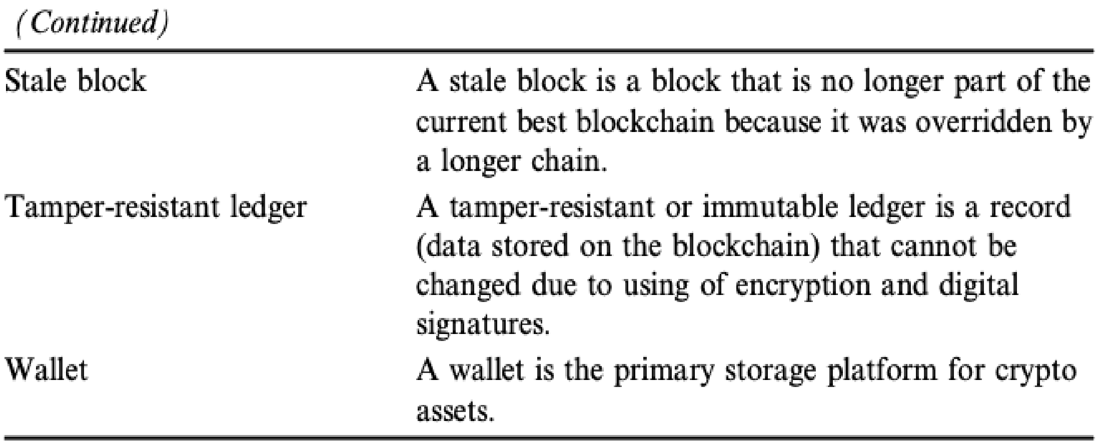
Nonce	A nonce, an abbreviation for “number only used once,” is a pseudo-random number that is used as a counter during the mining process. It is a number added to a hashed or encrypted block in a blockchain that, when rehashed, meets the difficulty level restrictions. Thus, a nonce is the number that blockchain miners are trying to solve.
Off-chain transaction	Off-chain refers to a cryptocurrency transaction that happens outside of a main blockchain and is not published there.
On-chain transaction	On-chain refers to a cryptocurrency transaction that occurs on the blockchain.
Oracle	An oracle is a way for a blockchain or smart contract to interact with external data. As third-party services, blockchain oracles serve as bridges between blockchains and the outside world.
Orphan block	An orphan block is a validated block that is not accepted into the blockchain network due to a time lag in the acceptance of the block in question into the blockchain. For example, assume two blocks are validated at a similar time. Once one block gets accepted in the node, then the other block is discarded, which is an orphan block. Thus, an orphan block is a valid and verified block but have been rejected by the chain
Peer-to-peer (P2P)	In blockchain, a P2P network is one where peers can communicate and do transactions directly with other network members without having to rely on an intermediary or a third party to perform confirmations or other verification processes
Private (permissioned) blockchain	A private blockchain is closed and invitation-only such that specific users or entities on a blockchain have authorizing powers over others, allowing them to appoint members or validators. It has centralized authorities and is often deployed in the area of internal business operations.
Private key	A private key is a cryptography allowing a user access to his or her cryptocurrency or transaction. It is equivalent to a password and thereby helps to protect a user from theft and unauthorized access to funds.
Proof of Activity (PoA)	POA is another hybrid of PoW and PoS that attempts to combine the best features of both mechanisms.

(Continued)

Proof of Burn (PoB)	POB is an alternative consensus algorithm that tries to address the high energy consumption issue of a PoW system.
Proof of Capacity (PoC)	POC is a consensus mechanism that uses a process called plotting.
Programmatic Proof of Work (ProgPoW)	ProgPow is a blockchain protocol consensus algorithm designed to reduce the mining efficiency advantage of specialized hardware like ASIC miners over less-advanced machines like a standard CPU, meaning average individual crypto participants can mine coins.
Proof of Elapsed Time (PoET)	PoET is a consensus algorithm that prevents high resource utilization and keeps the process more efficient by following a fair lottery system. For example, each participating node in the network is required to wait for a randomly chosen time period, and the first one to complete the designated waiting time wins the new block. Each node in the blockchain network generates a random wait time and goes to sleep for that specified duration. The one with the shortest wait time commits a new block to the blockchain, broadcasting the necessary information to the whole peer network. The same process then repeats for the discovery of the next block.
Proof of Retrievability (PoR)	PoR is a compact proof by a file system (prover) to a client (verifier) that a target file is intact in the sense that the client can fully recover it.
Proof of Storage	Proof of Storage is a consensus protocol used primarily to verify the integrity of a remote file.
Proof of Work (PoW)	PoW is the original consensus algorithm in a blockchain network. In a PoW algorithm, the miners compete against each other to validate a block and the first miner who presents validation for a block gets rewarded. For example, a miner repeatedly inserts transaction data (block) and a random string of digits (nonce of block) into a hashing formula, until the miner finds a desirable outcome – the PoW. Other miners can verify the PoW by taking the alleged input string and applying it to the same formula to see if the outcome is what the initial minor presented. Some view PoW as a controversial consensus algorithm because of the electricity costs involved in performing the formula calculations.

(Continued)

Proof of Stake (PoS)	PoS is a consensus algorithm that asks users to prove ownership of a certain amount of currency that is their stake in the currency. PoS gives the miners who hold coins (e.g., bitcoin) the ability to mine or validate transactions. In other words, the power of mining is proportional to the amount of coins a miner owns. Thus, the PoS process rewards larger stakeholders in the network.
Public (permissionless) blockchain	A public or permissionless blockchain is a decentralized ledger that is accessible to any user. Users do not need permission from anyone on the network to perform certain actions such as joining the network, receiving/sending transaction data, and participating in the consensus process to determine what blocks get added to the chain.
Public key	A public key is a cryptographic code or address used to facilitate transactions between parties that allow users to receive cryptocurrencies in their accounts. It enables the agent to access specific information, comparable to an access code.
Record	A record is a combination of transactions.
SHA-256	SHA-256 stands for Secure Hash Algorithm 256-bit, and it is used for cryptographic security. SHA-256 generates an almost-unique 256-bit signature for a text. Bitcoin uses SHA-256 for mining and creating addresses.
Sidechain	A sidechain is a mechanism allowing tokens and other digital assets from one blockchain to be securely used in a separate blockchain and then be moved back to the original blockchain if needed.
Smart contract	A smart contract is computer code operationalized within blockchain that automatically moves digital assets according to prespecified rules. Thus, smart contracts are codes that are built into the software that enable automation of certain job tasks or processes.
Soft fork	A soft fork is a change to the bitcoin protocol that makes only previously valid blocks or transactions invalid.
Stablecoin	A stablecoin is a crypto asset that normally takes the form of a coin or token that is connected or supported by an underlying asset including currencies or basket of commodities. The basic goal of stablecoins is to aid in developing of an alternative financial system with currency units not dependent or controlled by a government or other centralized entity.



(Continued)

Stale block	A stale block is a block that is no longer part of the current best blockchain because it was overridden by a longer chain.
Tamper-resistant ledger	A tamper-resistant or immutable ledger is a record (data stored on the blockchain) that cannot be changed due to using of encryption and digital signatures.
Wallet	A wallet is the primary storage platform for crypto assets.

Source: Baker, H.K., Nikbakht, E. and Smith, S.S. eds., 2021. The Emerald Handbook of Blockchain for Business. Emerald Publishing Limited.