ULP LAW REVIEW
REVISTA DE DIREITO DA UL-P

VOL. 17 N. 2 [2023]

ULP LAW REVIEW
REVISTA DE DIREITO DA UL-P
BI ANUAL | BI ANNUAL

DOUTRINA

SECÇÃO TEMÁTICA

Youness Bendahmane

Some Legal Aspects Of The Smart Contract (Blockchain)

CEAD FRANCISCO SUAREZ
Fdcp Faculdade de Direito e Ciência Política
UNIVERSIDADE LUSÓFONA | CENTRO UNIVERSITÁRIO PORTO

ULPLR

SOME LEGAL ASPECTS OF THE SMART CONTRACT (BLOCKCHAIN)

YOUNESS BENDAHMANE[1]

DOI: 10.60543/UL-PLR-RDUL-P.V17I2.9519

ABSTRACT

Smart contracts are regarded as one of the most promising applications of blockchain technology. While the concept has been recognised for several years, the emergence of blockchain has revitalised its development and provided it with new impetus. The term "smart" refers to the automated execution of these digital contracts, with conditions established by the involved parties at the time of creation. The potential applications of smart contracts are as varied as the types of contracts individuals engage in on a daily basis, covering sectors such as banking, insurance, healthcare, energy, and transportation. Furthermore, blockchain technology has the potential to replace numerous centralised trusted intermediaries, including brokers, financial advisors, notaries, and land registries, with decentralised computational systems. This transformative potential has generated considerable enthusiasm, alongside certain concerns. Scholars and professionals in computing, economics, and law emphasise the innovative and disruptive nature of these applications, considering them part of a broader digital revolution.

The advancement of decentralised authentication technology, referred to as "blockchain," has recently highlighted its potential for automating certain predefined operations, triggered, for example, by the occurrence of an external event. This automation technique was coined by its creator, computer scientist Nick Szabo, with the Anglo-Saxon term "smart contract." He proposed defining such a digital mechanism as "a computerised transaction protocol capable of executing the terms of a contract.[2]" In his perspective, certain contractual provisions, particularly those concerning the exercise of property and usage rights, would be more efficiently executed by the obligated party if their enforcement were entrusted to automated processing software. This would reduce the likelihood of contract breaches.

Embraced by blockchain developers, these smart contracts can serve as valuable adjuncts, particularly in the provision of various services, especially financial services, related to the exchange and circulation of crypto-assets. This practice is beginning to be applied in concrete scenarios and is simultaneously drawing the attention and scrutiny of legal scholars.

Blockchains are often regarded as a significant advancement in technology and computer systems, offering a level of security previously absent on the Internet. They can establish trust in digital data by recording information in

1 Professeur De Droit Prive; Faculté de droit d'Agadir (Professor of Private Law, Faculty of Law of Agadir). Email: youness.bendahmane@gmail.com.

2 SZABO N., Smart Contracts: Formalizing and Securing Relationships on Public Networks, First Monday 1997, vol. 2, no. 9, http://firstmonday.org/ojs/index.php/fm/article/view/548.

a blockchain database, where it becomes nearly impossible to delete or alter. This represents a novel and transformative development in the field of computing. More specifically, a blockchain is a data structure that facilitates the creation of a digital ledger, enabling the sharing of data amongst a network of independent participants. It is important to note, however, that there are three distinct types of blockchains.

To begin with, public blockchains, such as Bitcoin, are extensive distributed networks that function using a native token. They are accessible to anyone at all levels and are supported by open-source code maintained by the community. Secondly, there are permissioned blockchains, which regulate the roles that individuals can assume within the network, exemplified by platforms such as Ripple. Lastly, private blockchains are typically smaller in scale and do not necessitate the use of tokens. Access to these blockchains is strictly controlled, as they are often utilised by consortia of affiliated members for the exchange of confidential information.

All three types of blockchains employ cryptography, enabling each participant within a network to securely manage the ledger without relying on a central authority to enforce regulations. One of the most significant and impactful features of blockchain technology is its ability to remove the need for a central authority within the database structure. Although blockchain facilitates the creation of permanent records and transaction histories, it is important to acknowledge that nothing is entirely immutable. The permanence of records within a blockchain is contingent upon the stability and continuity of the network. Participation in a blockchain framework requires a substantial portion of the community to consent to modify information without altering the underlying data. Once data is entered into the blockchain, it becomes extremely challenging to alter or delete. This process involves network users who hold validation authority verifying the proposed entry, referred to as a transaction made by a community member. The validation process varies across communities, as each blockchain operates according to its distinct protocols and mechanisms.

It is relevant to examine, even briefly, in a comparative study of the legal systems, both in France and in Morocco, the innovative technology of blockchain, intended to be integrated into various digital solutions. Some jurisdictions have already implemented partial recognition of this technology. The French legal system, for example, has adopted provisions regarding blockchain, particularly for the transfer and custody of assets. On the other hand, the Moroccan legal landscape remains marked by a regulatory void in this area.

Morocco has not yet established a specific legal framework to govern blockchain-related operations. However, aware of the growing economic and security challenges, the Moroccan government is working to develop appropriate legislation. This bill, inspired by international best practices, aims to regulate activities related to blockchain while ensuring the protection of investors and the financial stability of the country. This comparison between the two legal systems will make it possible to analyse the divergent and convergent approaches to the regulation of this technology in these two countries.

Furthermore, these measures represent initial attempts to incorporate blockchain into the legal framework without comprehensive regulation. Regulating blockchain, in terms of legal oversight, presents significant challenges. This undertaking may even appear contradictory given the decentralised nature of the technology, which signifies a departure from the existing paradigm. The promise of blockchain resides in its independence from any form of centralised control, whether governmental or otherwise, and in its governance by the network itself. When applied to smart contracts, these characteristics suggest a degree of autonomy, whereby interactions between platform users

would operate independently of existing contractual frameworks and regulations.

Are the promises of this revolutionary technology, which fundamentally departs from the current contractual paradigm, attainable or merely illusory? What will be its relationship with existing contract law?

I. BLOCKCHAIN, A TOOL FOR REVOLUTION

In exploring the revolutionary nature of smart contracts, it is essential to analyse them from both technical and legal perspectives (A), thereby emphasising their vulnerabilities (B).

A. A CONTRACT WITHOUT INTERMEDIARIES: THE REVOLUTION OF SMART CONTRACTS

Blockchain technology holds legal significance across various disciplines, including corporate law, tax law, financial law, securities law, insurance law, *inter alia*. In the first section, we will examine the characteristics and limitations of blockchain, followed by an investigation into how the law could legitimise this revolutionary technology.

As noted above, the advantages of blockchain are manifold and generate considerable interest from various stakeholders. This leads to the considerations of transparency and decentralisation within the network, as well as the various types of transactions, particularly in exposing its vulnerabilities to evaluate its potential legal development.

A transparent, decentralised, and peer-to-peer network, blockchain – often referred to as a "chain of blocks"– is characterised as a "very large notebook that everyone can read freely, for free, on which everyone can write, which is impossible to erase and indestructible."

From an academic perspective, this technology could be described as serving the purpose of "constituting a decentralised database without a central control body. The data stored within the blocks are linked together, forming a chain." The Blockchain Institute of France defines the chain of blocks as "a technology for storing and transmitting information that is transparent, secure, and operates without a central control body."

At first glance, this definition appears conventional in comparison to existing methods of information storage and transmission. The novelty lies in the ability to transfer information or assets without a "central control body," which implies the absence of intermediaries such as banks, the state, notaries, or internet platforms. These are transactions based on the exchange of consent between parties without the presence of a third party as a trusted intermediary.

Notwithstanding, to utilise this technology within a legal context, it is crucial to first analyse the technical aspects to facilitate its effective implementation. Transactions conducted by users on the network are initially organised into blocks in chronological order.

As previously mentioned, the advantages of blockchain are numerous and generate considerable interest from various stakeholders, emphasising the network's transparency and decentralisation, as well as a variety of transactions. This interest particularly focuses on revealing its vulnerabilities to assess its potential legal development. A transparent, decentralised, and "peer-to-peer" network, blockchain – often referred to as a "chain of blocks"– is characterised as a "very large notebook that everyone can read freely, for free, on which everyone can write, and which is impossible to erase and indestructible.[3]"

3 J. P. DELAHAYE, « Les blockchains, clefs d'un nouveau monde » in Logique et calcul, mars 2015, p.81.

Each block comprises various pieces of information, including the owner's signature, details of each transaction, the creation time of the block (known as timestamping), and the recipient's public key[4].

Currently, intermediaries such as the state, lawyers, notaries, banks, *inter alia,* play a central role in daily transactions. However, they do not always receive unanimous approval, particularly concerning the cost of their services, which tend to be higher than those associated with using blockchain. In reality, technological advancement seeks to create a world that is increasingly individualistic and fast-paced, often leading to excessive transaction processing times and costs[5]. Blockchain facilitates the exchange of value in a decentralised manner, eliminating the need for intermediaries regardless of their legal status. This decentralisation is made possible through the use of a distributed ledger [6].

By definition, a distributed ledger is recorded simultaneously and synchronised across a network of computers managed by multiple contributors, documenting transactions across decentralised nodes. Decentralisation is the fundamental characteristic of blockchain, which makes it a particularly intriguing technology and leads to two main consequences[7]. Firstly, blockchain chains are designed to be distributed across multiple servers rather than being housed on a single server, in contrast to the more conventional model of a centralised network that stores all information in one location. These servers, headquartered in various parts of the world and owned by different individuals, encompass all electronic devices (computers, tablets, and smartphones[8]) provided by blockchain members[9]. This is a beneficial aspect, as it means that if a portion of the servers fails or malfunctions, the remaining servers will continue to function, thereby ensuring the continuity of exchanges and transactions.

Moreover, blockchain operates without a central server; there is no supervisory authority, meaning that no single entity holds control. Instead, multiple nodes exist, each considered equally trustworthy. The network must self-regulate through the consensus of its users, without the involvement of a trusted third party. Therefore, consensus is a fundamental aspect of the system. The most crucial concept is transparency, due to its decentralised and distributed nature among all network members, which allows each participant to have visibility into the operations conducted on the blockchain. Another significant characteristic of blockchain is its immutability. Once an operation is executed on the blockchain, it is permanently recorded, making it impossible to modify or delete that operation.

B. WEAKNESSES OF BLOCKCHAIN

A blockchain operates as a peer-to-peer system without a central authority overseeing the flow of data. One primary method to prevent central control while preserving data integrity is to expand the network, distributing it across independent users. However, numerous issues arise concerning various aspects of blockchain technology. Additionally, many

4 In asymmetric cryptography, there are two types of keys: the private key and the public key. The private key (as the name suggests) must be kept securely by its user and should not be shared with others. In contrast, the public key (as the name suggests) should be shared with the network.

5 In particular, within the banking system, we think of the sometimes high delays and costs associated with international transfers.

6 Known by its English acronym Distributed Ledger Technology.

7 A. TORDEURS, « Une approche pédagogique de la Blockchain » in Revue internationale des services financiers / International Journal for Financial Services, Bruylant, 2017, p. 14.

8 Within the limits of their computing and storage capacity.

9 R. BARON, Technical Aspects of Blockchain, in Blockchain and Law, edited by F. Marmoz, Dalloz, 2018, p. 18.

researchers and major companies are gradually addressing these challenges. Nevertheless, it is important to highlight these weaknesses to analyse its potential legal development. Several factors impede the evolution of blockchain and necessitate concrete alternatives and solutions from a legal perspective.

As noted earlier, blockchains rest upon the consensus of network nodes to establish their rules. This "democratic" system tends to be less certain than a "dictatorship," where a central authority can make decisions swiftly. Governance issues are prevalent, and a majority must be reached to implement any decision. From an energy perspective, the proper functioning of blockchain necessitates the computing power of computers to solve mathematical problems and verify block entries in the chain. As a result, millions of computers worldwide must operate continuously and simultaneously. However, this process incurs both economic and environmental costs[10].

To assess the scale of energy consumption associated with this system, we will analyse the most energy-intensive blockchain, Bitcoin. Several sources offer estimates based on the energy expenditure of the AntMiner S9 system, which consumes approximately 1375W per hour. It is estimated that the network consumes around 55 billion kWh annually[11].

The most contentious issue is anonymity, which is facilitated by asymmetric cryptography and electronic signatures. In Morocco, Law No. 53-05, relating to the electronic exchange of legal data and its implementing texts, has equipped the country with a legal framework recognising electronic documents and electronic signatures. It establishes the conditions for equivalence between handwritten and electronic signatures. Although no definition of blockchain is provided, some articles may be interpreted as applicable to operations conducted on the blockchain. Transactions involving cryptocurrencies are currently not prohibited in Morocco.

In practical terms, a blockchain does not need to ascertain the true identity of the individual storing information and conducting transactions [12]. Participants in the blockchain do not require this information because trust is placed in the infrastructure and the customised rules of the blockchain protocol. Each blockchain has its characteristics and rules outlined in its white paper[13]. The white paper, in French, is a collection of factual information about the project. Historically used in politics to describe strategies to be implemented, blockchain proponents refer to it as "the trust machine" because it redefines the concept of trust, leading to the widespread use of pseudonym[14]s. This is a strength of blockchain but also a source of negative consequences. Firstly, it fuels illegal practices such as money laundering, financing illegal activities such as terrorism and drug trafficking, or tax evasion[15].

The dilemma of justice resides in finding a balance between the ability to intrude into private lives for the greater good and the respect for privacy, akin to the social and legal issues associated with banking secrecy. However,

10 BEDDIAR, K., IMBAULT, F., Blockchain pour l'énergie, Malakoff, Dunod, 2018.p 37-39.

11 https://digiconomist.net/bitcoin-energy-consumption consulted 04/05/2024.

12 A. NARAYANAN, J. BONNEAU, E. FELTEN, A. MILLER, S. GOLDFEDER, Bitcoin And Cryptocurrency Technologies : A comprehensive introduction, Princeton University Press, Princeton, 2016 ; p.15-18

13 https://cryptoast.fr/quest-ce-quun-white-paper-livre-blanc consulted 20/02/2024.

14 P. DE FILIPPI, The interplay between decentralization and privacy: the case of blockchain technologies, Journal of Peer Production, 2016, p. 11.

15 M. OMRI, « Les cryptomonnaies sont-elles des super paradis fiscaux ? », Michigan Law Review, n°112, 2013, p.38-48 ; G. REUBEN, « Bitcoin : An innovation alternative digital currency », Hastings science and Technology Law Journal, n°4, 2011, p.160-208.

with the advancement of data mining[16], a component of Big Data[17] analysing vast amounts of data, the loss of pseudonymity can occur through methods such as blockchain tracing and "transaction graph analysis," which are used to identify the individuals behind pseudonyms [18]. This issue tends to diminish with the proliferation of blockchains. As blockchain networks expand, it becomes increasingly difficult to trace metadata [19] - associating data with the date it was recorded or generated - new blockchains are emerging that mask the source, destination, or volume of transactions through various encryption strategies to ensure anonymity and privacy[20].

Nonetheless, the law has historically adapted to emerging social phenomena, yet there remains a significant lag between the birth of new technology and its actual consideration by lawmakers[21]. The disintermediation inherent in blockchain, which removes the role of a trusted third party that the state could fulfil, exacerbates the state's disinterest[22]. While this response may seem logical and understandable, it highlights a level of insecurity that could potentially hinder the technology's development. For fiscal purposes, how will assets or cryptocurrencies stored on the blockchain be treated? What is the validity of the electronic document recorded on the blockchain or the smart contract established on it? These questions remain unresolved and may lead to public confusion regarding the use of this technology.

LAW AND BLOCKCHAIN

Mandatory norms are anticipated to play a crucial role in the regulation of international electronic contracts. First, the public policy exception continues to be undeniably relevant (A). Furthermore, in addition to the traditional rules that apply immediately to international contracts, it is important to investigate whether there is now a specific regulation governing these smart contracts (B).

A. THE PERSISTENCE OF THE PUBLIC POLICY EXCEPTION

Public policy was initially the central concept considered by theories advocating for a libertarian web. A first, one might have thought that the notion of public policy was irrelevant due to the limitations of state sovereignty, which cannot extend beyond national borders and, therefore, does not pertain to cyberspace.

16 Data mining is a key component of Big Data technologies and techniques for analyzing large volumes of data. It provides the basis for in-depth data analysis, predictive analytics, and data exploration.

17 The quantitative explosion of digital data has compelled researchers to find new ways to view and analyze the world. It involves discovering new methods for managing the scale of data capture, search, exchange, storage, analysis, and presentation.

18 Researchers from the University of San Diego and George Mason University have managed, through this process, to identify groups of merchants and clients: S. MEIKLEJOHN, M. POMAROLE, G. JORDAN, K. LEVCHENKO, D. MCCOY, G.VOELKER, and S. SAVAGE, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," in Proceedings of the 2013 Conference on Internet Measurement, ACM, New York, 2013, pp. 127-140.

19 A datum used to define or describe another datum, regardless of its medium (paper or electronic).

20 For example, signature circles: E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in Symposium on Security and Privacy, IEEE, Piscataway, 2014, pp. 459-474.

21 B. CHOULI, F. GOUJON et Y.-M. LEPORCHER, *Les Blockchains : De la théorie à la pratique, de l'idée à l'implémentation*, Collection Epsilon, ENI, 2017, p.31.

22 M. GUERINEAU, « Blockchain : l'ère de la transparence ? » in *Revue internationale des services financiers / International Journal for Financial Services*, Bruylant, 2016, p.79.

The North American doctrine tends to regard the Yahoo! case as a pivotal turning point, signalling the end of the notion of a borderless internet. To recall, a French judge ordered Yahoo! to restrict access to the sale of Nazi items for internet users located within French territory[23]. Yahoo!'s arguments before the French court exemplified the de-territorialised conception of cyberspace that was prevalent in the 1990s. The decision, which flared numerous debates across the Atlantic, firmly rejected this view. The first lesson from this emblematic case is that French public policy is intended to apply, including to e-commerce activities – a point that only proponents of "cyber-anarchy" could contest.

As regards public policy in international electronic contracts, it is clear that this notion will remain present. However, there is a risk that the specificity of its application will be gradually forgotten.[24]

There is a risk of overlooking the fact that an electronic contract, even if it is an international contract, is not governed by the same public policy rules as a domestic contract since the concepts of public policy vary fundamentally between jurisdictions. Furthermore, the "Rome I" regulation encourages us to restrict the application of public policy to matters of public interest only. Applying internal public policy indiscriminately to all electronic contracts would effectively negate their international nature and convert internal public policy into a set of borderless rules.

A second lesson arises from the reception of the French decision in the United States. Initially, in a ruling dated 7 November 2001, California Judge Jeremy Fogel deemed the decision to be contrary to the freedom of expression protected by the 1st Amendment of the U.S. Constitution. However, in a more nuanced ruling in 2006, the U.S. Federal Court of Appeals for the 9th Circuit in San Francisco acknowledged that the French decision, by merely prohibiting access to the site for individuals located on French territory, did not impact U.S. territory. As a result, the violation of the 1st Amendment was not established.

The approach taken by the Court is quite instructive: "Yahoo!'s U.S. website is written in English. It targets users in the United States and relies on servers located in California." The American judges first assessed the audience targeted by the site using various indicators. In other words, the federal judge employed a focus technique to determine whether federal public policy applied to the website. In principle, Yahoo!'s activities are protected by the U.S. Constitution because they are aimed at users within U.S. territory. Nevertheless, the opinion issued dismisses the notion that the 1st Amendment could have extraterritorial implications. Consequently, the French decision, which merely prohibits activities within its territory, does not constitute a violation of the constitutional provision.

If we shift our focus from constitutional law back to the principles of private international law, this solution can be compared to the application of the German doctrine of Inlandsbeziehung, or even to a public policy attachment that aims to establish connections with the cause to unilaterally determine its scope. The proximity of links to the forum's public policy can be assessed, if necessary, using the focus technique, as effectively illustrated by the approach taken by the Federal Court of Appeals[25].

Ultimately, public policy does not appear to be genuinely compromised by international electronic contracts. Instead, it adapts to its new dimension –cyberspace – by

23 LAVENUE, J.-J. (2006). Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberespace confronté à la notion d'ordre public. Lex electronica, 11(2), Automne/Hiver.

24 Boden, D. (2002). L'ordre public. Limite et condition de la tolérance : recherches sur le pluralisme juridique (Doctoral dissertation). Paris-I.

25 David MARTEL, Les contrats internationaux sur le web, Lamy Droit de l'Immatériel, N° 81, 1er avril 2012, p7.

employing techniques specific to this context. The real danger, conversely, would be an overly expansive interpretation of public policy rules, particularly given the potential for overriding mandatory provisions to come into play.

B. THE REGULATION OF BLOCKCHAIN TECHNOLOGY

Blockchains or at least those regarded as true blockchains – specifically public blockchains – are founded on liberal ideology, which asserts that they should not be subject to any human regulation. The famous adage "code is law," coined by Lawrence Lessig, encapsulates this notion. Currently, cryptocurrencies function as law, as long as computer codes establish rules among users. Notwithstanding, in light of new economic and financial challenges, it is reasonable to question the need for a new set of rules. If the ultimate aim of digital currency is to evade all controls and the activities of regulatory authorities, can we not speak of the emergence of a "*lex cryptographia*"[26]?

The participants in the blockchain ecosystem – such as developers, miners, exchange operators, and individuals conducting transactions – interact within the parameters and modalities outlined by the computer protocol. In the context of blockchain, terms like "trust," "decentralisation," and "technological democracy" are commonly used; however, there is little in the way of "regulation," and even less "law" or "legal framework."

Technology is a human construct. If we follow the adage "Code is law[27]", then it is indeed humans who write these "Codes." Based on this principle, it is humans who write and programme the computer code and configure the blockchain. While computer code serves as a regulator, its orientation is a result of human intervention, as individuals ultimately determine its direction. However, programming the blockchain code is akin to establishing the rules of the game for the entire ecosystem. Ultimately, this is nothing less than a political act.

When addressing the law in the context of technological innovations, it is crucial to implement regulations that do not hinder technological development[28] while also effectively addressing new legal challenges and ensuring both individual and collective protection. This is where smart contracts become significant, as they raise questions regarding legal recognition. The concept of translating traditional contracts into computer languages, or even programming them directly onto the blockchain, represents a branch of law that aims to harmonise legal frameworks with technological advancements.

As in other areas of law, it is unrealistic to achieve complete and perfect legal control over technologies. Several factors contribute to this, including the differing rates of development between law and technology, as well as the potential for errors in both fields. While errors are an inherent aspect of human nature, imperfect regulation can still be effective. To address the absence of perfect and effective control, two legal approaches can be adopted: state law and alternative norms.

26 L.LESSIG,*Ibid.,* p.55

27 *Ibid.* p.69.

28 POULLET, Y., & DINANT, J.-M. (2004). L'autodétermination informationnelle à l'ère de l'Internet. Conseil de l'Europe, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, November 18, 2004, p. 41. Retrieved from https://rm.coe.int/16806ae51f (accessed February 20, 2024).

CONCLUSION

The analysis of smart contracts, and more precisely of their technical nature, reveals that the inherent rigidity of computer language poses serious limits to the automation of contractual content. Therefore, smart contracts cannot claim, to date, to become a common or dominant practice in the contractual field. They are not able to replace contract law, which remains a legal framework applicable to all forms of contracts. Thus, the excitement over smart contracts, particularly Blockchain technology, which eliminates the need for an intermediary or institution as a trusted figure, may ultimately prove to be an illusion.

It is interesting to note that blockchain technology provides entrepreneurs with greater assurance regarding the execution of their contractual obligations, thanks to the elimination of human intervention, which plays a crucial role in this regard. In addition, this technology allows for more transparent contract execution and facilitates effective monitoring of contractual operations, without an intermediary. However, the use of smart contracts, when it becomes the sole tool, will introduce a series of new challenges for lawyers.

By 2030 or 2040, it is conceivable that everyday transactions, such as shopping, will be conducted via blockchains, and payments may be made with cryptocurrencies. It may also become possible to pay taxes using blockchain technology, obtain loans, sign employment or lease contracts, and record academic qualifications and work experience on blockchains. Additionally, even personal matters such as marriage contracts could be formalised through blockchain systems.

Finally, the rapid evolution of blockchain technology points to a future where decentralised systems could play a pivotal role in numerous aspects of daily life. As the technology matures and becomes more integrated into various sectors, its potential for transforming transactional processes – including financial, legal, and personal – becomes increasingly apparent. However, realising this vision will depend on resolving existing technical, legal, and regulatory challenges, as well as fostering public trust in blockchain's reliability and security. Further interdisciplinary research and development will be essential to address these complexities and to guide the future adoption of blockchain-based solutions.

BIBLIOGRAPHY

I. BOOKS

BEDDIAR, K., IMBAULT, F., Blockchain pour l'énergie, Malakoff, ed Dunod, 2018.

B. CHOULI, F. GOUJON et Y.-M. LEPORCHER, Les Blockchains : De la théorie à la pratique, de l'idée à l'implémentation, Collection Epsilon, ENI, 2019, 1ere Edition

M. GUERINEAU, « Blockchain : l'ère de la transparence ? » in Revue internationale des services financiers / International Journal for Financial Services, Bruylant, 2016, p.79

II. ARTICLES, CONTRIBUTIONS, AND REPORTS

J. P. DELAHAYE, « Les blockchains, clefs d'un nouveau monde » in Logique et calcul, mars 2015.

R. Baron, Aspects techniques de la blockchain, in Blockchain et droit, F. Marmoz (dir.), 2020/4 (N° 4), Dalloz, 2018.

Eva THÉOCHARIDI, La conclusion des smart contracts : révolution ou simple adaptation ? Lamy droit civil n°161, juillet 2018

A. NARAYANAN, J. BONNEAU, E. FELTEN, A. MILLER, S. GOLDFEDER, Bitcoin And Cryptocurrency

Technologies : A comprehensive introduction, Princeton University Press, Princeton.

P. DE FILIPPI, « The interplay between decentralization and privacy: the case of blockchain technologies », Journal of Peer Production, 2016.

M. OMRI, « Les cryptomonnaies sont-elles des super paradis fiscaux ? », Michigan Law Review, n°112, 2013, p.38-48 ; G. REUBEN, « Bitcoin : An innovation alternative digital currency », Hastings science and Technology Law Journal, n°4, 2011.

S. MEIKLEJOHN, M. POMAROLE, G. JORDAN, K. LEVCHENKO, D. MCCOY, G.VOELKER et S. SAVAGE, « A fistful of bitcoins : Characterizing payments among men with no names » in Proceedings of the 2013 conference on internet measurement, ACM, New York, Published – 2013 13th ACM Internet Measurement Conference, IMC 2013 - Barcelona, Spain

E. BEN SASSON, A. CHIESA, C. GARMAN, M. GREEN, I. MIERS, E. TROMER et M.VIRZA, « Zerocash : Decentralized anonymous payments from Bitcoin » in Symposium on security and privacy, IEEE, Piscataway, 2014.

M. GUERINEAU, « Blockchain : l'ère de la transparence ? » in Revue internationale des services financiers / International Journal for Financial Services, Bruylant, 2016.

P.DE FILIPPI, A. WRIGHT, Blockchain and the Law. The Rule of Code, Cambridge, Harvard University Press, 2018.

J. HUBIN, Y. POULLET, La sécurité informatique, entre technique et droit, Namur, Centre de recherches informatique et droit, 1998.

Lavenue J.-J., Internationalisation ou américanisation du droit public : l'exemple paradoxal du droit du cyberespace confronté à la notion d'ordre public, Lex electronica, vol. 11, no 2 (automne/hiver 2006).

Boden D., L'ordre public. Limite et condition de la tolérance : recherches sur le pluralisme juridique, Thèse, Paris-I, 2002.

David MARTEL, Les contrats internationaux sur le web, Lamy Droit de l'Immatériel, N° 81, 1er avril 2012.

III. WEBOGRAPHY

https://digiconomist.net/bitcoin-energy-consumption

https://cryptoast.fr/quest-ce-quun-white-paper-livre-blanc

https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b

Y. POULLET et J.M. DINANT, L'autodétermination informationnelle à l'ère de l'Internet, Conseil de l'Europe, Comite consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 nov. 2004, p.41 en ligne : < https://rm.coe.int/16806ae51f >

L. LESSIG, Code: And Other Laws of Cyberspace, Version 2.0, Basic Books, New York, 2006, p.52 en ligne : < http://codev2.cc/download+remix/Lessig-Codev2.pdf >