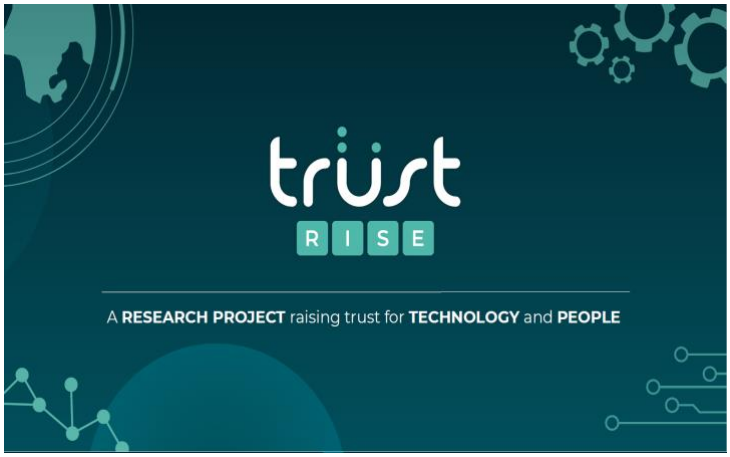

TRUST - digital TuRn in EUrope: Strengthening relational reliance through Technology

The *Digital Revolution*.
New Dimensions of Trust, Protection of Fundamental Rights, and Challenges for Contemporary Legal Systems

Policy Brief

Massimo Meccarelli (UniMc), Francesco Gambino (UniMc), Rafael del Asis Roig (UC3M), Ermanno Calzolaio (UniMc), Laura Vagni (UniMc), Oscar Celador Angon (UC3M), Andrea Raffaele Amato (UniMc), Elena Codoni (UniMc), Chiara Comberiati (UniMc), Alessandra Dignani (UniMc), Gabriel Faustino Santos (UniMc), Jacopo Fortuna (UniMc), Ludovica Ilari (UniMc), Chiara Iorio (UniMc), Beatrice Lupacchini (UniMc), Giorgia Vulpiani (UniMc)

trüst RISE

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement n. 101007820.
This document reflects only the author's view. The Research Executive Agency is not responsible for any use that may be made of the information it contains

The *Digital Revolution*.
New Dimensions of Trust, Protection of Fundamental Rights, and Challenges for Contemporary Legal Systems

The **digital change**, in an increasingly relevant way, is demonstrating an extraordinary innovative potential in terms of impact on people's lives, taking on an ever-greater importance for legal systems and their traditional categories. One of the challenges of the **TRUST** project: ***digital TuRn in EUrope: Strengthening relational reliance through Technology*** consists of investigating the new dimensions of trust implied by the technological and digital shift, considering its impact on legal change and its dynamics of adjustment.

To achieve this objective - from a methodological perspective - two relevant aspects need to be considered, which allow for a better understanding of the investigate phenomenon and provide valuable axiological coordinates for solving the problems emerging from the comparison between traditional legal systems and new innovative digital tools.

- The first factor is the ***temporal regimes*** inherent in the phenomenon of innovation itself. New digital technologies, in fact, follow transformation times that are misaligned with those that characterize the legal dimension. It is not just the speed at which they are realized, but also the very attitude towards change that distinguishes the technological from the legal sphere. While **technology** is necessarily projected towards its continuous improvement (***dynamism/transformation***), **law**, on the other hand, to fulfil its ontological function, tends to favour and maintain static configurations (***immutability/stativity/resilience***).
- The second factor concerns, instead, the **transdisciplinary dimension** of the problem. The digital shift, in fact, does not seem to be analysable from a single perspective - that strictly legal - but its understanding necessarily implies the involvement of different sources of knowledge, coming from different areas of law (public, private, international, administrative, etc.) and from the sectors of computer science, economics, ethics and history, which both policymakers and lawyers cannot do without. It is, naturally, a process that will only be able to express its structural effects in the long term - the outcomes of which are difficult (if not impossible) to predict - but which, nevertheless, cannot be approached without considering its intrinsic interdisciplinarity.

Combining, therefore, these two aspects, we have sought to investigate - from a legal perspective open to understanding the specificity of technological tools and their functionalities - the main innovations linked to the introduction of **Blockchain** and **new digital technologies** in the daily lives of their users (people, businesses, institutions, etc.). Starting from the very idea of a **decentralized system** - with all the implications that this entails in terms of privacy and consumer protection - or from the concept of **dematerialized goods** or **tools**, such as NFTs, Cryptocurrencies or Smart contracts, passing through the massive use of technologies based on **AI** in entrepreneurial or European Common Market contexts, reaching up to the ethical dilemmas raised by computer hacking to **Cybersecurity**. Trying to verify the compatibility of these new advanced technological tools with current **normative systems** (national and supranational) and trying to outline possible solutions (normative, regulatory, doctrinal, jurisdictional or soft regulation) that can make compatible the dynamism of technical innovation - in continuous and incessant transformation and implementation - with the resilience of law and its traditional categories, little inclined to radical change but inevitably

tending towards adaptation and transformation, if correctly understood and without prejudice towards the digital revolution.

The protection of rights and freedoms in the *Information Age*: innovative challenges and suitable legal solutions

There are many aspects of life where the advent of new technologies - and in particular **Blockchain** and other **advanced digital tools** - have had a significant impact, requiring legal systems to adapt to the change to better safeguard the **fundamental rights** and **freedoms** of both **users/utilizers** and **inventors/producers/suppliers**.

The relationship between law and new technologies is a theme that has developed progressively over time, taking on the value of an important factor of interest in contemporary society. This happened already with the first technological innovations of the 19th century - such as railways, telegraph, steam engines, electricity or the first internal combustion engines - which revolutionized the lives of hundreds of thousands of individuals in a very short period. The law, with its guiding value, often finds itself in crisis in the face of technical progress and the invention of tools or services that rapidly revolutionize life. Its inability to quickly keep pace with these advances produces an imbalance that challenges lawmakers and jurists to revise the existing regulatory system to implement it, to rethink old categories that have become inadequate (or even obsolete), to reinterpret institutions and principles in an innovative way, adapting traditional legal knowledge to face new unforeseen situations and emerging needs. Considering this, however, the role of law does not seem to be threatened, not even in these moments of crisis. Its centrality, in fact, continues to be an important factor in **promoting** and **developing trust** in new technologies, and this is because over time the performative force of its institutions (principles, categories, concepts, normative solutions, jurisprudence, etc.) has been able to resolve the conflicts that have emerged from technological implementation, guaranteeing an adequate space for the protection of the individual and their fundamental rights.

It is for this reason, then, that the advent of the most advanced technological tools must lead legal systems to renew themselves, without folding in on themselves - ignoring progress, or disregarding its innovative scope. It must push politics and legal science towards the resolution of new types of problems, identifying the best possible solutions to adequately combine technical development with the prerogatives (personal and patrimonial) of the individual.

Looking at the context of the European Union and its 27 Member States, at least seven main challenges can be identified that policymakers and legal interpreters must face today to ensure the use of new technologies in compliance with the standards of protection of fundamental rights and freedoms in the European common space. Here are the seven challenges:

1. Making **Regulation No. 2016/679** (**GDPR**) compatible with **blockchain technology**, ensuring its use does not endanger users' rights.
2. Implementing EU rules on digital tools to adapt them to the new issues arising from the spread of **Artificial Intelligence** (**AI**) systems.
3. Redefining some fundamental categories of private law to make them compatible with dematerialized assets, such as **NFTs** or **Cryptocurrencies**.
4. Reinterpreting the fundamental principles governing contract law and those ensuring the proper functioning of the European Market, adapting them to the use of intelligent tools like **Smart contracts**.

5. Devising solutions that can safeguard business actors from the use of **computerized procedures** that could threaten environmental sustainability or harm the correct assessment of relevant interests.
6. Harmonizing rules on land ownership to enable large-scale use of blockchain in **cadastral digitalization**.
7. Carefully assessing the ethical-legal weight that certain **Cybersecurity tools** can assume, thereby mitigating cyber threats to data security.

Blockchain and Regulation No. 2016/679 (**GDPR**)

One of the most pressing issues for the European legal system is undoubtedly the compatibility between **Regulation (EU) No. 2016/679** - the ***General Data Protection Regulation*** (**GDPR**) - and **Blockchain**. The main difficulty lies in reconciling two instruments - one regulatory (GDPR) and the other technological (Blockchain) - based on fundamentally different structural characteristics that appear to be incompatible. The GDPR is based on a centralized model with identifiable controllers and data processors, whereas Blockchain (especially in its permissionless form) is decentralized and lacks centralized control. The GDPR was introduced before the widespread adoption of blockchain, which explains why it was not designed to address the challenges posed by decentralized technologies. Despite these challenges, the European regulation represents the fundamental normative text that guarantees uniform protection of rights related to new technologies in the EU, and Blockchain must necessarily comply with it. The conformity of Blockchain to the GDPR depends more on the application modalities of the technology than the technology itself, which helps to understand why the solution to the problem cannot be univocal but depends on various factors that emerge in specific cases of use.

One of the primary concerns is identifying who can be considered the **data controller** in a blockchain network and, consequently, how users can exercise their GDPR rights. The main challenge is to balance the protection of users' personal data with the development and use of blockchain in compliance with the regulation. This entails significant obligations for data controllers (especially in the context of permissionless blockchain), where identifying them and applying the regulation remains an open challenge. Only specific regulations that consider the peculiarities of blockchain, adapting the GDPR requirements to different use cases, can guarantee effective protection of data subjects' rights without hindering its use. In this perspective, an interesting experiment is the **regulatory sandbox**, which has gained ground as a solution to address the challenges of regulatory inconsistency in **Distributed Ledger Technology** (**DLT**). The purpose of this sandbox is to enable regulators and supervisors to interact with innovators, share best practices, and improve their understanding of blockchain issues within a pan-European regulatory framework. The *European Blockchain Regulatory Sandbox* - promoted by the European Commission under the Digital Europe program - aims to create a safe regulatory environment to test and better regulate the use of this technology. Although the path is not without obstacles, the possibility of creating European "gold standards" for blockchain that can serve as a reference for other global jurisdictions appears significant.

In addition to these issues regarding the functioning of the blockchain network and its implications for the protection of individual rights in the EU, the GDPR also provides for strict controls on the transfer of personal data outside the European Economic Area (EEA), requiring service providers to ensure that such data is transferred to countries with adequate levels of protection according to EU standards. This requirement is particularly challenging to meet in a public blockchain where data is replicated across all nodes, regardless of their geographical location. One of the main

innovations of the GDPR is that compliance is not limited to European countries but extends to any entity offering goods or services in the European Union, regardless of whether they are European or not. All individuals and companies operating in the European Union will be responsible for processing personal data in their possession, must comply with various rules related to processing security, and must appoint a data protection officer, potentially facing severe sanctions in case of non-compliance. Even if data in the blockchain can be encrypted or pseudonymized, it is often possible to re-identify individuals behind transactions, thus violating the right to anonymity guaranteed by the GDPR.

Artificial Intelligence (**AI**)

In addition to imposing standards for the protection of personal data in Blockchain, Regulation (EU) No. 2016/679 (GDPR) also aims to create a unified legal framework for the development, use, and implementation of **Artificial Intelligence** (AI) systems within the European Union. Its main purpose is to ensure that AI is human-centred, reliable, and safe to use, oriented towards respecting and protecting the fundamental rights of individuals (privacy, health, safety, etc.) and free from abusive conditioning by third parties. In this regard, the GDPR promotes technological innovation and protects consumers from unfair practices. To this end, European legislation defines several key concepts, such as "**AI system**" - which includes any system capable of making predictions, recommendations, or decisions with varying degrees of autonomy -; "**biometric data**" and "**emotion recognition**", regulating the use of this information to avoid ethical and privacy issues. In parallel, under the GDPR, "**responsible parties**" / "**providers**" - defined as those who develop or market such systems - are required to ensure that their products comply with European standards and that constant conformity assessments and post-service surveillance of the systems are carried out. The regulation also establishes specific authorizations for "**sensitive contexts**", and the provision of a clear framework for surveillance in the event of data breaches. It is up to national and EU supervisory authorities to ensure that the use of AI meets the highest ethical and security standards to protect users from abuse by service providers/operators.

NFTs and Cryptocurrencies

Another highly topical issue is related to **non-fungible tokens** (**NFTs**) and **cryptocurrencies**, which represent a significant challenge for traditional legal categories. Currently, intellectual property rights related to NFTs remain ambiguous. The purchase of an NFT does not necessarily transfer the underlying intellectual property rights, unless explicitly stated. Discussions among jurists on the topic suggest that intellectual property protections (including copyright and trademark laws) are applicable to NFTs. As the NFT market continues to grow, it is likely that legal issues related to copyright, registered trademarks, and digital art protection will evolve significantly. Artists and creators may need to adapt their practices to account for both traditional and digital protections, while legal systems must continue to adapt to the specific challenges posed by NFTs, clarifying their status as autonomous works of art or simple digital representations of existing intellectual property. This finding inevitably leads to considering the issue of civil liability related to the creation and circulation of NFTs. Currently, Italian law regulates Distributed Ledger Technologies (DLT) and smart contracts through Article 8-ter of Law 12/2019. This provision defines DLTs broadly but does not specifically address the topic of NFTs. At the supranational level, **Regulation (EU) No. 2023/1114** - the ***Markets in Crypto-Assets Regulation*** **(MiCAR)** - excludes NFTs, focusing instead on fungible cryptocurrencies. This regulatory gap leaves disputes related to NFTs to be resolved based on general principles of contract and property law. Given the diversity of NFTs, their legal treatment may require a case-by-

case analysis. Some NFTs, such as those representing financial products, may fall under securities regulations, while others may be more closely linked to property or contract law frameworks. Another emerging issue related to NFTs - but also concerning cryptocurrencies - is their inheritance regime. As digital assets, both NFTs and cryptocurrencies can theoretically be included in wills or trusts. However, among the practical challenges is access to the private keys necessary to transfer NFTs and cryptocurrencies posthumously, which highlights the importance of succession planning that considers digital assets. A possible solution to ensure the transmission of digital assets is the "digital legacy" or "password legacy" model, where access credentials are included in a will or securely stored for the heir. In this model, credentials serve as a "key" that guarantees access to digital content or assets, such as NFTs or cryptocurrencies. Despite growing awareness that digital assets can be part of a person's estate, legal innovations and more detailed solutions are needed to ensure the smooth transmission of these assets.

Blockchain and Smart contact

In the context of the European Market, **Blockchain** poses disruptive challenges, as it has the potential to reshape multiple economic and legal dynamics, including those governed by European competition law. The ***Treaty on the Functioning of the European Union*** (**TFEU**) prohibits agreements, decisions by associations of undertakings, and concerted practices that have as their object or effect the restriction or distortion of competition in the internal market. In this sense, Blockchain can play a variety of different roles. On the one hand, it could become a venue for anticompetitive agreements; on the other hand, its inherent transparency could serve as a compliance tool, allowing for precise traceability of certain transactions and thus limiting opportunities for clandestine collusion. Since the technology is based on shared protocols and consensus algorithms, it could theoretically facilitate coordination between market actors if network nodes use blockchain to agree on prices, allocate markets, or coordinate certain strategic decisions. One of the main practical difficulties in applying competition law to blockchain networks lies in the highly decentralized nature of the technology, which can make it difficult to identify with certainty the individual or individuals responsible for the illicit conduct and, consequently, subject to sanction. The European Commission will therefore need to adopt interpretive criteria capable of dealing with participation in a blockchain, or specific regulatory changes that can address emerging critical issues. Possible strategies for making the application of European law more effective, without stifling the potential of blockchain, include strengthening collaboration between Competition Authorities and regulatory bodies in the fintech and digital sectors. Secondly, developing dedicated guidelines for the blockchain sector that serve as indicators of possible collusion or abuse of dominant position. Finally, specialized training on blockchain for Competition Authority and Market personnel and judges is essential, given that analysis of potential violations requires not only legal expertise but also in-depth knowledge of distributed protocols, consensus algorithms, cryptographic methods, and community-based governance dynamics.

On the other hand, from a more civil law perspective - but still looking at the proper functioning of the common market - the use of **Smart contracts** can have a significant impact, not only on the falsification of competition rules, but also on the correct formation of the contractual will of individual consumers. In this context, the delicate problem of defects in consent determined by error, erroneous manifestation of contractual will, and possible computer error that compromises the functioning of the blockchain-based protocol, leading the consumer to make a purchase they would not have otherwise made. Smart contracts - due to their technical characteristics and peculiar self-execution - represent a significant risk for consumers, since the effects produced automatically by this software

(tendentially immutable) could be the result of a system error or could be far from the will of the contracting parties, modifying or completely vitiating it from the outset. The solution to problems of this type could be to adapt traditional civil law rules to the characteristics of the new technology, developing a new theory of error and contractual will that takes into account what can happen in the digital space.

New technologies and corporate governance

In recent decades, corporate practice has seen a massive use of new technologies, and an increasing number of entrepreneurial realities are using **Artificial Intelligence** to improve environmental sustainability goals. Not to mention that digital tools can be exploited to establish channels of dialogue and listening with stakeholders identified by the company, as well as to manage information flows and support the administrative body to comply with recent European regulations. Among other innovation sectors, hypotheses regarding the automation of corporate reporting are widespread, recently regulated by **European Directive No. 2022/2464** - known as the ***Corporate Sustainability Reporting Directive*** (**CSRD**). Artificial intelligence tools are indeed used to facilitate a reporting system capable of aggregating, processing, and communicating the necessary information for corporate sustainability obligations. Furthermore, the exploitation of blockchain technologies and smart contracts, especially for large digital companies, represents an opportunity to involve shareholders and stakeholders in business decisions, experimenting with forms of decentralization of decision-making processes. However, most of these tools can also have a negative impact that needs to be taken into account. These technologies, while representing a valid support for the conduct of virtual business meetings - favoring greater involvement of shareholders and stakeholders in management decisions and strengthening the guiding role of the assembly or dialogue with institutional investors. At the same time, they can pose risks, such as in the application of artificial intelligence based on data analysis procedures derived from advanced machine learning mechanisms, unfairly discriminating stakeholders of equal merit. From a legal perspective, the main issue is defining the liability of directors for decisions made based on intelligent technology, primarily when the assessments made by the algorithm have led to financial, strategic, and operational choices inconsistent with the company's interest and, possibly, with the pursuit of sustainability goals. To date, there is no specific regulation at the European level governing this phenomenon. However, it can be argued that the use of algorithms - although it can enable the optimization of recommendations and indications produced following already identified management and strategic objectives at the company level - cannot alone select relevant interests and make the necessary balancing, replacing directors in the task of directing the company.

Cadastral digitalization

The application of **Blockchain** to **land registries** - like any other technical innovation - inevitably involves both opportunities and risks. It is a slow and difficult process that in all countries of continental Europe depends on the systems adopted for the transaction of property rights and the related functions attributed to land registration. Undoubtedly, blockchain offers an opportunity to improve the efficiency of existing cadastral systems, provided that adequate adaptation and recognition of the legal relevance of this system are made. In this regard, there are many national legal systems that do not yet consider transactions carried out through blockchain as legitimate and therefore recordable in land registers. One of the main conditions for the application of blockchain technology in this field would therefore be the harmonization of the rules governing the registration

of land rights. This harmonization would make it possible to provide the population of the European territory with tools that facilitate access to cadastral services, making useful information on property registration available within the European Union and providing guidance for better management of cadastral systems in different jurisdictions.

Ethics of Cybersecurity

Blockchain technology has emerged as a powerful tool for addressing the complex ethical and legal challenges that arise in the field of **Cybersecurity**. Its unique characteristics, such as decentralization, transparency, cryptography, and immutability, have sparked considerable interest in finding innovative solutions to mitigate cyber threats. In this context, blockchain can be considered a key strategy for mitigating ethical risks, strengthening trust, ensuring data integrity, and promoting accountability in digital transactions. However, blockchain alone is not sufficient to address the entire spectrum of ethical risks in cybersecurity and must be integrated with other approaches - such as quantitative assessments of ethical risk - that provide a structured methodology for evaluating and mitigating potential threats. By combining blockchain technology with these quantitative assessment methodologies, interested organizations will be able to establish a more robust and ethically valid cybersecurity framework. However, to maximize the potential of blockchain in cybersecurity, it is necessary to:

- **Adopt ethical frameworks**. Principles of fairness such as beneficence, justice, and solidarity should guide the design and implementation of blockchain systems
- **Promote innovation**. Continuous research on hybrid models is essential to overcome the limits related to privacy, while preserving the strengths of blockchain.
- **Encourage collaboration**. Cross-sector partnerships are fundamental to address technical, legal, and ethical challenges, ensuring that blockchain solutions are effective and fair.
- **Improve transparency and trust**. Efforts to make blockchain systems more transparent and comprehensible will promote trust among stakeholders and encourage its wider adoption.

About TRUST Project

TRUST promotes an interdisciplinary research program, involving academic and non-academic institutions, in order to understand the role of trust in the implementation of digital technologies and suggest actual means of development.
Assuming that the digital transformation of European society can be fully achieved only if technologies evolve in a trustworthy environment, the project analyses the mutual influence between trust and digital technologies in order to raise relational reliance in people-to-people, people-to-business and people-to-authorities interactions.
The attention is on blockchain technology (BCT) as one of the most relevant forms of Distributed Ledger Technology. BCT is considered a trust-building machine as it creates new forms of relational reliance. BCT projects the issue of trust in a new dimension that we intend to explore, in adherence with the initiatives and key actions promoted by the EC in the Communication "Shaping Europe's digital future" (COM (2020) 67final), where it is remarked that trust and digital transformation of society go hand-in-hand.
The research and knowledge transfer programme evolves around key topics, such as: the development of a suitable regulatory framework for the effective integration of BTC in a trust-based society; the transition towards a fair and competitive peer to peer economy; the applications of BTC in the field of AI, to assure security and trust; the development of new models of collaborative governance for smart and trust-based cities.
The consortium gathers expertise from different backgrounds (legal, economic, engineering), belonging to EU countries, as well as Israel and China. Complementary research perspectives, innovative training and international/intersectoral cooperation will boost staff careers development by studying how the use of digital technologies can shape a trustworthy European environment, in which citizens are empowered in how they act and interact, and promote economic growth as well.

Partners of TRUST Project

Link to TRUST Project Website