European Commission

JRC TECHNICAL REPORT

Policy and regulatory challenges for the deployment of blockchains in the energy field

Work-Package 6

Fulli, G.

Kotzakis, E.

Nai Fovino, I.

2021

EUR 30781 EN

Contact information
Name: Igor Nai Fovino
Address: via E. Fermi 1, 21027, Ispra, VA, Italy
Email: igor.nai-fovino@ec.europa.eu

EU Science Hub
https://ec.europa.eu/jrc

JRC125216

EUR 30781 EN

PDF ISBN 978-92-76-40551-1 ISSN 1831-9424 doi:10.2760/416731

Luxembourg: Publications Office of the European Union, 2021

How to cite this report: Fulli, G., Kotzakis, E., Nai Fovino, I., *Policy and regulatory challenges for the deployment of blockchains in the energy field*, EUR 30781 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-40551-1, doi:10.2760/416731, JRC125216.

Contents

Foreword 1

1 Introduction 2

1.1 EC blockchain strategy 2

1.2 Digital energy and blockchains 4

2 Project Rationale and Technology Trends 6

2.1 Energy Industry DLTs piloting landscape 6

2.2 Research activities in DLT for energy 8

2.3 What the experimental tests demonstrated 9

2.3.1 The pros 10

2.3.2 Cons (i.e. implementation problems) 11

3 Blockchain in the Energy Sector, opportunities, barriers and policy needs 13

3.1 Energy digitalisation initiatives and blockchains 13

3.1.1 Policy context 13

3.1.2 Opportunities 15

3.1.3 Challenges and barriers 16

3.1.4 Policy and Regulatory Needs 19

3.2 Energy, Blockchain, Cybersecurity and Privacy 23

3.2.1 Policy context 24

3.2.2 Opportunities 29

3.2.3 Challenges and barriers 29

3.2.4 Energy Blockchain Cybersecurity Policy Needs 30

3.3 The role of standards in relation to DLT/Blockchain 31

3.3.1 ISO/TC 307 Blockchain and distributed ledger technologies 31

3.3.2 ITU Focus Group on Application of Distributed Ledger Technology 32

3.3.3 CEN and CENELEC Joint TC on Blockchain and Distributed Ledger Technologies 32

3.3.4 IEEE Blockchain Initiative 32

4 Final Considerations 33

References 35

List of abbreviations and definitions 38

List of figures 39

Foreword

This report represents the final deliverable of the energy blockchain project, financed by the European Commission DG ENER through ad-hoc funding coming from the European Parliament.

This report, after summarising the evidences, results and considerations emerged along all the phases of the energy blockchain project, illustrates opportunities, barriers and consequent policy needs concerning the use of blockchain in the energy sector.

1 Introduction

Among the various digital technologies and solutions, blockchain recently attracted much interest due its perspective manifold applications in the energy, climate and sustainability sectors. Blockchain indeed promises to support several European Union's climate-neutrality and sustainability policies, thanks to its potential to drastically change the market rules and streamline the decision-making processes and the system management mechanisms.

The policy and legislative initiatives on blockchains are moving their first but quick steps, worldwide and in the EU, with the financial sector being the most targeted due to the high interest concentrated on crypto currencies and their potentially disruptive effects on the banking and transactive economic sectors.

The regulations and policy actions on digital finance/blockchain represent an important reference for the energy system digitalisation as well, since financial transactions are at the core of the energy market operations and certain mechanisms aimed at promoting legal certainty and support innovation in the financial sector can well be borrowed and applied to the energy sector.

1.1 EC blockchain strategy

The EC blockchain strategy [1][2] includes the following legislative proposals and actions (see also Figure 1), meant to bring clarity and legal certainty first of all in the digital finance sector:

The Regulation proposal on Markets in Crypto-assets [3]. This proposal is part of a Digital Finance package aimed to further enable and support innovation and competition in the financial sector while mitigating the risks.

The Regulation proposal on a pilot regime for market infrastructures based on distributed ledger technology [4]. This proposal, besides introducing legal certainty and ensuring financial stability, aims to: support innovation, by removing obstacles to the application of new technologies in the financial sector and by promoting the uptake of technology and responsible innovation via a pilot regime; instil consumer and investor protection and market integrity.

A joint statement of the European Commission and the European Central Bank to explore the possibility of issuing a digital euro, as a complement to cash and payment solutions supplied by the private sector [5].

Besides the aforementioned initiatives, the EC's blockchain strategy includes [6],[7] (see again Figure 1):

- Developing joint visions and initiatives through a European Blockchain Partnership harnessing national blockchain efforts into a pan-European approach.
- Increasing funding for blockchain research and innovation, both in the form of grants and by supporting investment in start-ups.
- Financing the European Blockchain Services Infrastructure (EBSI). The EBSI is a network of distributed nodes across Europe aimed to deliver cross-border public services and enhance the way citizens, governments and businesses interact.
- Proposing a regulatory sandbox1 with blockchains in the financial, energy and other sectors (expected to become operational in 2021/22).

[1] A sandbox is a facility that brings together regulators, companies, and tech experts to test innovative solutions and identify obstacles that arise in deploying them.

- Supporting interoperability and standards adoption. The EU is involved in the work of international standard organisations and is engaging with global bodies.

Promoting blockchain education and skills development.

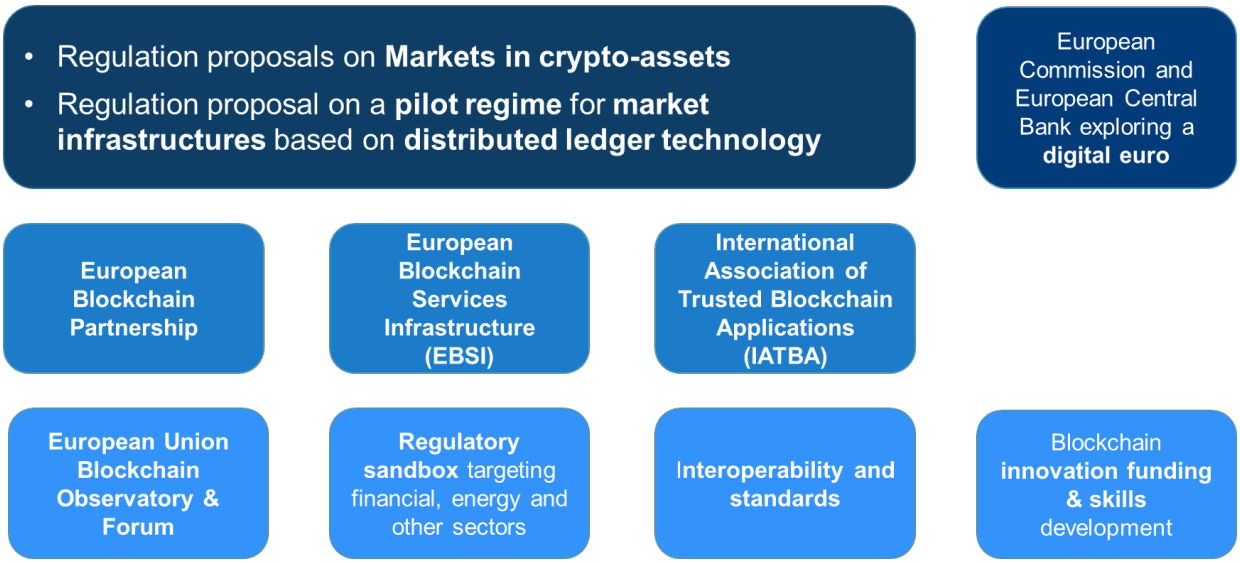

Figure 1 - EC Blockchain strategy

Of all the listed initiatives, two are extremely relevant from an "operational perspective", and for that reason, merit to be described further.

The first is the European Blockchain Partnership (EBP)2, establishing a cooperation mechanism between the European Commission, all EU Member States and some members of the European Economic Area (Norway and Liechtenstein). It is a joint public sector endeavour with the aim to reap the potential of blockchain to enhance the way citizens, governments and businesses interact, by enhancing trust between entities and improving the efficiency of operations, and to help create new business opportunities and to establish new areas of leadership.

The second is the European Blockchain Services Infrastructure (EBSI)3, which aims to support EU-wide cross-border public services or services in areas of public interest, in compliance with relevant regulation like GDPR (General Data Protection Regulation) 4 and eIDAS (electronic IDentification Authentication and Signature)5 and with the highest standards in terms of security, privacy or sustainability.

[2] More info about the European Blockchain Partnership, including the full list of EBP member countries can be found here: https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
[3] More info about the European Blockchain Service Infrastructure: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi
[4] Regulation (EU) No 679/2016: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[5] Regulation (EU) No 910/2014: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Today, EBSI is in the process of being materialised as a network of distributed nodes across Europe (the European blockchain), that will support an increasing number of applications focused on specific use cases.

Seven use cases were already selected by the EBP for EBSI and new ones will come gradually with a set of 20 potential use cases already identified. .

It is clear that there are gaps in existing blockchain solutions to enable the delivery of more demanding cross-border blockchain services (e.g. regarding higher performances, full compliance with the EU legal framework, security, interoperability, robustness, sustainability). For that reason, to further boost the take-off of blockchain technologies, the European Union's Horizon 2020 Research and Innovation Programme allocates funding for the blockchain Pre-Commercial Procurement (PCP), to focus on the development and testing of novel distributed ledger technologies or blockchain solutions. Such a public infrastructure should meet core requirements of scalability and throughput, interoperability with other systems, security, robustness, sustainability, energy efficiency and continuity of the service. It should build on the EU legal framework, in particular the GDPR Regulation, the eIDAS Regulation and the Network and Information Security (NIS) Directive6.

1.2 Digital energy and blockchains

The digital transformation is key to reach the EU's climate-neutrality targets and is already impacting the energy system design and operation.

In this context, the European Union recently put forward two ambitious overarching political initiatives, respectively in the green and digital fields, which display strong synergies:

- The European Green Deal is the EU's plan for the sustainable growth. It aims to contribute achieving the Paris Agreement objective of keeping the global temperature increase to below 2°C [8].
- The EU's Digital Strategy addresses crucial digitalisation issues relating to privacy, security, safety and ethical standards and promotes the deployment of an infrastructure fit for the future [9].

The above-described headline ambitions include new acts aiming to reinforce/complement (see Figure 2) digital energy-relevant legislative actions – such as the Energy Union/Clean Energy Package, the General Data Protection regulation, the Directive on security of network and information systems – proposed in previous policy cycles.

[6] Directive (EU) 2016/1148 : https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

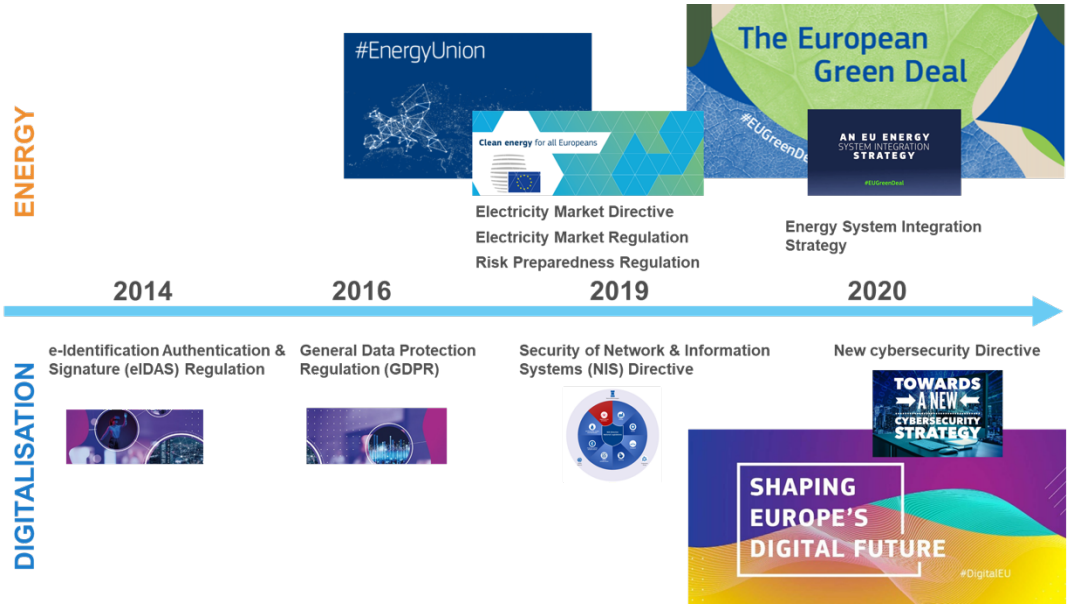

Figure 2 - Recent EU legislative initiatives on energy digitalisation [17]

Several energy digitalisation aspects tackled by the legislative acts illustrated above, can have direct or indirect effects on DLT deployment. They range from the resilience analysis of emerging digital technologies, to the definition of cyber-security tasks for system operators/digital service providers andfrom the assessment of security of energy supply in highly digitalised energy systems, to the production of regional risk preparedness plans coping with extreme cyber events. Additional relevant acts and initiatives regard the general data protection regulation addressing digital services, the harmonisation of electronic identification schemes used in digital platforms, the set-up of fair and shared data access and management procedures, the promotion of adequate digital energy system functionalities and interoperability properties the stimulation of growing digitalisation investments and the design of new digital-enabled market architectures.

2 Project Rationale and Technology Trends

The scope of this project was that of experimentally explore the use of distributed ledgers and blockchain technologies in the energy domain, in order to understand:

1. What is the maturity of the technology
2. What is its potential and in which specific subdomains of the energy sector could be applied
3. What are the current limitations
4. What are the barriers (if any) to the effective use of DLT in this sector.

The scope of this section is to summarise briefly the different pieces of evidence, results and considerations emerged along all the phases of the project in a coherent way, to then introduce the main subject of this report, i.e. the identification of opportunities, barriers and consequent policy needs concerning the use of blockchain in the energy sector.

2.1 Energy Industry DLTs piloting landscape

The study's landscape analysis, clearly showed that industrial actors in the energy domain are seriously investing in blockchain technology pilots and tests.

In the analysis conducted, it emerged how DLT is seen by industry as a potential means to enhance Transmission System Operators (TSOs) and Distribution System Operators (DSOs) network management capabilities by automatically maintaining verifiable data on network assets that can autonomously transact with each other.

In this context, DLT could help dis-intermediate the industry by transforming TSOs and DSOs roles of top-down energy providers - and possible single points of trust and failure in the energy supply chain - into peers operating in a horizontal network where also producers from DERs could freely interact with both industry and retail players.

In turn, DLT could be deployed to solve the new problems created by the interaction among traditional energy suppliers and producers from distributed and renewable energy sources. As documented in work-package 2 of this project, the actors in the industry are conducting research on DLT properties to improve confidentiality, integrity, and availability in the grid management services delivery.

One of the main domains of grid management, where tests are being carried-out, is smart metering, i.e. the increase of software implementations to give intelligence to electricity meters. DLT is one of the implementations that many industry players are exploring since it could offer data authenticity, integrity and asynchronous timestamping in order to optimise grid operations.

Another grid management niche wherein DLT has been prototyped is electric mobility, or e-Mobility. Alongside Artificial Intelligence, DLT smart contracts implementations have the

potential to revolutionise for instance the automotive industry together with the business environments of many other connected industries, e.g. public administration and insurance.

Expanding the landscape analysis taking into consideration the nexus between Internet of Things and DLT, this project highlighted another potentially disruptive aspect: in the energy domain, DLT might have, for example, the potential to reformulate the relationships among humans and machines with the mediation of automated transactions of different kind: energetic (energy availability), economic (energy pricing), environmental (weather forecasting), etc.

On a completely different level, many energy players are exploring DLT at the level of financial and business applications. In this domain, many of the business cases, typical of the FinTech world, are translated in applications for investment and value transfer backed by electricity.

As metering is a central component in grid management, the same applies to billing as it can be thought of as its business counterpart. In fact, cryptocurrency transfer is a property of DLT that is leveraged by both utilities and proponents of customer-centred business models in the energy sector, both in advanced economies and less developed countries.

As a subset of billing, a few actors in the power system industry are exploring the potential of DLT to address a widespread problem, namely imbalance settlement. DLT could indeed help to manage trust and energy value flow in time, by addressing inefficient and suboptimal approaches to reserve dimensioning, while increasing consumer protection, and optimise consumption and cash flow capabilities of all stakeholders involved.

These considerations can then apply also to wholesale energy trading practices. In this case, DLT can disrupt the industry by offering higher level of automation and disintermediation in an untrusted environment where the boundary between wholesalers and retailer would blur. Proponents of DLT in these types of use cases advocate for the deployment of DLT for the reduction of both transaction and operational costs in the transfer of energy and economic value in the industry.

Moreover, according to the vast majority of initiatives analysed, the division among wholesalers and retailers, producers and consumers would further decrease. Indeed, the case for DLT applied to the physical exchange of electricity and money peer-to-peer is considered as the most challenging, while potentially most disruptive for the industry. There are a good number of initiatives that provide DLT investment vehicles, such as Initial Coin Offerings to experiment especially in the Distributed Energy Resources (DER) and renewables domains.

Finally, the landscape analysis examined proposals for DLT applications for asset management (of e.g. renewable generation, fossil based plants and other climate-friendly or -altering assets). In these cases, DLT inherent properties, such as the distributed architecture, the timestamped, cryptographically secured and tamper-proof transaction history can offer tools for asset certification, proof of origin of energy production and green certificates and carbon credits trading.

Although the case for DLT application to the energy sector is a fascinating technical challenge, it is necessary to firmly stress that DLTs still have to demonstrate their viability, reliability and

possibly standardisation in all of these possible areas of deployment. If it is true that this technology can in principle offer many revolutionary breakthroughs in the electrical power industry and beyond, it is also true that at the time of writing the vast majority of projects and businesses do not go beyond the conceptualisation phase.

To our knowledge, there is not a standardised and solid framework for the deployment of DLT at the grid management and business application levels. Security properties do not yet offer mission critical levels of performance, especially to take products from the prototyping stage to real world in production environments at a mass scale. However, as it emerged from the landscape analysis and survey data, more research and development is underway in order to understand for what types of use cases DLT is a viable technology to be deployed in the energy sector.

The survey conducted among energy stakeholders confirmed the interest in DLT application within the energy sector, in particular to support uses cases in (a) Local energy communities (microgrids) and P2P marketplaces (b) decentralised exchange, (c) Retail electricity markets, (d) Flexibility services and proof of origin of supply or demand.

2.2 Research activities in DLT for energy

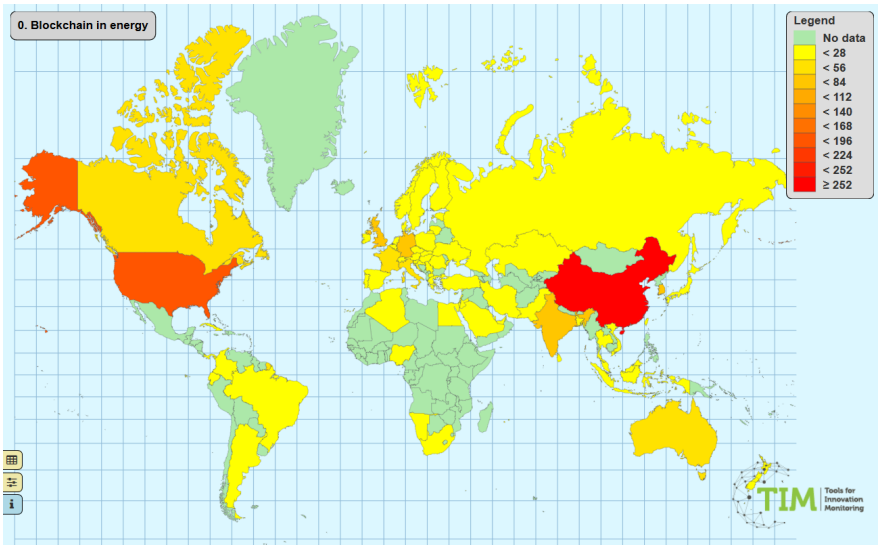

Figure 3: Country distribution of the publications on blockchain for the energy sector

Figure 3 shows the current world-wide trend in scientific publications concerning DLT in the energy sector. The dominant country is China with 262 publications, followed by USA within 205. In the European Union the leading country is Germany with 66, while the other major players are Italy and France with 51 and 34. In fact, the supremacy of these countries in EU is highly related with their developments in the energy domain itself.

Adding up the overall EU scientific efforts, brings EU to the forefront with 284 publications, demonstrating that the EU can lead the research and innovation in the energy systems supported by blockchain.

As far as patents in the blockchain-based energy field are concerned, China dominates the landscape, as it has registered more than 50% (146/253) of worldwide patents in this domain. US holds 7% (18/253) of the patents, while the EU companies hold only 2% of the overall patents. On one hand this contradicts the results of EU's scientific publications. On the other hand it might be the case where a) research institutes and universities in EU do not patent their research in this field, and b) related industries and organisations do not participate actively in research activities.

In the EU, Germany, Italy and France are leading the research field. However, research funding activities show high involvement of smaller players i.e., Greece that can boost their developments in the energy sector and blockchain.

Figure 4 summarises some clear indications on which domains raised higher interest.

Again, the trend confirms the results of the desktop analysis.

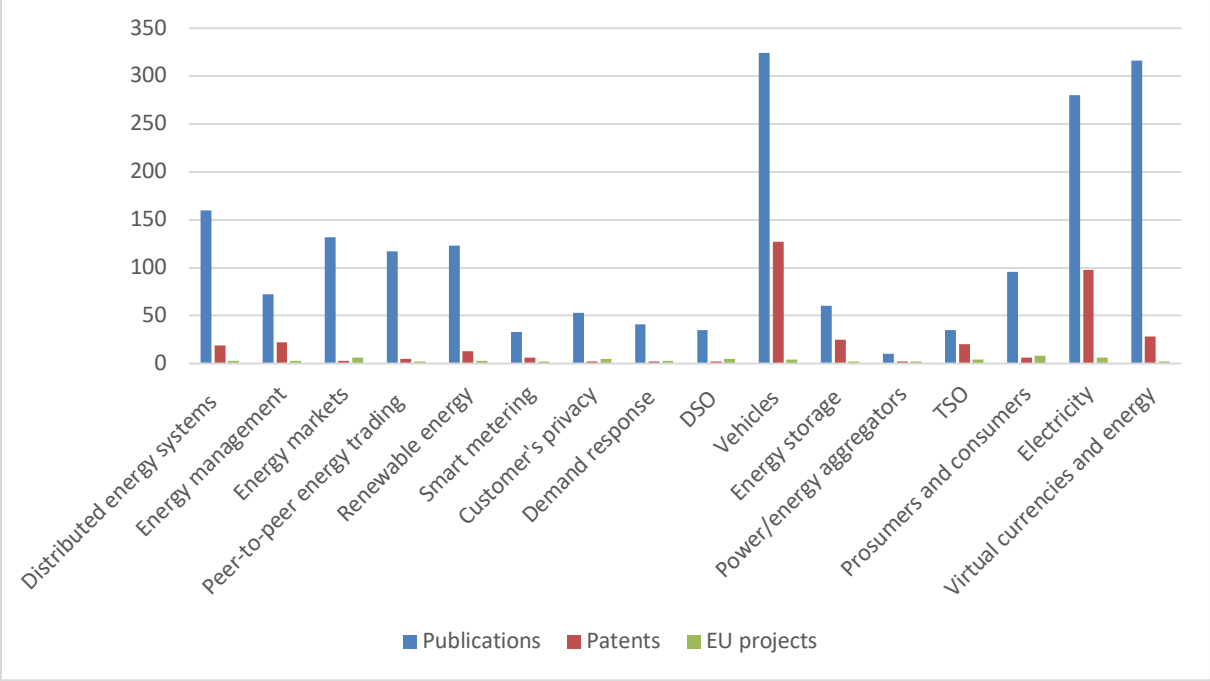

Figure 4. Comparison of the different energy domains

2.3 What the experimental tests demonstrated

The evidence emerging in the first part of this project, showed clearly that the energy industry is looking at DLT and more specifically at blockchain technologies as a potential way to change the energy operation paradigm. The second part of this project has been devoted instead to the on-field deployment of testing use-cases, to identify, first-hand, the potential advantages and problems which the use of this technology could pose in the near future. In particular, five different use cases have been selected for implementation, testing and analysis:

- Smart metering
- Energy communities

- Flexibility services
- Certification of origin
- Electro mobility

The report “Blockchain in the Energy sector, on field deployment and analysis of experimental use-cases” describes in details the technical deployment of the use cases, the testing setup and the obtained results.

A brief summary of what emerged from the tests is presented here below.

2.3.1 The pros

In general, the analysis has shown in all the cases the potential for a working and viable implementation of a blockchain solution.
In the energy flexibility use case, the simulations proved that the solution is scalable to thousands of assets. This can be assumed as the simulations were done on a per second basis whereas demand response events would typically take several minutes with a minimum of a settlement period (for example 15 minutes). The use of blockchain in this scenario will facilitate the service verification, the corresponding financial settlement and shorten the time for it in comparison to what is done presently. It will also allow for a communication of data between the TSO and DSO which is incentivised in the Clean Energy Package (CEP). The adoption of smart contracts and facilitation of demand response (DR) event tracing will enable the large-scale service provision, paving the way to citizen engagement and involvement in the energy market.

In terms of device resources consumption, the tests showed how the CPU utilisation is affected only by the number of transactions per second which needs to process, while the memory consumption is affected by both the number of nodes in the network and the number of transactions submitted. The tests showed however a moderated consumption of these resources, which, in devices designed to execute only this specific task, seems also acceptable.

The number of transactions per second processed and the end-to-end delay time are today adequate for the flexibility use case.

Lastly, in terms of resources, it is worth mentioning that the bandwidth is also influenced by both the number of (a) participants and (b) transactions per second submitted to the system, especially the ordering service as it is responsible to share the data with the corresponding entities. Thus, network resources should be defined properly in order to eliminate fundamental operational flaws.

The same type of considerations can be done for what concerns the e-mobility use-case that extends, de-facto, the DR use-case.

Since a typical DR event lasts no less than 900 seconds (15 minutes) and the seldom expected frequency of requests of such events, the systems would allow thousands of assets to be considered. Furthermore, it should be mentioned that asset power from the same aggregator will be added (aggregated), which decreases the effort requested to the blockchain. **These conditions suggest that DLT is more than capable of being implemented in a real-world scenario for DR in terms of event recording. Same considerations, in term of performances, scalability end-to-end delay are valid for the e-mobility use case.**

The smart-metering use case is in a way the "layer 0" of the Energy Community use case, meaning that, in that particular case it entails only the aspects concerning the notarisation of consumptions and billing, i.e., it is a pure case of transaction registry, that represents exactly the most straightforward use one could think of DLT use. Tests confirmed that DLTs used in this particular use case would not have any particular performance and scalability limitations. The same thing can be said for the "certificate of origin" use case, which is simply another application of the same "transaction validation and storing" functionality.

The full energy community use case, with smart-contracts controlling the neighbourhood energy market, distributed smart meters validating transactions etc. has been the most complex and challenging set-up to be implemented. However, the implementation deployed in the JRC labs demonstrated to be resilient, stable and scalable, even with in house built controllers and devices. There is hence no reason to think that an industrialised solution would not work with at least the same level of performance.

The logic implementation over a blockchain system showed that even computationally low-end devices, could be a client to a blockchain system and send transactions periodically. More importantly, it showed that integration between the "energy domain" and the "blockchain domain" is feasible in terms of technology and logic.

As a whole, the experiments and tests conducted on the deployment of the energy community use-case showed that **blockchain can be used as the distributed driving brain of such a system, being able to cope with performance, scalability and synchronisation requirements.**

2.3.2 Cons (i.e. implementation problems)

The implementation of the use cases goes beyond the setting up of the blockchain and smart contracts. Many factors should be considered for its implementation such as permissions, number of nodes or transactions per second just to mention a few, which impacts on the easiness of the implementation. Access to data (coming from the meters) was also a potential barrier as blockchains work using the most classical Internet protocols, and not all the meters support Internet connections. This poses obviously another important problem, which is the need for a stable Internet connection for the system to work properly. This is however a requirement which will be in general, more and more frequent with the digitalisation of the energy system; Internet will become a critical service needed to operate the grid. The still embryonic stage of blockchain platforms (and in particular, of smart contracts), is another obstacle to the deployment of complex automatisms as some functionalities are still under development.

The interaction with the existing systems was another challenging factor. In particular the integration with legacy systems, to gather readings and system data, constitutes today the biggest challenge.

This is the reason for which the energy communities use case, focused on the logic and the integrations of the "energy" and the "blockchain" worlds. To that purpose in-house smart-meters were built, with additional connectivity functionalities, able to interact with the blockchain directly.

The biggest challenge in such use cases, is how to trust the measurements and the "digital twin" of a physical object; in this case energy. Even if almost impossible to ensure a 100% trusted system, with the use of a common set of smart meters that independently register the measured energy, along with each household's smart meter measurements, we can assume that the level of trust achieved is reliable for such operations. The same problem is related to the use of blockchain for "certificate of origin": once the data is acquired and stored in the blockchain, is secure and there is no mean to tamper with it. The challenge hence is to ensure the security and integrity of the data before it reaches the blockchain. This is however a common problem of every cyber-physical system, and it is not limited to blockchain. Mechanisms to secure the acquisition of physical data are anyway already well understood by the energy community (for example in smart-meters).

Final considerations: the study demonstrated a clear interest of the energy industry toward the exploitation of the blockchain potentials. Pilots and use-cases are flourishing all around Europe. In house conducted tests, confirm the potential use of blockchain in this context, both in term of performances and scalability.

Trends show that the interest is mainly on the higher layers of the energy grids (energy management, flexibility, certification and billing), and in those situations where many stakeholders are involved at the same time, with different level of security and trust (the case of energy communities). Energy operations and generation are instead at the moment outside the blockchain game. This is mainly due to the lack (at the moment of redaction of this report), of adequate guarantee in term of safety, certification, and standardisation that are the driving requirements when concerning the operation of critical infrastructures.

3 Blockchain in the Energy Sector, opportunities, barriers and policy needs

As described in the previous section, blockchain and more in general DLTs have the potential to technically boost the digitalisation of the energy sector enabling the implementation of new features and new energy market paradigms.

To take-off successfully however, new policy initiatives are advisable to boost their development and adoption. The scope of this section is to first summarise the current policy landscape, highlighting then the sectorial needs and barriers, and then to come up with suggestions on future policy initiatives designed to support this innovative sector. Two perspectives will be presented, that of Energy digitalisation, and that of Energy cybersecurity.

3.1 Energy digitalisation initiatives and blockchains

3.1.1 Policy context

Energy digitalisation has to do with the improvement of the energy system performances via data, analytics and a deeper interconnectivity between humans, devices and machines, thus fostering different energy and economic sector integration [10][11].

The European Green Deal, put forward in 2019, repeatedly highlights the role of energy digitalisation towards a sustainable economy transition and in particular stresses that:

- the European energy market shall not only be fully integrated and interconnected but also digitalised;
- digital technologies are both a critical enabler of the Green Deal's sustainability goals and a large contributor to energy consumption increase;
- accessible and interoperable data, a modern infrastructure and artificial intelligence are key to innovate the energy system and the EU economy.

Attaining the objectives of the Green Deal, by reforming the energy system and market in accordance with the climate-neutrality objectives, first entails implementing key legislative provisions issued in the context of the Energy Union's begun in 2015. The most relevant ones - for the energy digitalisation process - are included in the Energy Union's Clean Energy for all Package and described in the following:

- the **Electricity Market Regulation 2019/943** [12]. As stated in its preamble, the electricity system shall integrate all available flexibility source, particularly demand side solutions and energy storage, and should make use of digitalisation through the integration of innovative technologies. The main energy digitalisation issues addressed in the Electricity market Regulation are:
    - The system operators (article 13) shall reduce the need for downward redispatch of renewables and high-efficiency cogeneration, making investments in electricity grid digitalisation and flexibility services.

    - Tariff schemes (article 18) shall provide incentives (to transmission system operators and distribution system operators) to increase system efficiencies, to foster market integration and security of supply, to support efficient investments, to support related research activities, and to facilitate innovation on digitalisation, flexibility services and interconnection.
    - The system operators (articles 30 and 55) shall promote digitalisation by deploying smart grids, efficient real time data acquisition and intelligent metering systems. The system operators shall support the development of data management, cyber security and data protection.
- the **Electricity Market Directive 2019/944** [13]. The main energy digitalisation issues addressed in the Electricity Market Directive are:
- Smart metering systems (articles 19-22) shall be deployed to assist the active participation of customers in the electricity market. Such deployment may be subject to a cost-benefit assessment and every final customer is entitled (upon request) to have a smart meter installed even if the cost-benefit analysis is negative.
- Data management and interoperability (articles 23-24). Member States shall ensure efficient and secure data access and exchange, as well as data protection and data security. Member States shall facilitate the full interoperability of energy services. The Commission shall adopt, by means of implementing acts, interoperability requirements and non-discriminatory and transparent procedures for access to data.
- Distribution system operators shall act as a neutral market facilitator and can procure flexibility services (articles 31-32), acting in accordance with transparent, non-discriminatory and market-based procedures developed in coordination with transmission system operators and other relevant market participants.
- Digitalisation is included among the tasks of the transmission system operator (article 40).
- the **Risk Preparedness Regulation 2019/941** [14]. Some of the cyber security threats associated with energy digitalisation are addressed in the Risk Preparedness Regulation. The Regulation recognises how, even where electricity crises start locally, their effects can rapidly spread across borders. Extreme events such as cyberattacks (or cold spells, heat waves and others) may affect entire regions at the same time. As a consequence, cyber-incidents need to be properly identified as a risk, and the measures taken to address them shall be properly reflected in the risk-preparedness plans. Hence, Member States shall develop national risk preparedness plans and coordinate their preparation at regional level, including measures to cope with cyber-attacks.

Within the Green Deal headline ambition, the energy digitalisation process and actions were reinforced by the following legislative act:

- the EU Strategy for Energy System Integration COM(2020) 299 final [15], representing a blueprint for actions to better interface different energy and economic sectors, including the digital one. The Communication recognises how digitalisation can: unleash the potential of customers (having a flexible energy consumption across different sectors) to contribute to renewables integration; enable interlinked flows of energy carriers; allow for

more diverse markets to be connected with another; provide more granular time/spatial data of energy supply and demand.

The EU Energy System Integration Strategy, among others, foresees the European Commission delivering three key products relating to energy digitalisation in 2021:

- The EC implementing acts on interoperability requirements and transparent procedures for access to data within the EU, as already called for by the Electricity Market Directive.
- A system-wide Digitalisation of Energy Action Plan, aimed to develop a competitive market for digital energy services that ensures data privacy and sovereignty and supports investment in digital energy infrastructure. This action plan could accelerate the implementation of digital solutions, building on the Common European energy data space, announced in the European Data strategy [16]: more specifically, the Common European energy data space is aimed to promote a stronger availability and cross-sector sharing of data, in a customer-centric, secure and trustworthy manner, as this would facilitate innovative solutions and support the decarbonisation of the energy system.
- A Network Code on cybersecurity in electricity, as requested by the Electricity Market Regulation, with sector-specific rules to increase the resilience and cybersecurity of cross-border electricity flows.

Several energy digitalisation aspects tackled by the legislative acts illustrated above, can have direct or indirect effects on the blockchain deployment as discussed in the next sections.

3.1.2 Opportunities

The transition to a climate-neutral economy - targeted by the Paris Agreement and the European Green Deal - requires the development of a global sustainability market, with the energy sector covering one of its largest shares.

Blockchain solutions - thanks to their decentralisation, immutability, transparency, security, verifiability, smart contract/tokenisation features - can enable and facilitate several segments of such marketplace.

In order to seize such opportunities, several governments, businesses and organisations are establishing collaborative platforms, to explore the blockchain potential in a variety of use cases.

In particular the following use case classes are singled out in the energy and sustainability fields [17]-[19]:

- Green Certificates and Carbon Credits: Blockchain promises to streamline fragmented and complex market structures for renewable certificates, carbon credits or general environmental attributes. Blockchain offers traceability of (renewable) energy produced and its tokenisation capability can create climate-related tradable digital assets, univocally identify stakeholders in a certain marketplace and develop new payment systems in the financial circuits.

- Energy crypto-assets & investments: The tokenisation, decentralisation and transactive-supportive features of blockchain and cryptocurrencies can support investments in energy assets/infrastructures and create new markets or business models based on co-ownership and sharing.

- Internet of (Energy) Things: Blockchains could improve architectural and operational features of the Internet of Things and the Internet of Energy Things, facilitating smart devices communication and automation, machine-to-machine interactions, asset management and the overall operation of networked internet-based platforms.

- Electricity metering and billing: When integrated with metering infrastructure, blockchains and smart contracts can provide consumers, distributed generators and prosumers with the opportunity of energy services, automated billing and perspective administrative cost reductions.

- Electricity market and trading: Blockchain-enabled distributed trading platforms might disrupt market operations such as wholesale market management, local trading within energy communities and flexibility service exchange within distribution grids or with transmission grids. The use of distributed ledger technology, with all transactions recorded in a decentralised ledger, can expedite and condense trading and settlement to nearly real-time [4].

- Electricity system operation and flexibility: Blockchains could assist (or even replace) human decision-making in running decentralised networks, providing flexibility services or managing power system assets.

- Electric mobility: The decentralised nature of e-mobility (including electric vehicles) makes them a natural application for blockchains, facilitating the transactions and interactions among vehicles, drivers/passengers and charging stations.

3.1.3 Challenges and barriers

Blockchain is a technology trialled in numerous energy use cases and applications, showing promising performance improvements. Still, several regulatory, legal, technological and operational issues hinder the deployment of distributed ledger technologies and crypto-assets, in the financial sector [4] and beyond. Some of the main obstacles to blockchain-enabled energy solutions deployment are as follows (security and privacy aspects are discussed more in-depth in chapter 3.2) [20]-[27]:

- Innovation and technology limitations. Innovation in the blockchain ecosystem is happening at a frenzy pace. A major challenge is to reconcile the clarity and stability of the legal framework, with the rapidity to react to the innovation changes in the digital energy systems [32].

  As much as potentially disruptive, most blockchain solutions show somewhat limited performances when it comes to optimising costs, speed (latency/throughput), node numbers, and security at the same time. Hence more research and innovation actions are needed before deploying large-scale blockchain applications in the energy system. Grants for blockchain projects are delivered in the EU primarily through the Horizon programme.

From 2016 to 2020, the Commission provided over EUR 200 million in prizes and grants through Horizon 2020 programme [1].

- Legal uncertainty and liability. In the currently tested blockchain-enabled energy ecosystems, the legal, financial and technical responsibilities are not clearly allocated among the actors (humans, machines and programs). Shall all consumers/prosumers in a decentralised peer-to-peer system be legally recognised as traders? Regulatory uncertainties also regard the applicable laws and jurisdictions for decentralised network operations and for smart contract execution. As stated in the EC proposal for the regulation of crypto-assets in the financial sector [1]: "There are no rules for services related to crypto-assets, including for the operation of trading platforms for crypto-assets, the service of exchanging crypto-assets against fiat currency or other crypto-assets, or the custody of crypto-assets. The lack of such rules leaves holders of crypto-assets exposed to risks, in particular in areas not covered by consumer protection rules". How can a smart contract - i.e. a blockchain-based computer program automatically executing instructions - be made legally binding? As also noted in [4], transparency, reliability and safety requirements are still missing on the protocols and the smart contracts underpinning crypto-assets. Clearly identifying roles and liabilities is particularly important in case of security breaches which could lead to financial losses, market anomalies or electricity disruptions. Those breaches could be linked to human/technical errors – such as loss of keys, issues in blockchain updates, smart contract malfunctions, payment defaults, technical failures - or malicious events and intentional tampering. Who is actually liable in case of those events?

- Data access and use restrictions. In most of the EU countries, energy consumption data can be mainly or uniquely handled by the distribution system operators. Blockchain pilots showed the potential advantages of automatically generating invoices and triggering smart contracts, provided that energy data can be effectively accessed and used. Currently there are several limitations and constraints on the legal possibility of exploiting data in a blockchain e.g. to activate smart contracts. Only by properly accessing metering data electricity customers can fully benefit from competition in the retail markets and contribute to innovative flexibility services provision.

- Market discrimination, consumer participation and silos approach. Fairness is an important criterion for designing more decentralised energy markets not discriminating any player, be they people or businesses. Independent aggregators currently do not participate in electricity markets on a level playing field with other operators/suppliers and practices preventing customers to contract agreements with emerging actors are still present. Also consumers are not fully engaged in digital energy projects and they often step out from pilots after an initial phase of interest [20]. The blockchain's promise to democratise energy cannot be held if many users cannot (afford to) be on board.
  Associating the appropriate distributed ledger solution to the different use cases is crucial as different blockchain technologies can enable much different electricity market governance schemes and role types for consumers. Most of the blockchain-enabled energy projects rely on Ethereum - in permissionless or permissioned configurations - or

other emerging technologies such as Hyperledger - with permissioned schemes. The permissionless design usually entails that every user contributes to manage the blockchain in a trustless environment (without a central authority supervising the interactions among peers). This however comes at a cost of a more expensive validation process. Permissioned applications need instead a small group of trusted and known nodes (either a man-in-the-middle or e.g. users within a microgrid or a company) to validate transactions; this allows for reducing the validation costs as only a fewer number of nodes need to interact to maintain the blockchain but also requires full trust on the validators.
Putting the customer at the centre of the energy system requires also changing regulatory approaches from silos-thinking to silos-breaking, identifying and exploiting more the possible interfaces and synergies between different energy systems (e.g. electricity, heat, gas,…) and economic sectors (e.g. transport, health,…). Market players will need to be able to identify and exploit use/business cases across interlinked energy and non-energy system configurations [27][32].

- Lack of interoperability and common standards. Several protypes and pilots have shown the urgent need for ensuring the interoperability of different blockchain solutions, of on-chain and off-chain systems, of IoT devices and cloud-based solutions with blockchain networks[7]. The more the power sector becomes coupled with other sectors such as transport and heating, the more the lack of interoperability standards across industries lead to inefficiencies and malfunctions. How to strike a balance between innovation and interoperability of solutions? Setting standards and ensuring the long-term interoperability of blockchain-enabled devices (including meters, sensors, appliances), might help developing markets for demand response, distributed energy resources and flexibility services in general. Guaranteeing interoperability, standardisation and blockchain-readiness of the smart metering infrastructure is particularly important as smart meters enable virtually all the services put forward by distributed ledger technologies. This is even more urgent since 266 million smart meters are expected to be installed by 2030, for a total €46 billion investment, covering 92% of the European consumers [28].

- Energy consumption. Most of the blockchain-enabled energy/sustainability solutions are based on Ethereum. Such technology, which still uses an energy intensive proof-of-work consensus mechanisms, announced in late 2020 the objective to switch to more energy efficient proof-of-stake validation system with its Eth 2.0 upgrade. The overall challenge is to ensure that the increasing transaction volumes from all the expected use cases and applications can be supported while keeping the environmental footprint in check.

- Real vs digital assets and security of supply. Blockchains can represent digital assets (such as cryptocurrencies)existing only on-chain or representing real-world objects/values existing off-chain - such as market shares, electricity commodities, infrastructures and services. Using blockchain technology for off-chain assets management is a complex task:

[7] As an example, a recent blockchain technology - Polkadot - is getting mounting attention as it promises to enable cross-blockchain transfers of any type of data or asset (not just tokens). Connecting to Polkadot should give the ability to interoperate with a wide variety of blockchains.

the stored and transacted data (e.g. related to renewable energy certificates) may not always - unintentionally or maliciously - accurately represent the real ones (i.e. the renewable energy effectively produced) [20][27]. A misalignment between real assets and digital data might impact the market functioning and, possibly even more critically, the energy system reliability and resilience. While cyber security and privacy aspects are thoroughly addressed in the next chapter, it is here worth mentioning the security of electricity supply challenges attached to blockchain. Is it concretely possible to reliably run a "physical" system (off-chain) just relying on a "virtual" blockchain (on-chain)? To date just a few blockchain-enabled pilots tried to take into account the whole spectrum of physical constraints involved in power system management.

3.1.4 Policy and Regulatory Needs

As described in section 1.1, the EC blockchain strategy encompasses several policy actions and legislative initiatives (addressing the financial sector [3]-[5] and other sectors including the energy one [1]).

In continuity with this strategy, some of the main policy and regulatory actions needed to tackle the energy digitalisation challenges described in section 3.1.3, are illustrated in the following points.

- Pro-innovation regulation and technology experimentation. A major regulatory challenge is to reconcile the stability of the legal framework with the rapidity to react to the pace of innovation [32]. The EU and national legislators should keep developing a comprehensive pro-innovation legal framework for digital applications, starting from better regulating blockchain-enabled digital assets and smart contracts [3].
  The EU should keep providing funding for blockchain research and innovation, both in the form of grants and by supporting investment in start-ups. Significant budget for blockchain projects is expected in the Horizon Europe programme.
  Large-scale and multidisciplinary pilots that target integrated architectures, interoperable applications, and harmonized standards are still needed to test the merits and challenges of blockchain use cases and applications. Regulatory sandboxes are increasingly used in a range of sectors, for example in finance, health, transport as well as energy, often including the use of new, emerging technological solutions. The Council of the European Union encouraged the Commission to continue considering the use of regulatory sandboxes and experimentation clauses when drafting and reviewing legislation. On 2020 the EC adopted proposals for regulatory sandboxes/experiments with blockchains in the financial sector and beyond [32]-[35].
  As also underlined in [4], supporting responsible innovation via a pilot regime might help removing obstacles to the application of new technologies (in the financial sector and beyond) and promoting technology uptake. Reporting mechanisms on distributed ledger technologies pilots - including cost-benefit and risk analyses -, similar to the ones proposed in the digital finance sector [4] should be common practice in the energy sector as well.
- Legal certainty, governance and decentralised responsibilities. The EU energy law needs to introduce/implement provisions for the decentralisation of the governance structures

following the decentralisation dynamics occurring in the electricity system. As observed by [27], “A blockchain-based electricity sector would not only change the role of prosumers towards active market participants, but also requires developing solutions for decentralised responsibilities of supply and system operation.” To what extent can emerging socio-political and technological trends subvert the wholesale transmission and retail distribution boundaries and equilibria? Who will be responsible for ensuring that financial transactions are properly settled? Regulatory options span from introducing new responsible entities/platform operators, entrusting the energy suppliers/aggregators or imposing more obligations on energy consumers/prosumers [20][22][32]. If energy markets are to remain the instruments that enable long-term policy and innovation initiatives, new reforms need to be rolled out (starting from the promising ones in the electricity market time and spatial scales), in order to properly distribute costs, benefits and responsibilities among current and emerging actors [32].
This also implies “a policy shift from defining consumers as a homogenous group towards understanding them as market peers with different commercial and flexibility abilities [27]”.

- Data hubs and management rules. Designing adequate energy data hubs/architectures – with consented data access and use rules - is essential for governing the dynamics and transactions within an energy system hosting an increasing number of decentralised actors and resources. As recommended by the Council of European Energy Regulators CEER [23]: “Data needs to be collated and made available not only to network operators but also to current and potential market participants”. Additionally: “generation, consumption and network data needs to be given a clear market value to incentivise prosumers and their intermediaries to profit from using the data to optimise their behaviour” [23]. Finally CEER recommends that energy digitalisation shall be promoted from the regulatory viewpoint by: generating the right sort of data (appropriately granular data on the electricity system is needed, data which is beneficial for managing the whole system); making data accessible, interoperable (for current and potential market participants, subject to appropriate cost-benefit analysis) and secure (in line with cybersecurity and data protection requirements) [23].

- Market redesign, consumer engagement and sector integration. Predictably flexible regulations should enable market players to assess the profitability of investments through meaningful prices (i.e. by giving the right price signals) [23][32]. Member States shall establish consistent and harmonised regulatory frameworks to allow the fair participation of independent aggregators to electricity/flexibility markets, while coordinating the access of transmission and distribution system operators to distributed energy resources [13][22]. As noted by [27], since there is a plethora of on-chain/off-chain, permissioned/permissionless options for blockchains, the legislative and regulatory aims should “not be defining the one and only “correct” blockchain design for the electricity sector, but instead enabling governance processes which determine the blockchain design for a specific purpose”.
  Blockchain technology favours a regulatory perspective shift from integrating consumers into the market to transforming consumers in peer-to-peer market players. However how

is it possible to engage and protect all consumers, not just those with PV panels on their rooftop? Regulators need to be flexible and respond to market and technology developments, making sure that innovation and digitalisation benefit and empower consumers; in particular adequate access to energy data can better engage them [27][29]. Some of the most successful user engagement projects started from assessing the consumer needs and expectations, not only and necessarily in energy saving and monetary terms [20].

A consistent approach in the regulation of several cross-cutting sectors (energy, ICT, transport, etc.) is needed to reach the Green Deal objectives. On the same token, a consistent regulatory and legal frame may be beneficial for the blockchain upscale in the energy sector. The EU and national decision makers should continue making efforts to combine energy and climate change policy actions with other proposals linked to, among others, digital markets, circular economy innovation agendas, and capital market/investment plans [32].

- Support to interoperability and standards. The EC should continue being involved in the work of international standard organisations such as ISO, ETSI, CEN-CENELEC, IEEE and ITU-T, and should continue engaging with other relevant bodies globally such as INATBA (International Association for Trusted Blockchain Applications) to promote interoperability requirements and harmonised standards for blockchain-enabled solutions.

  The JRC smart grids and cyber security laboratories can scale up their pre-normative research activities in support of the policy decision making, with a view at identifying critical issues in the deployment of sustainable energy blockchain-enabled use cases [36][37].

- Sustainability. While keeping their energy performances in check, blockchain technologies can contribute to meet the EU's 2050 climate-neutrality, energy sustainability and circular economic objectives (see Figure 5).

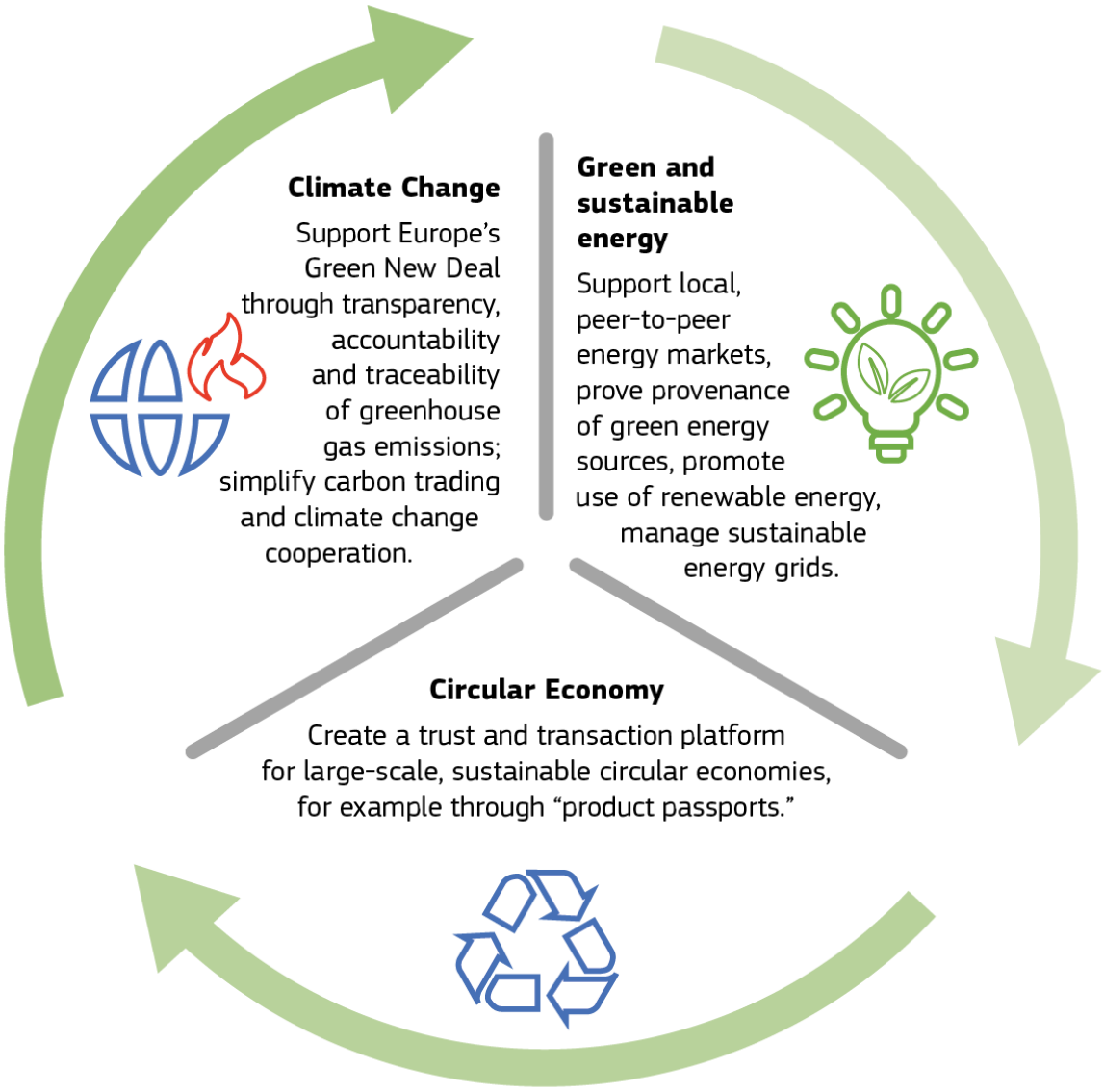

Figure 5 - Blockchain sustainability potential [7]

- Protecting blockchain as a critical infrastructure. Since there is no recognised central authority in the case of disputes or conflicts, and since the energy supply business usually involves the use of critical infrastructure, a proper emergency plan is required to lay out the procedures to follow in the event of system failures [20]. What proposed in the digital finance sector [4], may be relevant to the energy sector as well: "DLT market infrastructures should also be subject to additional requirements, compared to traditional market infrastructures" in order to avoid inter alia security and privacy threats. "A DLT market infrastructure should be required to inform members, participants, issuers and clients on how they intend to perform their activities and how the use of DLT will create deviations compared to the [traditional service provision]".

3.2 Energy, Blockchain, Cybersecurity and Privacy

We are living in an era of great opportunities enabled by digital technologies: access to information and knowledge has never been as easy as it is today. Global economic growth and human well-being are becoming increasingly dependent on the adoption of digital technologies.

However, this intertwining of digital technologies in our daily lives brings with it heightened vulnerability to the deliberate exploitation of unsecure digital systems. This increases the potential impact of cyber-attacks while reducing the advantages of the digitalisation of our society. To understand why cybersecurity is so central, we need look no further than the COVID-19 crisis which has triggered an increase in the cybersecurity risk facing European businesses, governments and citizens. Cyber-attacks have become more frequent as the weaknesses resulting from the focus on fighting the pandemic have been exploited.

Digital technologies are currently at the heart of all our critical infrastructures. Hence, their cybersecurity is already, and is becoming increasingly, a matter of national security. Therefore, cybersecurity is both costly and crucial.

The number of citizens impacted simultaneously by a single cyber incident can be huge as a consequence of the pervasiveness of connected devices: 3 billion accounts in the attack on Yahoo in 2013, 77 million users in the attack on Sony PS3 in 2011, 1.3 million and 250 000 impacted citizens, respectively, in the attacks on Estonia and Ukraine in 2017, just to cite a few examples.

At the same time, cyber-attacks are also becoming more and more complex, demonstrating the attackers' enhanced planning capabilities and knowledge. An example of the growing complexity is the spread of malware able to infect both mobile and IoT devices, hugely amplifying the distributed computational power of cyber attacks while making it more difficult to effectively mitigate an attack. As cyber attackers operate outside the norms of regulation and law, this flexibility gives them a significant advantage over defenders who normally do not enjoy such freedom. The attackers have the crucial advantage of time which in cyberspace can be measured in milliseconds.

Contrary to popular belief, cybersecurity is not merely a matter of technologies. Rather, it has an impact on society and is influenced by the attitude of individuals while they are 'living their digital life'. Their preferences, desired digital services and the way in which they are used are the first considerations when trying to design a more secure cyberspace. Once again, the explosion of teleworking and online schooling during the first half of 2020 due to the COVID crisis and, as a consequence, the higher number of cyberattacks show the extent to which our lives are intrinsically dependent on digital services and why we need urgently to increase their security.

If we think of digitalisation, immediately we think of 'online services', e-commerce, IoT, smart devices, etc. Their common denominator is the establishment of a minimum level of trust in the operations performed, in privacy and in data protection. Cybersecurity is the enforcer of these three dimensions, ensuring that trust is not misattributed, that digital processes

maintain their integrity and availability, and that privacy and data protection are well preserved.

When considering the energy sector, it is evident how cybersecurity is essential to ensure the secure functioning the grid and indirectly, of all the services relying on energy delivery to operate.

The energy digitalisation brought however on the table new challenges for cybersecurity: in the previous decades, when the energy grid was an almost isolated system, the classical "firewalling" approach was more than capable to keep attackers outside. Now is not anymore the case: to operate a smart grid in effective way, all the devices and services need to be tightly interconnected and the boundary between the "external and internal world" are not anymore so clear. Cybersecurity becomes in this case a shared responsibility of all the actors in the game, from energy generation to transmission and distribution companies, from energy aggregators to end-users and more.

The implementation of energy flexibility and energy community use cases developed in this study clearly showed how, to have everything working in perfect way it will be needed to have in place mechanisms ensuring a high level of trust among actors with different competences, interests, business models and scopes, not in term of agreement, but in term of operational and automatic tasks and activities.

Under this perspective, blockchains, being by definition completely distributed infrastructures able to ensure trust among parties without a centralised trusted party, might offer a new perspective on the way in which enforce cybersecurity in the new digitalised energy infrastructure.

3.2.1 Policy context

In February 2020, the Commission issued its ideas and actions for a digital transformation that works for all, reflecting the best of Europe: open, fair, diverse, democratic and confident. It proposes a European society powered by digital solutions that put people first, opens up new opportunities for businesses, and boosts the development of trustworthy technology to foster an open and democratic society and a vibrant and sustainable economy. Following this new attention to digital technology, in 2020 the following key documents have been issued:

- a Communication on Shaping Europe's digital future8, which sees cybersecurity as a principal ingredient in a successful digital transformation where European citizens and businesses trust that their applications and products are secure;
- a White Paper on Artificial Intelligence (COM(2020) 65 final)
- a European Strategy for Data (COM(2020) 66 final).
- a new European cybersecurity strategy (JOIN(2020) 18 final)
- a proposal for a revised NIS directive (2020/0359)
- a proposal for a directive on the resilience of critical entities (2020/0365)

[8] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

There are obviously other policy initiatives that can be taken into consideration (see table below). The package of policy documents just mentioned is already enough to depict clearly the challenges that will need to be covered to support successfully the deployment of blockchain in the energy sector.

Date	EU initiative	Reference
19/02/2020	Shaping Europe's Digital Future White Paper on Artificial Intelligence A European Data Strategy (European Commission, 2020a)	 COM(2020) 65 final COM(2020) 66 final
03/04/2019	COMMISSION RECOMMENDATION on cybersecurity in the energy sector	C(2019) 2400 final
26/03/2019	Cybersecurity of 5G Networks (European Commission, 2019)	C(2019) 2335 final
12/09/2018	Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (European Commission, 2018c)	COM(2018) 630 final
13/06/2018	Joint Communication to the European Parliament and the Council – Increasing resilience and bolstering capabilities to address hybrid threats (European Commission, 2018b)	JOIN/2018/16 final
13/09/2017	Joint Communication to the European Parliament and the Council – Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (European Commission, 2017b)	JOIN/2017/0450 final
13/09/2017	European Commission, Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication	COM(2017) 477 final

	Technology cybersecurity certification ('Cybersecurity Act') (European Commission, 2017d)	
13/09/2017	'Commission Recommendation 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises' (European Commission, 2017a)	C/2017/6100
07/06/2017	Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') – Adoption	9916/17
March 2017	Report of the High-Level Advisory Group of the EC Scientific Advisory Mechanism Cybersecurity in the European digital single market. 2017 (European Commission and Directorate-General for Research and Innovation, 2017)	
6/07/2016	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (European Parliament and Council of the European Union, 2016a)	EU Directive 2016/1148
15/07/2016	European Cyber Security Organisation (ECSO), 'Cyber Security contractual Public-Private Partnership,' ECSO – European Cyber Security Organisation (ECSO, 2019)	
27/04/2016	European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive	Regulation (EU)2016/679

	95/46/EC (General Data Protection Regulation)	
06/04/2016	'Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats a European Union response' (European Commission, 2016b)	JOIN(2016) 18
28/04/2015	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – The European Agenda on Security (European Commission, 2015)	COM/2015/0185
07/02/2013	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: 'An Open, Safe and Secure Cyberspace' (European Parliament et al., 2013)	JOIN/2013/01

Table 1: Summary of EU Initiatives relevant to cybersecurity

The compass giving the direction of the future cybersecurity policy landscape, is obviously the recently approved European Cybersecurity Strategy. The strategy aims at boosting the collective resilience of Europe against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

The strategy does not make distinction between connected devices, the electricity grid, or the banks, planes, public administrations and hospitals, as in the new European digital strategy clearly all these elements are seen as a unique interconnected ecosystem, where the failure of an item can easily have an impact on all the others.

Following the strategy, the Commission is making proposals to address both cyber and physical resilience of critical entities and networks: a Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2'), and a new Directive on the resilience of critical entities. They cover a wide range of sectors and aim to address current and future online and offline risks, from cyberattacks to crime or natural disasters, in a coherent and complementary way.

Still in the context of the NIS2, the Commission, in order to respond to the growing threats, due to digitalisation and interconnectedness, will strengthen security requirements imposed on the companies.

The proposed Critical Entities Resilience (CER) Directive, that is the third pillar of this new wave of security related policy documents, expands both the scope and depth of the 2008 European Critical Infrastructure directive. Ten sectors are now covered: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space. Under the proposed directive, Member States would each adopt a national strategy for ensuring the resilience of critical entities and carry out regular risk assessments. These assessments would also help identify a smaller subset of critical entities that would be subject to obligations, intended to enhance their resilience in the face of non-cyber risks. These include entity-level risk assessments, taking technical and organisational measures, and incident notification.

Elements of cybersecurity, more specifically concerning the Energy ecosystem, are contained in the Recommendation on "Cybersecurity of the energy sector" (C(2019) 2400 final). The document paves the way toward the definition of a cybersecurity network code, defining clear sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

The hearth of blockchain technologies is about data and transactions. A blockchain is, indeed, a long chain of data. For that reason, from a policy perspective, it is important to keep into consideration also the data protection context.

In the EU, data protection is enshrined in Article 8 of the Charter of Fundamental Rights (European Union, 2012). In addition, the GDPR (European Parliament and Council of the European Union, 2016b), which entered into force in 2018, puts forward a set of rules designed to ensure the protection of citizens' personal data and strengthen their fundamental rights.

The GDPR acknowledges the importance of cybersecurity to protect personal data as a prerequisite for the collection and processing of personal data[9]. Moreover it introduces the principles of data protection by design and by default; the by design principle refers to the need to consider data protection requirements starting from the inception and design phases of a product or service, while the by default principle refers to the fact that even without explicit configuration by users, the product or service ensures a minimum level of data protection. Both principles are in line with the security by design and by default principles well established and adopted by the cybersecurity community.

Only effective integration and close cooperation, between data protection and cybersecurity, can ensure that personal data will be well protected and will not be misused and that citizens will ultimately be in control of their personal data.

[9] Article 4 of the GDPR (principles relating to processing of personal data) states that personal data shall be '*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")*'. Further, article 32 (security of processing), requires that both data controller and processor implement appropriate technical and organisational measures to ensure the security of personal data, following a risk-based approach.

3.2.2 Opportunities

Blockchain can enable parties with no particular trust in each other, to exchange digital data on a peer-to-peer basis, with fewer or no third parties or intermediaries. Thanks to properties which include decentralisation, tamper-resistance, transparency, security and smart contracts, blockchain has been followed with interest by the cybersecurity community, given its potential to introduce new mechanisms to ensure trust and integrity in digital transactions.

The intrinsic nature of blockchain has some interesting advantages:

- It provides disintermediation and uses a model that does not require trusted parties.
- The parties have full guarantee that the transactions will be executed as expected.
- Being fully distributed, blockchain services and the underlying data, are resilient to failures, Denial-of-Service (DoS) and, in general, make a well-designed system harder to attack. As a result, the transactions and data stored in the blockchain are themselves resilient to cyber attacks and remain under the control of the users' community.
- Blockchains are transparent and cannot be modified.

In addition, what makes blockchain appealing from a cybersecurity perspective, is the concept of smart contracts, a computer program that is embedded in a blockchain which inherits the characteristics of blockchain and thus has no downtime, censorship or third-party interference. As a result, smart contracts cannot be altered, thereby covering another cybersecurity priority, i.e. 'process integrity'.

In other words, today, blockchain appears to be a promising option to be considered when it comes to enforcing trust, resilience to DoS, integrity and the authenticity of data and processes.

All these features, projected on the energy domain, sound quite promising, as they would allow to implement a transparent trust mechanism across different stakeholders.

However, while blockchain holds potential benefits for cybersecurity, several challenges remain. From a development perspective, the main challenge is the lack of best practices and experience on how to develop professional services, based on blockchain in a secure way. This also affects the deployment of smart contracts.

3.2.3 Challenges and barriers

Although the industry believes that DLT could enhance systems' security, the novelty of the technology is per se a barrier to its adoption in mission critical sectors, as the platforms on which they are built, have not provided any assurance concerning their intrinsic development security and robustness.

The same key components which contributed to boost the flexibility of blockchains, i.e. the smart contracts, are still in their early development stages and are still subject to many limitations.

The secure interaction with the physical world is another key factor that needs to be explored, investigated and standardised. As underlined, many times in this report, when the data is in the blockchain, it becomes virtually secure and immutable, but the problem is exactly how to guarantee that what entered in the blockchain from the physical world is in fact trusted.

This brings us to an additional challenge related to the interaction with legacy systems. All the experiments conducted on field, showed how legacy systems and devices are obviously uncapable to interact with a blockchain, just because they were not designed for this purpose. Hence, to integrate them into a blockchain based energy infrastructure there is the need to design on aone hand “bridges” or “interfaces” allowing legacy systems to connect to the blockchain, and on the other hand to start designing new energy devices, with already embedded blockchain functionalities, for the next generation energy grids.

From a security perspective, another great challenge is related to connectivity. Blockchain exploits the Internet and more in general the classical telecommunication networks, to deliver its services.

The use of blockchain into mission-critical infrastructures, such as the energy grid, implies also the availability of an extremely secure, stable and redundant network connection, resilient to cyberattacks and denial of services.

Indeed, this challenge is not specific of the energy sector, but of all the critical infrastructures of our society; the more they are moving to the digital world, the more the reliance on telecommunication networks becomes relevant.

From a more legal perspective, the ownership of the responsibility, for what concerns the cybersecurity of a blockchain based service, is another big challenge. By definition, a blockchain is a distributed system, and even when a private blockchain is considered (i.e., with a closed number of actors involved), issues exist on the key question “who is responsible for what”. The energy community use-case is a clear example, where we have in the “game” many different actors, with different type of systems, with different type of cybersecurity measures in place, all together collaborating to feed the blockchain.

It is clear that in a sector such as the energy grid, regulatory actions would be needed to define a minimum number of cybersecurity requirements, to be achieved in order to be part of the blockchain system.

Ownership of responsibility is also a barrier when it comes to data protection regulations. In a fully distributed system where the blockchain is “stored” on all the nodes of the system, who is the data owner? Who is the data controller? Who would be in charge for a data-breach notification if something illicit happens?

These are indeed the key questions that require a support policy side to be solved.

3.2.4 Energy Blockchain Cybersecurity Policy Needs

As mentioned in the previous section, the novelty of blockchain technologies, and the lack of assurance concerning their intrinsic cybersecurity is a barrier for their adoption in the context of critical infrastructuresHence the need for a policy action pushing forward the research agenda on blockchain cybersecurity. This would allow to quickly identifying the actual cybersecurity limitations of the technology and their improvement.

Standardisation would also be extremely important, to ensure a common minimum level of cybersecurity of blockchain platforms. Standardisation initiatives would pave the way toward

interoperability, which in mission critical infrastructures, is a key factor to ensure technology diversity and resilience against cyber-attacks.

On a medium run, within the context of the cybersecurity act, the Commission should push forward in the cybersecurity certification rolling plan an item concerning cybersecurity certification of blockchain technologies, to define a certification scheme. This would allowan adequate cybersecurity assurance level for what concerns the blockchain implementations, which aim at being used in specific sectors.

The energy digitalisation phenomenon poses, from a cybersecurity perspective, a question on the resilience and security of the modern telecommunication network and Internet.

From a strategic autonomy perspective, Internet governance and development are today outside the control of Europe. If Europe wants to leads the digital development based on blockchain technologies, as a precondition, it is of utmost importance to start a deep reflection on how Europe could secure the stability and security of its “portion of Internet”, and on the way we can change it to secure our cyber-physical critical infrastructures.

3.3 The role of standards in relation to DLT/Blockchain

Standards can play a vital role in supporting the growth of the DLT/blockchain. The aim of this section is to provide some basic information in order to elicit further the discussion across relevant energy sector stakeholders with an interest to blockchain

3.3.1 ISO/TC 307 Blockchain and distributed ledger technologies

ISO/TC 307 Blockchain and distributed ledger technologies Technical committee has published four standards on blockchain and distributed ledger technologies until now.

1. ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary
2. ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
3. ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
4. ISO/TR 23576:2020 Blockchain and distributed ledger technologies — Security management of digital asset custodians

One of the main issues of ISO/TC 307 is blockchain interoperability. Interoperability is considered important on applications to/from/between layers of blockchain/DLT and the important “facets” to be considered are the following:

- Syntax: Format of information
- Semantics: Meaning of information
- Behaviour: Informational rules behind information and services

- Policy, Trust, Organization: Legal and organizational rules behind information and services
- Transport: Method of moving information

NIST has been in collaboration with ISO in order to define blockchain standards. It has launched several project on DTL, focusing on interoperability, privacy, user tracking and integrity [ref: Loïc Lesavre, Priam Varin, Peter Mell, Michael Davidson, James Shook. "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems", January 14, 2020. NIST Computer Security Division, Information Technology Laboratory https://doi.org/10.6028/NIST.CSWP.01142020]

3.3.2 ITU Focus Group on Application of Distributed Ledger Technology

The ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) was established in May 2017 with the aim to 1) identify and analyse DLT-based applications and services; 2) draw up best practices and guidance supporting the implementation of those applications and services on a global scale; and 3) propose a way forward for related standardization work. FG DLT concluded in August 2019 by publishing 8 deliverables including regulatory frameworks, assessment criteria for DLT platforms, DLT reference architecture and relevant use cases (https://www.itu.int/en/ITU-T/focusgroups/dlt)

3.3.3 CEN and CENELEC Joint TC on Blockchain and Distributed Ledger Technologies

CEN-CENELEC has launched a new TC on DLT (https://www.cencenelec.eu/news/brief_news/Pages/TN-2019-049.aspx) based on the recommendations on successful adoptions of DLT [25] with the aim to identify and adopt international standards already available or under development. The JTC works in close contact with ISO/TC 307 ‘Blockchain and DLT and it focuses on specific European legislative and policy requirements, in support of the development of the EU Digital Single Market.

3.3.4 IEEE Blockchain Initiative

With regard to energy sector, IEEE created the Working Group P2418.5-Energy Blockchain WG in the Standards Committee SBLC-Smart Buildings, Loads and Customer Systems with the aim to formulate an interoperable reference framework model for DLT. This framework model serves as a guidelines for Blockchain DLT use cases in Electrical Power industry; Oil and; energy Gas value industry chain, covering the Renewable energy industry and their renewable related sources services of generation. Moreover, it supports a system interface for DLT applications in the energy sector based on open protocols. The WG has also assessed the security, interoperability, scalability and performance through the evaluation of consensus algorithm and smart contracts for the energy sector.

[ref: https://blockchain.ieee.org/standards]

4 Final Considerations

While the digital transformation is a key enabler to reach the Green Deal objectives, a consistent approach in the regulation of several cross-cutting sectors (energy, transport, finance etc.) is equally needed.

The EC aims to ensure that the "regulatory framework is innovation-friendly and does not pose obstacles to the application of new technologies" [3]. Blockchain can support and streamline evidence-based decision-making in the climate and sustainable energy fields.

Blockchains are gradually improving their performances while impacting more and more sectors far beyond finance.

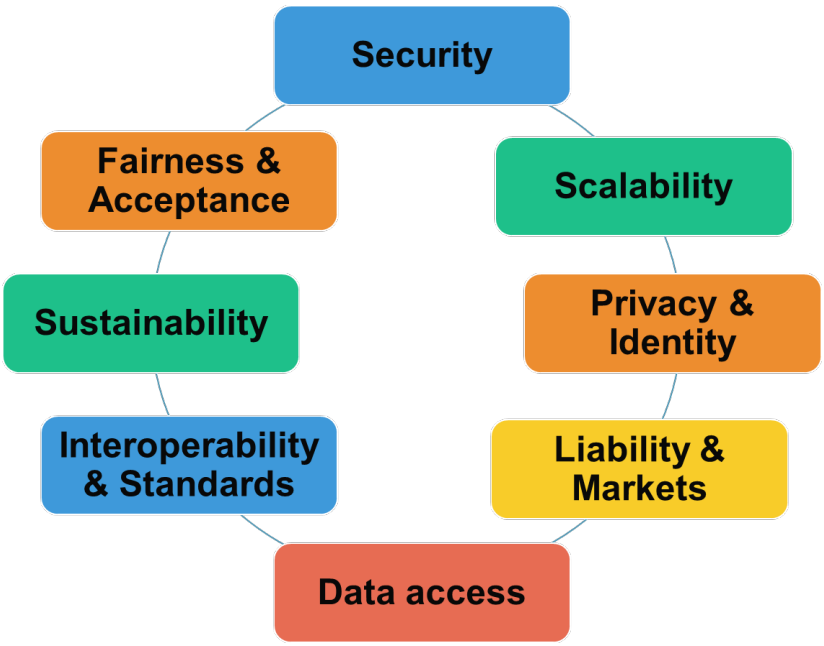

Figure 6 - Blockchain deployment challenges [17]

Several aspects and interfaces, must be properly understood in the blockchain ecosystem to govern the introduction of blockchain-based electricity delivery options and services [17][32]. Among the main motivations which call for regulating initiatives concerning the use of blockchain in the electricity sector (see also Figure 6), one can consider the following ones:

- Balance technical innovation with the scalability of solutions, to ensure the adoption of approaches fit for purpose and future proof
- Define and allocate decentralised responsibilities of electricity supply and distribution: disintermediation and distributed architecture are two of the most peculiar characteristics of blockchain technologies. While these features are in fact key enablers in the trusted integration of different actors in the smartgrid ecosystem, on the other can potentially create confusion in term of responsibilities and liability.

For that reason a reflection is needed to establish clear rules, roles and duties in this new type of energy paradigm.

- Incentivise consumers to invest in flexibility technologies: in this study we demonstrated how the flexibility use-case scenario would benefit from the adoption of blockchain technologies; however still regulatory initiatives would be needed to make the adoption of blockchain an advantage also for the consumers, to enlarge the community of those participating in the flexibility “energy economy”. The same type of initiative would also be needed in the case of Energy Communities.
- Find a balance between consumer empowerment (self-responsibility) and protection [20][27].
- Bost the adoption of cybersecurity certification schemes both in the domain of blockchain core infrastructure and in the domain of end user applications and devices (e.g. IoT), to ensure the full coverage of the energy digitalisation value chain

Recently issued regulation proposals in the digital finance/crypto-asset sectors, contain interesting approaches and solutions, which could be applicable to or of inspiration for the energy sector as well. In this respect, one of the main challenges for policy decision makers, is to strike a balance between supporting innovation, protecting consumers and upholding market integrity [3][4].

It remains to be seen to what extent blockchain can support or subvert business models in the transitioning electricity systems and markets. Indeed, blockchain represents only one of the enabling technologies of power system innovation: several digital technologies (including Artificial Intelligence, big data, IoT and BC) will probably need to be compbined to achieve the climate-neutrality and sustainability targets.

The JRC smart grids, blockchain and cyber security laboratories [36][37]stand ready to scale up their pre-normative research activities in support of policy decision making, with a view at identifying critical issues in the deployment of blockchain-enabled sustainable energy solutions.

As an immediate example, the JRC started cooperating with Local Energy Community initiatives, in the context of the ERIGRID project [38], to test innovative solutions foreseeing the deployment also of blockchain technologies. In particular, the first testing activities will be conducted on the blockchain-based smart metering solutions adopted in the first authorised Italian Local Energy Community, recently inaugurated in Magliano Alpi (Piedmont Region) [39].

References

[1] European Commission, Legal and regulatory framework for blockchain, https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain

[2] European Commission, Policies on Blockchain, https://ec.europa.eu/digital-single-market/en/policies/76615/76123

[3] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final. https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-593-F1-EN-MAIN-PART-1.PDF

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology, COM (2020) 594 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594

[5] Joint statement by the European Commission and the European Central Bank on their cooperation on a digital euro, 2021, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/210119-ec-ecb-joint-statement-digital-euro_en.pdf

[6] European Blockchain Services Infrastructure, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi

[7] European Blockchain Strategy – Brochure, https://ec.europa.eu/digital-single-market/en/news/european-blockchain-strategy-brochure#:~:text=The%20EU%20Blockchain%20Observatory%20%26%20Forum,in%20this%20transformative%20new%20technology.

[8] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Green Deal COM/2019/640 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:640:FIN

[9] European Commission, Shaping Europe's digital future, 2020, https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[10] IEA, Digitalisation and Energy, Technical Report, 2017, https://www.iea.org/reports/digitalisation-and-energy

[11] ETIP SNET, Digitalization of the energy system and customer participation, 2018, https://www.etip-snet.eu/wp-content/uploads/2018/11/ETIP-SNET-Position-Paper-on-Digitalisation-short-for-web.pdf

[12] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3Acoord019R0943

[13] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944

[14] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0001.01.ENG

[15] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Powering a climate-neutral economy: An EU Strategy for Energy System Integration COM/2020/299 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:299:FIN

[16] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A European strategy for data, COM(2020) 66 final, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[17] G. Fulli, Lectures on electricity sector digitalisation and blockchains, Smart Grids course, "ICT for Smart Societies" Master Program, Politecnico di Torino, 20/21, https://ses.jrc.ec.europa.eu/

[18] IRENA Brief, DIGITAL APPLICATIONS FOR THE ENERGY TRANSITION: BLOCKCHAIN, 2018, https://innovationweek.irena.org/-/media/Files/IRENA/Innovation-Week/SessionalDocuments/Summary/IRENA-IW2018-Session-Summary---Blockchain.pdf

[19] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, https://www.sciencedirect.com/science/article/pii/S1364032118307184

[20] EU Blockchain Observatory & Forum, Workshop Report - Energy and Sustainability, – Online Video Conference, 5 March 2020, https://www.eublockchainforum.eu/sites/default/files/reports/workshop_17_report_-_energy.pdf

[21] JRC, Digital Transformation in Transport, Construction, Energy, Government and Public Administration, 2019, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digital-transformation-transport-construction-energy-government-and-public-administration

[22] NERA Economic Consulting, Eurelectric, Blockchain in Electricity: a Critical Review of Progress to Date, 2018, https://cdn.eurelectric.org/media/3115/paper1_blockchain_eurelectric-h-BA73FBD9.pdf

[23] addestino, EC, EBSI – European Blockchain Services Infrastructure, Open Market Consultation report, 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69281

[24] CEN-CENELEC Sector Forum Energy Management, Blockchain in the energy sector: challenges and opportunities, 24 October 2019 workshop, https://www.cencenelec.eu/news/events/Pages/EV-2019-040.aspx

[25] CEN-CENELEC, White Paper on standards in Blockchain & Distributed Ledger Technologies, 2018, https://www.cencenelec.eu/news/brief_news/Pages/TN-2018-085.aspx

[26] EC, Data Driven Energy Services. How to Engage Consumers, 29 April 2020 Workshop, https://ec.europa.eu/digital-single-market/en/news/workshop-data-driven-energy-services-how-engage-consumers

[27] L. Diestelmeier, Changing power: Shifting the role of electricity consumers with blockchain technology – Policy implications for EU electricity law, Energy Policy, 2019, https://www.sciencedirect.com/science/article/pii/S0301421518308711?via%3Dihub

[28] Tractebel, EC, Benchmarking smart metering deployment in the EU-28, 2019, https://op.europa.eu/en/publication-detail/-/publication/b397ef73-698f-11ea-b735-01aa75ed71a1/language-en?WT.mc_id=Searchresult&WT.ria_c=37085&WT.ria_f=3608&WT.ria_ev=search

[29] Council of European Energy Regulators (CEER), Consultation on Dynamic Regulation to Enable Digitalisation of the Energy System, Conclusions Paper, 10 October 2019, https://www.ceer.eu/documents/104400/-/-/3aedcf03-361b-d74f-e433-76e04db24547

[30] Council of European Energy Regulators (CEER), Regulatory Aspects of Self-Consumption and Energy Communities 2019

[31] PwC, Tractebel, EC, Assessment and roadmap for the digital transformation of the energy sector towards an innovative internal market, 2020, https://op.europa.eu/it/publication-detail/-/publication/c6e0bbeb-6411-11ea-b735-01aa75ed71a1/language-it/format-PDF/source-search

[32] G. Fulli, M. Masera, A. Spisto, S. Vitiello, A Change is Coming: How Regulation and Innovation Are Reshaping the European Union's Electricity Markets, IEEE Power & Energy Magazine, 2019, https://ieeexplore.ieee.org/document/8608071

[33] Council Conclusions on Regulatory Sandboxes and Experimentation Clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XG1223(01)&from=EN

[34] Attrey, A., Lesher, M. and Lomax, C., 'The role of sandboxes in promoting flexibility and innovation in the digital age', OECD Going Digital Toolkit Policy Note 2, 2020, https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf

[35] E. C. van der Waal, A. M. Das, T. van der Schoor, Participatory Experimentation with Energy Law: Digging in a 'Regulatory Sandbox' for Local Energy Initiatives in the Netherlands, Energies, 2020, https://www.mdpi.com/1996-1073/13/2/458

[36] JRC Smart Grids Interoperability Lab (SGIL), https://ses.jrc.ec.europa.eu/digital-grid-interoperability-under-test

[37] JRC Experimental Platform for Internet Contingencies (EPIC), https://ec.europa.eu/jrc/en/research-facility/experimental-platform-internet-contingencies-epic

[38] ERIGrid 2.0: European Research Infrastructure supporting Smart Grid and Smart Energy Systems Research, Technology Development, Validation and Roll Out – Second Edition, https://erigrid2.eu/

[39] Comunità di Energia Rinnovabile (CER) di Magliano Alpi, https://cermaglianoalpi.it/

List of abbreviations and definitions

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEP	Clean Energy Package
DLT	Distributed Ledger Technologies
DoS	Denial-of-Service
DR	Demand Response
DSO	Distribution System Operator
EBSI	European Blockchain Services Infrastructure
EC	European Commission
eIDAS	electronic IDentification Authentication and Signature
EU	European Union
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
IEEE	Institute of Electrical and Electronics Engineers
INATBA	International Association for Trusted Blockchain Applications
IoE	Internet of Energy
IoT	Internet of Things
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union
JRC	Joint Research Centre
NIS	Network and Information Security Directive
TSO	Transmission System Operator
TTP	Trusted Third Party

List of figures

Figure 1 - EC Blockchain strategy 3
Figure 2 - Recent EU legislative initiatives on energy digitalisation [17] 5
Figure 3: Country distribution of the publications on blockchain for the energy sector 8
Figure 4. Comparison of the different energy domains 9
Figure 5 - Blockchain sustainability potential [7] 22
Figure 6 - Blockchain deployment challenges [17] 33

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-30781-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/416731

ISBN 978-92-76-40551-1