Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr
Cilt:5 Sayı:2
Geliş:05.11.2023
Kabul:25.12.2023

# Distributed Ledgers And Their Implications In Information Technology Law

*Necla SÜMER ÖZDEMİR*
*Rekabet Başuzmanı, Rekabet Kurumu, Dış İlişkiler ve Rekabet Savunuculuğu Dairesi Bşk. Yrd.*
*Çankaya, Ankara, Türkiye*
*nsumer@rekabet.gov.tr*
*n.sumerozdemir@gmail.com.tr*
*ORCID ID: 0000-0002-6934-8174*

ABSTRACT
Electronic communications security has gained a considerable significance in parallel with the increasing usage of the information and communication technologies. Being one of these technologies, distributed ledger technologies (DLTs), more specifically the blockchains, are regarded as a revolution which propose a new era, called "blockchain of things" following the era of "internet of things". While DLTs promoted the business functionalities and compliance with information security obligations, it has also some vulnerabilities. By the DLTs the cost of intermediaries could easily be eliminated while at the same time assets/transactions are recorded and secured digitally. Nevertheless, this has simultaneously resulted in decentralised power/anarchy. Besides, majority of the studies focus on the contributions of the DLTs. This article aims to concentrate on the security aspect of this technology, which is often disregarded. Thus, after addressing fundamental characteristics of DLTs, it will unfold their tools and advantages in terms of compliance to information security obligations, then, exercise its vulnerabilities and related risks with respect to information security legal frameworks from over the world.
*Keywords:* distributed ledger, blockchain, encryption, anonymization, information security

# Dağıtık Defterler ve Bilgi Teknolojileri Hukukundaki Yansımaları

ÖZ
Elektronik haberleşme güvenliği, bilgi ve iletişim teknolojilerinin artan kullanımına paralel olarak kayda değer bir önem kazanmıştır. Bu teknolojilerden biri olan dağıtık defter teknolojileri (DLT'ler), özellikle blokzincirler, "nesnelerin interneti" çağının ardından "nesnelerin blok zinciri" olarak adlandırılan yeni bir dönemi çağrıştıran bir devrim olarak kabul edilmektedir. DLT'ler, ticari işlevleri ve bilgi güvenliği yükümlülüklerine uyumu sağlamakla birlikte bazı güvenlik açıklarına da sahiptir. DLT'ler sayesinde, aracılık maliyetleri kolayca ortadan kaldırılabilir, varlıklar/işlemler dijital olarak kaydedilir ve güvence altına alınır. Ancak, bu aynı anda adem-i merkeziyetçilik/anarşi ile sonuçlanmaktadır. Dahası, bu alandaki çalışmaların çoğu DLT'lerin katkılarına odaklanmaktadır. Bu çalışma, DLT'lerin genellikle göz ardı edilen güvenlik yönüne odaklanmayı amaçlamaktadır. Bu çerçevede, DLT'lerin temel özelliklerini ele aldıktan sonra, bilgi güvenliği yükümlülüklerine uyum açısından DLT'lerin araçlarını ve avantajlarını ortaya çıkaracak, ardından dünyanın dört bir yanındaki bilgi güvenliği yasal çerçevelerine ilişkin güvenlik açıklarını ve ilgili riskleri analiz edecektir.
*Anahtar Sözcükler: dağıtık defter, blokzincir, şifreleme, anonimleşme, bilgi güvenliği*

*Atıf Gösterme* Sümer Özdemir, N., (2023). Distributed Ledgers and Their Implications in Information Technology Law, *Kişisel Verileri Koruma Dergisi*. 5(2), 15-27.

*The views expressed here are personal to the author and do not reflect those of any regulatory authority.

The increasing usage of information and communication technologies has simultaneously necessitated establishment of electronic communications security. Distributed ledger technology (DLT), which is regarded as a revolution notably in finance sector, is a prominent example of these technologies. While it promoted both the business functionalities and compliance with information security obligations, it has also several vulnerabilities that need to be mitigated.

Information security issues have become a primary concern especially for financial institutions, whose fundamental function rely on the safe storage and communications of assets. To be more specific, for a traditional money transaction, a trusted third party is required between sender and receiver even if it is conducted in digital environment. Moreover, ledgers have been used to record information, particularly about assets like money and property. Yet via recent algorithms, it is possible now to create digital distributed ledgers jointly by all the users instead of a central controller (UK Government Office for Science, 2016). Thereby, the cost and workload of intermediaries could easily be eliminated while at the same time assets/transactions are recorded and secured digitally.

DLT is first introduced via blockchain technology of Bitcoin in 2008, and it paved the way for several sectors to facilitate their business operations and security standards. By decreasing the costs and eliminating intermediaries or trusts, increasing automation and enabling time stamping, DLTs provide a new ground of competition between the traditional finance companies and the fintech companies (Accenture, 2016). Yet, it has been implemented in several areas including diamond markets, disbursing of international aid payments, delivery of public services, provenance for goods and intellectual property (UK Government Office for Science, 2016).

With the increased potential of blockchains envisioned by businesses, governments and regulators have started discussions on DLTs. Federal Reserve Board and Security Exchange Board in the United States, Financial Conduct Authority in the United Kingdom, European Central Bank of the European Union among all the others have started to recognize advantages of DLTs while at the same time started to monitor the regulatory risks (EU Blockchain Observatory and Forum, 2019). Switzerland[1], France[2], Hong Kong (Lexis PSL TMT Team, 2018) governments had declared initiations to adopt DLT-friendly

[1] 'Switzerland's Blockchain Legal Framework Adopts Friendly Bottom-up Approach' (*Cryptotapas*, 3 January 2019) <https://www.cryptotapas.com/switzerlands-blockchain-legal-framework-adopts-friendly-bottom-up-approach/> accessed 9 February 2019.

[2] 'France Pioneers Blockchain Legal Framework for Unlisted Securities' (*Clifford Chance*, January 2018) <https://www.cliffordchance.com/content/dam/cliffordchance/PDFDocuments/Client%20Briefing%20-%20France%20-%20Blockchain%20for%20unlisted%20securities%20180750-4-2....pdf> accessed 3 March 2019.

legal frameworks or attract DLT-based investments. Estonia's government have already implemented blockchain-based health services in e-government.[3] As for Turkiye, reports addressed the potential of country to become leader in DLT-based economy having regard to its young population, geopolitical position and economic potential (Turkish Republic Ministry of Environment, Urbanization and Climate Change 2022, 107-109[4]; Presidency of Strategy and Budget, 2023). Furthermore, recent security incidences and huge amounts of fines boosted the use blockchains/DLTs in other areas as well. Thus, not only have the governments been seeking for comprehensive regulations but also businesses consider DLTs as an effective way of compliance.[5]

Nevertheless, as the usage of blockchain has increased, debates are polarised over the issue of decentralised power and anarchy. Yet, replacement of the term "internet of things" with "internet of blockchains" induced the concerns regarding lack of legal control. However, this perception is found similar with the one when internet was first emerged. Though anticipation for internet was "a wild west" that falls beyond the reach of law, it is pertinent that the law soon was adapted to online world and an effective control over internet is being implemented now (Filippi and Wright, 2018; Lexis PSL TMT Team, 2018).

Likewise, governments have already alerted to identify how to regulate the DLTs [6] and also incentivise investments in that technology. Many countries acknowledged the need for legal certainty and proposed regulatory regimes for the DLT-based applications, afterwards. In that respect, Markets in Cryptoassets Regulation, the leading example of a crypto assets legislation, have been enacted in the EU. Similarly the authorities in the EU and Turkiye work on introducing digital Euro and digital Turkish Lira, respectively[7].

Notwithstanding above points, on one hand DLTs are simple databases for recording and safeguarding the information/transactions. On the other hand, they are vehicles to empower applications which in the

[3] 'E-Governance' (*e-Estonia*) <https://e-estonia.com/solutions/e-governance/> accessed 4 March 2019.
[4] For that purpose, open data platforms, particularly blockchain-based geographic information systems, approval of notary records and listing of land records are encouraged.
[5] Like BASELIII, SWIFT, Visa (UK Government Office for Science, 2016; European Network and Information Security Agency (ENISA), 2014)
[6] New York State Department of Financial Services started to regulate Bitcoin via requiring licence to businesses offering digital currency services to New York residents.
[7] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf; https://www.sbb.gov.tr/wp-content/uploads/2023/09/Orta-Vadeli-Program_2024-2026.pdf, p.67 accessed 4 November 2023.

end could totally alter current way of business operations (Lexis PSL TMT Team, 2018). Although it has become a hot debate topic, security aspect of this technology is virtually disregarded. Thus, this article will first highlight the definition, and fundamental characteristics of DLTs, then, unfold its tools and advantages in terms of compliance to information security obligations, lastly, exercise its vulnerabilities and related risks with respect to information security legal frameworks. As the security aspect of the DLTs represents an infant stage in most of the countries, legal frameworks from over the world will be illustrated with an aim to assist the countries in a multi-directional way.

## DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAINS

Distributed ledgers refer to asset databases which can be shared within a network and each of the participants of this network (i.e. nodes) has its own identical copy. DLT technology provides maintaining cryptographic records of electronic transactions by these nodes. Each record has a time stamp. Additional to recording, it can be used to validation, authentication and process of transactions or any other information exchange. No central authority functions in that system. Instead, updates are constituted independently by the users and each update is recorded after the majority agrees on and constructs a consensus. Transactions are established directly between senders and receivers (Lexis PSL TMT Team, 2018; Stephen and Alex, 2018).

Blockchains may possibly evoke the same meaning with DLTs, but they constitute just one form of DLTs. They are employed by groups of blocks of a set of information/document/transaction and cryptographically secured with a header consisting of the time of the block is set, a block reference number, and a hash that links the block to the previous ones (Lexis PSL TMT Team, 2018). Each block is engaged with another block. Data in a block cannot be changed, rather one can just add data to an existing block which gives the blockchain an immutability feature. Not all DLTs employ blocks that are tied together in a chain. Additionally, blockchains may be formed with a central authority or control may be distributed among nodes. But it is the very blocks that distinguishes blockchains from DLTs (Ray, 2019).[8]

There are various types of blockchains. The best classification can be made according to (i) types of

[8] Since the two are commonly used interchangeably, for the sake of this article to focus on compliance and regulation, no distinction will be made between each other. Albeit it is a large area to assess (includes smart contracts or cryptocurrencies etc.), technical characteristics are restrictively reflected in purpose to be able to focus on legal aspects of the technology.

nodes (validation/participation nodes) or (ii) accessibility to the network. Participation nodes cannot necessarily add data to the ledger, according to particular technology at hand, they may be required to apply to validation nodes to get permission. In terms of accessibility, public blockchains can be accessed by anybody and anyone who has adequate computer knowhow can join the verification of transactions in the network. Whereas, private blockchains are more akin to an intranet, i.e. established by private undertakings like companies, (government) agencies or consortiums and they set rules to control access and validation (Lexis PSL TMT Team, 2018; EU Blockchain Observatory and Forum, 2019).

According to abovementioned criteria several variants can be observed in practice. For instance, Bitcoin constitutes a public permisionless blockchain, where anybody can participate and also validate the nodes. It has no network owner and rules about registration, all nodes are able to see all data, but have the freedom to encrypt the data they use and apply to a third party intermediary in order to disguise its address. By contrast, in private permissioned blockchains which are particularly used in financial institutions, nodes are subject to approval of the controllers. Moreover, specific rules can be established to govern who can see which data (Lexis PSL TMT Team, 2018; EU Blockchain Observatory and Forum, 2019).

## CONTRIBUTIONS OF DISTRIBUTED LEDGER TECHNOLOGY TO COMPLIANCE

One of the major strengths of blockchain is its contribution to fundamental objectives of information security. It ensures the accuracy and completeness of information and processing methods via its two revolutionary features. First, each node has identical copies of the ledger, and each addition to ledger simultaneously updates all other copies. To be able to hack the system, at least 51% of the nodes should be falsified which is deemed almost impossible by the proponents of the technology. The risk of mere dependency on a third party intermediary is eliminated as it is governed by individuals from all over the world (Park and Park, 2018: 165–166; UK Government Office for Science, 2016: 47–48).

Second, besides the network security itself, a considerable degree of security for individuals can also be ensured. Information in each block are recorded by their hash values which are attained according to hash values of the previous nodes. During the transactions, digital signature of the participants is also verified via an electronic signature algorithm. Yet, in order to attack an asset (wallet in the case of Bitcoin) the attacker needs to obtain both the private and public keys. In this way, the encryption verifies that the information in each block is not altered. Even in case the data is altered, its time can easily be monitored by tracking the change in hash values. Thus, these two features are proposed to maintain and secure a high level of integrity and consistency of the information (Park and Park, 2018: 165-166; UK

Government Office for Science, 2016: 47-48).

One projected area of this feature is know-your-customer processing. Currently, financial institutions are legally required to identify their customers and their source of assets against money laundering or terrorism financing. Since the process is complex and costly, use of blockchain for a know-your-customer database where data is encrypted and can be accessed via permission of customers on as-needed basis is suggested to streamline this obligation (Filippi and Wright, 2018: 653).

Third proposed strength is transparency. As information held in the blockchain is accessible to all participants, the need for a third party verification is eliminated. While this brings a cost-reduction advantage for businesses in terms of information security, it enables a transparent access to both auditors and regulators. This may pave the way for, in particular, financial institutions to comply with regulations like Sarbanes-Oxley Act[9] under which they are obliged to conduct regular internal/external audits, or NIST[10] where transparency is underlined as a way of compliance.[11] Similarly, it would ease the process of certifying with private standards.

Fourth, most information security incidences are results of or at least contain human error. A joint study conducted by the Stanford University and a security firm in 2022, reported that 85% of data breaches are caused by human error.[12] By increasing automation, security risks from employees/third parties may be decreased. This would streamline the information security governance.

## LEGAL ISSUES

DLT is projected to shift traditional business to a new paradigm; however, it is still a maturing technology. Thus the existing law lacks ability to adequately cover all the aspects. Additionally, how to apply information security law to blockchains has not attained much attention yet (The EU Blockchain

[9] 116 Stat. 745, §103.

[10] National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (National Institute of Standards and Technology 2018) NIST Cybersecurity White Paper 19 <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> accessed 14 April 2019.

[11] In Turkiye, the direct and indirect use of crypto assets in payments transactions, the provision of payment services and electronic currency exports is forbidden via a regulation issued by the Central Bank (2021). The Regulation defines crypto assets as "*an intangible asset representing a value or right that can be created and stored virtually through distributed ledger technology or any other similar technology and that can be distributed over digital networks*". This definition distinguishes crypto assets from capital markets instruments. See https://www.resmigazete.gov.tr/eskiler/2021/04/20210416-4.htm, accessed 4 November 2023.

[12] Similarly, 95% of security incidents involve human error as a contributing factor (ENISA, 2015:20).

Observatory and Forum, 2019: 15). Rather, current studies focus on how blockchains can apply to different sectors[13] or how to cover blockchains in regulations (ENISA, 2014; UK Government Office for Science, 2016). However, its vulnerabilities exercised below, should not be underestimated due to the risk of non-compliance with information security frameworks. Countries mostly do not have a single regulation, rather the information security frameworks represent a range of standards like General Data Protection Regulation (GDPR) or sector specific compliance regulations like Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act in the USA. Yet, a robust cyber security system could be established with the knowledge of all. Thus, the study will concentrate on the DLT related legal issues from all over the world.

First, in terms of vulnerabilities, private keys are considered to be the most notable part of blockchain security. Taking Bitcoin as an example, due to common usage of personnel computers or smart phones of nodes, malwares can penetrate easily through e-mails, USBs or applications and it is open to reuse attacks as well as other attacks. Taking into account these risks, some studies do raise concerns on the immutability of the technology, arguing 51% of the nodes can be falsified with developing computer techniques (Park and Park, 2018: 166). Some scholars further this idea by envisaging that in ten years quantum computers will have the ability to solve one way encryption model of blockchains (Fedorov et al, 2018).

In that respect, public blockchains are more prone to security incidences compared to private ones. Though compulsory for just the United States government agencies, NIST requires a particular care to information systems where public access is allowed. It states security controls should be applied with discretion since some control baselines like personnel security controls may not be applied for public access.[14] In those cases, sandboxing can be considered as suggested by UK Cyber Essentials Scheme, a voluntary certification standard though government suppliers obliged to comply with. It proposes sandboxing in the use of applications as a way of creating an isolated environment with a limited access to the rest of a device or a network, so that, other files or applications that are not related to transaction at hand can be kept beyond the reach of malwares.[15] By this measure, for instance, governments can separate security of each blockchain-based function such as voting, health-tracking, e-residence etc. from each other.

---

[13] 'Accord Project' <https://www.accordproject.org/faq> accessed 14 April 2019.
[14] NIST, p.57.
[15] 'Certification' (*Cyber Essentials*, 27 September 2017) <https://www.cyberessentials.ncsc.gov.uk/getting-certified/> accessed 13 April 2019.

Second issue is about data anonymisation. GDPR and Turkiye's Personal Data Protection Law does not apply to data processing if it has been anonymised. Nevertheless, to be able to meet GDPR standards, Article 29 Data Protection Working Party (2014) stated that the anonymisation techniques should be robust enough across (i) reversal and (ii) linkability risks. In other words, (i) encrypted data should not be re-established for instance by brute-force-decryption, (ii) the individual should not be singled out or linked to a data for instance by following the usage patterns or context or combining with any other information.

To be precise, firstly, encryption of data can be classified as reversible and non-reversible (hashing) for the sake of analysing blockchains. Reversible encryption corresponds to obfuscation of data where only the person who has the key is able decrypt it. This type of encryption may be symmetric where exactly the same key is used for both encryption and decryption, or asymmetric, where security is increased by using a public and secret key as is the case in public blockchains (The EU Blockchain Observatory and Forum, 2019: 20). Yet, even in asymmetric encryption, it is hard to contend that the algorithm is impossible to break. In 1970s, case of RSA algorithm[16] illustrated this argument (Kuszmaul, 2019). Furthermore, recent incidences pertaining Bitcoin also demonstrated how this vulnerability can transform into a security issue (Lee, 2017).

In that respect, on some public blockchain transactions, addresses of senders and receivers are visible. Past security incidences illustrated that actual users can be identified by following patterns of transactions in combination with other data. Even data is encrypted with high level security, the key remains somewhere making data reversal possible. The EU Blockchain Observatory and Forum (2019: 21) regards reversibly encrypted personal data as just pseudonymised data and reasonably argues that GDPR continues to apply them. Similarly, Turkish Data Protection Authority (2018:39) underlines the significance of ensuring the data is anonymous and suggests statistical methods like k-anonymity, l-diversity, t-closeness to strengthen the anonymity of the data in order to prevent data reversal. Besides, HIPAA distinguishes de-identified health information from the personally identifiable information, and considers it adequate only if the remaining information could be used to identify the individual. In order to de-identify information, either (i) a formal determination by a qualified statistician or (ii) removal of specified identifiers is required. Due to immutable feature of blockchains, they may not utilise the safe

[16] RSA algorithm, which was invented by Rivest, Shamir and Adleman, is the most popular public key algorithm. It was deemed as the key is uncrackable, yet by detecting the common factors among separate public keys, 12.934 public keys were broken among 6.2. million ones.

harbour that HIPAA provides unless they remove identifiers.[17]

Contrary to reversible encryption, hashing creates a unique and fixed size of characters for each data input meaning that reversal is no longer possible. Each hashed data is different from others such that they are also called as digital fingerprints. However, it should be noted that robustness of hashing algorithms can also differ in itself. Article 29 Data Protection Working Party (2014: 20) distinguishes some hashing algorithms from others, where the range of input values are limited and easy to be replayed through the hash function. For instance if national identification numbers are used as input to a hash function, data can easily be revealed by hashing all possible input values and comparing the results with existing one. To eliminate this risk, several mitigation methods are recommended such as salting or peppering i.e. including additional data to input.

In that respect, question of whether hashing personal data in blockchains provides full anonymisation or just pseudonymisation arouses attention as hashing function resembles the most notable characteristics of blockchains. Nonetheless, the answer could not be clarified yet for two reasons. First, it depends on the particular hashing algorithm used. Second, no supervisory authority or European Data Protection Board or a jurisdiction has addressed this issue yet (The EU Blockchain Observatory and Forum, 2019: 20-21).

Moreover, *staysure.co.uk* case, where hackers could identify the keys used in encryption and decrypted payment card information of customers, illustrates the significance of proper encryption. Information Commissioner's Office found it liable by not taking sufficient safeguards, wrongly retaining CVV[18] numbers, and failing to delete completely because of human error which is also not compliant with PCI-DSS.[19] One conclusion can be drawn from this case for blockchains in addition to adequate encryption is to retain minimum personal data as possible. Since it is not possible to delete/rectify data once added to chains, blockchains contain risk of non-compliance with data minimisation principle which is employed in several standards/regulations.[20]

[17] 45 C.F.R. § 164.514(b)
[18] Card verification value/card control numbers.
[19] Payment Card Industry-Data Security Standard. 'Breach of Payment Card Data Security Standard Leads to £175,000 ICO Fine for Insurer' <https://www.out-law.com/en/articles/2015/february/breach-of-payment-card-data-security-standard-leads-to-175000-ico-fine-for-insurer/> accessed 13 April 2019.
[20] For example, PCI-DSS requires in its first milestone to remove sensitive authentication data and limit data retention, HIPAA (45 CFR 164.502(b), 164.514(d)) imposes minimum necessary requirement to limit unnecessary or inappropriate access to and disclosure of protected health information.

Another derived consequence of encryption method would affect the coverage of blockchains under state data breach notification laws. For example, Alaska security breach notification law covers information in any form on an individual that is "not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired".[21] Thus, in case an organisation operating via the blockchain technology suffers from a security attack, it may possibly have to notify the breach if the data accounts for personally identifiable information.

Second issue regarding anonymization is linkability risk which also relies on the specific algorithm. If for instance, a complicated set of data is used to hash a transaction and also dataset is salted with random characters, it may be more difficult to re-identify personal data. Whereas, if just hash of the address of an individual is sent to ledger to authorize a transaction, after a while, it would be possible to monitor behavioural patterns such as time and frequency of transactions. Even the whole transaction can be revealed in case additional information is linked to the transaction (The EU Blockchain Observatory and Forum, 2019: 22). Consequently, maximum level of protection should be pursued to eliminate linkability risk arising from pattern analysis.

This risk came into practice with *JCDecaux* case in France. An advertising company, JCDecaux asked authorization from French data protection authority for a pedestrian tracking system which captures MAC addresses of smartphones in a street via devices located on billboards in a street for a four-week period. The purpose of the company was just to conduct a quantitative analysis to estimate the flow of pedestrians and apply a salt-hashing to eliminate identification risk. Not surprisingly, neither authority nor the appeal court authorised this application since, inter alia, it was not compatible with anonymisation standards due to linkability of location records relating to the same individual.[22]

A last point worth underlining is the enactment of the Regulation on Markets in Crypto-Assets (MiCA) by the EU in May 2023, which represents a comprehensive law specifically dedicated to crypto-assets, one of the main applications of DLTs. By designing rules for the provision of crypto-assets that fall outside the scope of the EU legislative acts on financial services, it is aimed to eliminate the risks to the

[21] Alaska Statute §45.48.010.

[22] 'The French Conseil d'Etat Says "non" to JC Decaux and Deals the Final Blow to Its Plan for a Pedestrian Tracking System on Advertising Panels' (*marketinglaw*, 24 May 2017) <https://marketinglaw.osborneclarke.com/advertising-regulation/french-conseil-detat-says-non-jc-decaux-deals-final-blow-plan-pedestrian-tracking-system-advertising-panels/> accessed 3 March 2019; Sophie Stalla-Bourdillon, 'Anonymisation, Pseudonymisation, WiFi Tracking and the French: The JCDecaux Case' (*Peep Beep!*, 12 April 2017) <https://peepbeep.wordpress.com/2017/04/12/anonymisation-pseudonymisation-wifi-tracking-and-the-french-the-jcdecaux-case/> accessed 2 March 2019.

holders of those crypto-assets as well as to market integrity, including in terms of both market abuse and financial crime, and to facilitate transparency, uniformity and security. The regulation brings provisions for the crypto-asset service providers and addresses obligations to have effective administrative arrangements to ensure that their systems and security protocols meet Union standards. Yet, these standards will be specified via guidelines which are meant to be issued by European Banking Authority and European Securities and Market Authority, until 30 December 2024 and the regulation will be fully implemented from 30 December 2024. Therefore, the question of how to apply the regulation to crypto-assets is not clarified in the time of this study.

## CONCLUSION

Overall, DLTs and in particular blockchains are expected to totally alter the way of businesses. Not only they provide significant cost-efficiencies and enhance business functionalities via automatisation, but also facilitate compliance with security frameworks. As each user has identical copies of the ledger, any information change is reflected to whole network, and information is either hashed or encrypted for accuracy and completeness. Thus, they contribute to confidentiality, integrity, availability of the information, provide transparency and also streamline information security governance.

Nonetheless, security aspect of these technologies should not be neglected. Though not emphasized as much as its advantages, DLTs are not risk proof. First, 51% attacks are not deemed impossible with the advanced technology. Especially in public blockchains, if private keys are identified, immutability feature would be eliminated. Second, data may not totally be anonymised under blockchains, rather pseudonymised. In that respect, data may be revealed either by reversing the encryption or linking it to other relevant data. Consequently, several techniques such as sandboxing and salting should be adopted and encryption/hashing functions should be employed with due diligence.

In conclusion, compliance is not just about the technology, it is about how the technology is used (The EU Blockchain Observatory and Forum, 2019: 28). Thus, in spite of these security risks, DLTs can continue their revolution in “blockchains of things” era. Nevertheless, security aspects should not be undermined for not becoming obsolete before maturing.

## BIBLIOGRAPHY

Accenture. (2016) Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking. *Everyday Bank Research Series* <https://www.paymentscardsandmobile.com/wp-content/uploads/2016/05/Final-Accenture-Payment-Services-PSD2-PoV-Web-April-2016-1.pdf> accessed 3 May 2023.

Article 29 Data Protection Working Party. (2014) *Opinion 05/2014 on Anonymisation Techniques* 0829/14/EN WP216. <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 4 November 2023.

European Network and Information Security Agency. (2014) Network and Information Security in The Finance Sector: Regulatory Landscape and Industry Priorities. <http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514150:EN:HTML> accessed 10 February 2019.

European Union Agency for Network and Information Security. (2015) *Information Security and Privacy Standards for SMEs: Recommendations to Improve the Adoption of Information Security and Privacy Standards in Small and Medium Enterprises* <http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML> accessed 4 November 2023.

Fedorov, A. K., Kiktenko, E. O. and Lvovsky, A. I. (2018) Quantum Computers Put Blockchain Security at Risk. *Nature*, *563*, 465.

Filippi, P. D. and Wright, A. (2018) *Blockchain and the Law: The Rule of Code* (2nd edn). Cambridge, Massachusetts: Harvard University Press.

Kuszmaul, W. (15 January 2019) The (Almost) Secret Algorithm Researchers Used to Break Thousands of RSA Keys. *Algorithm Soup* <https://algorithmsoup.wordpress.com/2019/01/15/breaking-an-unbreakable-code-part-1-the-hack/> accessed 3 May 2023.

Lee, Y.N. (12 December 2017) Bitcoin Hack: Expect Larger Cyber Attacks in 2018, A10 Networks Says. *CNBC* <https://www.cnbc.com/2017/12/12/bitcoin-hack-expect-larger-cyber-attacks-in-2018-a10-networks-says.html> accessed 3 May 2023.

Lexis PSL TMT Team (ed). 2018. *An Introduction to Technology Law* (1st edn). United Kingdom: LexisNexis.

The EU Blockchain Observatory and Forum. (2019) *Blockchain and the GDPR* <https://www.eublockchainforum.eu/reports> accessed 3 May 2023.

The EU Blockchain Observatory and Forum. (2018) No Law unto Itself: Blockchain and the European Legal and Regulatory Framework. *EUBlockchain* <https://www.eublockchainforum.eu/news/no-law-unto-itself-blockchain-and-european-legal-and-regulatory-framework> accessed 9 February 2019.

Turkish Data Protection Authority. (2018) *Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Rehberi* <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf> accessed 11 May 2023.

Turkish Republic Ministry of Environment, Urbanization and Climate Change. (2022) *Blok Zincir ve Metaverse Teknolojisi Çalışma Heyeti Sonuç Raporu* <https://webdosya.csb.gov.tr/db/cbs/icerikler/blokz-nc-r-ve-metaverse-calisma-heyet--raporu-20220823173218.pdf> accessed 4 November 2023.

UK Government Office for Science. (2016) *Distributed Ledger Technology: Beyond Block Chain* <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain> 3 May 2023.

Park, Jin and Park, Jong. (2018) Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry* 9, 164.

Presidency of Republic of Turkiye-Presidency of Strategy and Budget. (2023) *Medium Term Program 2024-2026* <https://www.sbb.gov.tr/orta-vadeli-programlar/> accessed 4 November 2023.

Ray, S. (20 February 2018) The Difference Between Blockchains & Distributed Ledger Technology. *Towards Data Science* <https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92> accessed 25 February 2019.

Stephen, R. and Alex, A. (2018) A Review on BlockChain Security. IOP Conference Series: Materials Science and Engineering 012030, 396.