EUROPEAN CYBER SECURITY ORGANISATION

ECSO Technical Paper on Distributed Ledger Technologies

WG6: SRIA and Cyber Security Technologies

June 2022

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO Members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg6_secretariat@ecs-org.eu.

Disclaimer

This document is classified as internal to ECSO.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources including external websites referenced in this publication.

Copyright Notice

Executive Summary

Blockchain is one of the World´s most disruptive technology, being a powerful force able to drive innovation across different industry and public domains. It can be seen as an enabler of a new secure and democratic digital economy, an enabler of Internet Trust technologies.

Technological and architectural features, together with governance, scalability, reliability, interoperability among Distributed Ledger Technologies (DLTs), integration with legacy systems, economical changes, as well as compliance with EU regulation and policies need to be considered in order to take Blockchain to its full potential.

As a disruptive technology, nobody is fully aware of the potential effect on society, the economy or in industry, but it is necessary to be ready to take the appropriate measures for standardisation, legislation, and regulation.

Table of Contents

Executive Summary ii

1. Introduction 4

2. Relevance of Blockchain Technology 5

2.1. Current ecosystem 5

2.2. Technological aspects 6

3. Technical Challenges 9

3.1. DLT applied to cybersecurity 9

3.2. Security and privacy in DLT 12

4. Relevant Standardisation Activities 13

4.1. CEN-CENELEC JTC 19 13

4.2. CEN-CENELEC Focus Group on Blockchain and DLT 13

4.3. ETSI ISG PDL 13

4.4. ISO/TC 307 Blockchain and distributed ledger technologies 14

4.5. ITU-T Study Groups 14

4.6. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) 14

4.7. W3CBlockchain Community Group 14

4.8. IEEE Blockchain 15

5. Implications of legislations and regulations 16

6. Recommendations and future directions 18

1. Introduction

Blockchain is a disruptive technology that opens new possibilities for improving many services currently delivered by the national and regional governments and even offers the possibility for the creation of new services, new business models and ways of doing different things that we still can't imagine. Even though the possibilities are enormous, its knowledge and application are still in the preliminary stage, and in fact many of the existing different publicly backed initiatives around the world are still in the stage of use case or proof of concept.

When talking about Blockchain or other Distributed Ledgers it is possible to think in two different ways. The first one is trying to solve certain problems in industry or society using Blockchain, e.g., traceability of items, and the other one is a most disruptive way of solving problems using Blockchain in which either value chains can be changed eliminating intermediaries or creating new business models around the use of tokenized value. In both scenarios, Blockchain can be seen as a technology that can solve certain cybersecurity issues and at the same time it is a new technology that needs to be properly secure.

The European Commission has also started with its own specific Blockchain initiatives with the aim of positioning the European Union as a reference in the development and implementation of Blockchain-based solutions[1] with the following activities:

- EU Blockchain Observatory and Forum
- Horizon Prize on Blockchain for Social Good
- Financing Blockchain and Distributed Ledger Technology (DLT) projects

As it seems logical to think that the implementation and deployment of a Blockchain infrastructure could increase technological knowledge and act as an enabler facilitating the use of EU services based on blockchain and the establishment of new business models and new applicable regulation, the European Commission is building an EU Blockchain Services Infrastructure (EBSI)[2]. An initial set of use cases has been identified including notarisation, diplomas, European digital identity and trusted data sharing.

[1]https://ec.europa.eu/digital-single-market/en/blockchain-technologies

[2] https://digital-strategy.ec.europa.eu/en/policies/ebsi

2. Relevance of Blockchain Technology

2.1. Current ecosystem

Blockchain is one of the world's most disruptive technologies which is becoming a powerful force driving innovation across different industry domains. A technology that allows individuals and communities to reach agreement on permanently recorded information without any central or trusted authority. As a new platform technology with the salient features of decentralization, immutability, transparency with pseudonymity, consensus-based decision making and automation driven by Smart Contracts[3], Blockchain allows us to create a new secure and democratic digital economy that is also expected to create a new specific industry within the cybersecurity market. A new industry focused on enabling the software industry and companies of any domain to create a new secure, decentralized and highly automated business.

With the wealth of opportunities across all sectors, Europe wants to position itself as a leader in this new generation of internet Trusted technologies. Moreover, blockchain systems are currently not designed with an EU-aware focus, leading to technology that is not always compatible with EU laws, and thus suffering limited adoption. For this reason, one of the first actions that was carried out by the European Commission has been the setup of the European Union Blockchain Observatory and Forum with the purpose of accelerating Blockchain innovation and the development of the Blockchain ecosystem within the EU, and so assist Europe's position as a global leader in this transformative new technology by mapping key initiatives, monitoring developments and inspiring common actions. In this context, the Observatory has established two dedicated working groups to identify and research existing blockchain initiatives throughout the EU and beyond: Blockchain Policy and Framework Conditions WG, and Use Cases and Transition Scenarios WG. Moreover, it has published various thematic reports investigating the use of blockchain for various use cases such as healthcare and Non-Fungible Tokens (NFTs), and key aspects such as energy efficiency of blockchain technologies.

Talking at a country level, some are far more welcoming than others, since some of them have initially established expert groups with the objective of understanding and appropriating the technology to apply it, while others have identified concrete use cases of services that they would like to implement in Blockchain. However, the most advanced countries have already established and implemented real proofs of concept, and the fact is that very few have already deployed complete governmental services into the Blockchain. More specifically, countries such as Estonia, Dubai, Singapore, Sweden, Australia, Holland are already at the forefront of Blockchain initiatives. Very recently, the Central American state El Salvador has established bitcoin as legal currency in the country in June 2021.

The standardisation of Blockchain technologies is also another area in which work is already underway both in Europe and globally with initiatives like: CEN/CENELEC Blockchain focus Group, IEEE Blockchain WG, ISO TC 307, ANSI Accredited Standards Committee X9 and ITU-T SG17

[3] https://ieeexplore.ieee.org/abstract/document/9083784

DLT Security between others. Section More details on relevant standardisation in Blockchain is discussed in Section 3.1.

From a point of view closer to technology, we must highlight global alliances such as Hyperledger (Linux Foundation) or the Enterprise Ethereum Alliance (EEA), and locally initiatives like Alastria (Spain) the first multisectoral semi-public Blockchain/DLT infrastructure, supporting services with legal effectiveness or 4T-DLT in Switzerland for an open, secure, interoperable and reliable DLT infrastructure.

It is also necessary to remember, that our laws, rules and norms are based on a benign internet, and we tend to extrapolate technologies by overestimating short-term effects of technological changes and underestimating the long-term effects. By anticipating the immediate uses of new technologies, we also need to understand its manifestation in society and provide the appropriate measures for legislation and regulation background by strong cooperation between government, industry, and academia. More information about the legislations and regulations impacting or using blockchain is available in Section 5.

2.2. Technological aspects

Architectural features (permissioned/permissionless solutions, transactional capacity, network size/number of nodes, etc.), governance, scalability, resiliency, interoperability between existing Blockchain systems, initiatives or infrastructures, integration with legacy system, as well as compliance with EU regulation and policies must be considered.

Technologically focusing on the cybersecurity of Blockchain/DLT technologies, efforts could be devoted to key topics like:

1. **Blockchain — one word, different meanings:**

There are several ways to approach DLT and its different features. In a recent report[4], researchers from the University of Cambridge presented a comprehensive framework for evaluating DLT implementations. They identified four different types of actors: *developers, administrators, gateways,* and *participants.* They also divide the DLT ecosystem into three layers: *protocol, network,* and *data*. This is a good example of one taxonomy in this domain.

Of course, there are also other ways to explore DLT and a traditional way to categorize different Blockchains and DLTs is to make a distinction between *private* and also in *permissioned public Blockchains* and *permissionless* (or open) Blockchains.

In the case of Interoperability, one recent paper[5] proposes an inter-Blockchain protocol and framework for conducting transactions between different Blockchains via a separate *router Blockchain*. It can also be mentioned the Interledger protocol that has been liberated by Ripple, and that has been implemented in Hyperledger, under the Hyperledger Quilt denomination or

[4] https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/

[5] https://ieeexplore.ieee.org/document/8431965

Hyperledger Cactus that are one step forward for the interoperability of networks based on this initial protocol[6].

2. **Digital Identity based on blockchain:**

On the Internet, many services require to have access to the customer identity. Today people want to make sure they don't just "offer" their personal information and confidential information and want to limit its access once they stopped working with the service provider. Moreover, companies have to face new privacy issues and regulations on personal data (GDPR for instance) that make it a mutual challenge both for customers and service providers.

Numerous solutions based on blockchain technology enable people to just "regain control" of their personal information for a limited amount of time. With a blockchain based solution, people can manage how they want to share their information and be able to take it back at any time without any trusted third-party involvement. The SSI paradigm is a notable example in that area.

As an example, Indy is a DLT project from Hyperledger providing digital identity solutions (along with Aries and Ursa) aiming the decentralization of identities. The upcoming ISO Technical Report TR23249 will provide a comprehensive overview on DLT systems for identity management.

3. **Information gathering and validation:**

In a classic (centralized) network every stakeholder in an information transmission or sharing will need to trust a third party managing and distributing the information itself.

Because of that, stakeholders will need to rely on this third-party honesty and capability of ensuring the integrity and accessibility of the information.

Blockchain based solutions offer a way of making sure the data integrity is preserved and the accessibility of the data cannot be locked. Since every stakeholder is part of the same distributed network the integrity of the information is insured by the whole network itself, increasing its reliability and accessibility.

Since the data privacy is also one of the main concerns regarding personal, confidential, or sensitive information, blockchain has been associated to *zero knowledge proof* systems. With such a protocol, stakeholders of a decentralized network can prove an information without having to reveal the information itself to another network member (for instance a user could want to insure to a shop he has enough money to make a purchase without revealing its banking details or his exact credit).

4. **Non Fungible Tokens (NFTs)**

According to the Ethereum Foundation[7], a Non Fungible Token (NFT) is a "*token that we can use to represent ownership of unique items. They let us tokenise things like art, collectibles, even*

[6] https://interledger.org/

https://www.hyperledger.org/projects/quilt

[7] https://ethereum.org/en/nft/

real estate. They can only have one official owner at a time and they're secured by the Ethereum blockchain – no one can modify the record of ownership or copy/paste a new NFT into existence." NFTs are an exciting innovation that model the indivisibility of the ownership of a digital media and the lifecycle of the NFTs comprises phases like the creation (from a content creator), repeated buys and sells with the corresponding change of ownership, where the original creator could also get a fee on each of the subsequent sells. The NFT could be a digital-only media (e.g. a digital photo), a digital twin of a physical object (a 3D model of an artwork) or a replacement for a once physical object now dematerialized (e.g. a ticket for a concert or a museum). The scarcity of the NFT results in a value as determined in a free market, and the owners are usually eager to show their collections of NFTs through different settings (from a web page to an augmented/virtual reality environment like the metaverse).

NFTs pose a set of cybersecurity problems including secure management of their lifecycle (which requires in turn sound identity management of the owners), durability of their digital representation, disintermediation of the access to the underlying digital data, unambiguous rendering of them in different settings, interoperability with different environments and DLTs, and contrast to falsification. NFTs could be associated to digital transformation processes, IoT settings and very often DLTs and blockchains systems.

3. Technical Challenges

The DLT landscape is evolving, and different challenges appear, with different standardization bodies working on it globally. The decentralization promoted by DLTs makes it possible to address typical cybersecurity problems but, at the same time, represents a new horizon where ensuring security and privacy is a must. The achievement of the technological challenges presented by DLTs represents new possibilities with great potential for the public and private sectors, where data sharing and transaction control are two key factors.

3.1. DLT applied to cybersecurity

Over the last decades the value of information exchanged through the Internet grew exponentially. As a predictable result, cyber-hacking also grew exponentially since the value of the data leaked or locked by a hacker is more crucial, sometimes essential, for an organization.

Today, cyber networks and digital data face multiple cyber-security challenges in order to protect their data. There are many reasons for this, but the most important is the complexity of IT systems. The more complex a system is, the less secure it becomes. Billions of connected digital devices (PCs, smart phones, IoTs, embedded devices, hardware providing the backbone of the critical infrastructures, etc), have hundreds of billions of lines of code connected all together through the internet which is hosting billions of websites and portals managing unimaginable amount zettabyte of data, all adding up to the large attack surface where everything is connected and dependent on each other.

Ransomware attacks like the Colonial Pipeline, WannaCry, Petya or Locky are few examples of devastating attacks aimed to ransom money to their users who had a deadly need of their files in order to make their company work. WannaCry alone touched more than 300,000 victims in 150 countries. But organisations also have risks associated with their human resources in terms of their lack of understanding of cyber risks, lack of awareness, lack of clear processes and so on. In fact, ransomware usually comes after a human threat.

DDoS attacks are also frequent to lock the access to specific information or service. By disabling a service or the access of an information a cyber-hacker can lead to millions of dollars loss for a company. Recently the betting platform Winamax saw its poker services closed once again for DDoS reasons, impacting its revenue and user experience.

Data Corruption is the third mayor cyber-risk carried by companies. Hackers can in some cases have a direct access to an information and corrupt it (issue a payment, corrupt a banking statement etc.).

In parallel of those attacks, Cloud infrastructures are every time more exploited by every type of organization to have access to Iaas, Paas or SaaS solutions. However, by relying on external IT services, companies depend on the cloud provider infrastructure, e.g., the Fastly global Internet outage had an impact on all its customers. Moreover, the role of the cloud service provider becomes crucial as companies using cloud services might tend to lose their sovereignty over the data they collect, store and exploit. Storing data on “the cloud” for instance leads to confidentiality problematics as well as integrity and access issues that are not fully handed by the company IT

services. In fact, it is a trust issue, everybody created data over the Internet, but the question is what the service provider does with that data.

As everything is connected supply chains pose a huge threat, especially because larger organisations spend more on cyber security, but they are dependent on their suppliers, usually SMEs who lack resources and understanding of the importance of cyber security and might be under a different legal environment (e.g., outside EU) which can make security trade-offs hard.

Several challenges that are present in the field of security can be tackled using DLT/Blockchain technologies.

Technological challenges:

- **Data integrity & availability**: the advanced electronic signature of each transaction in a blockchain network together with other global integrity mechanisms (Merkle tree, block hash, etc.) offer us a complete integrity of the information in a network in which depending on its size and distribution can also guarantee the full availability of this information.

- **Global identity of users and devices**: blockchain proposes a unique and standardized identity for the identification and authentication of users and devices in the network based on pseudo-anonymous public key cryptography in public networks, an on digital certificates (usually x509v3) in private networks. This standardization forces a common identity technology in each network, which allows achieving higher levels of interoperability, as well as ensuring the non-repudiation of each and every one of the network transactions.

- **Security and integrity of software/firmware and log files**: the hashes of the software and its updates can be recorded in a secure, immutable and decentralized way (without a SPOF) thanks to blockchain, and the devices can make sure that the current version has not been corrupted or altered by malicious users. Also, in the industrial field we can register the latest versions approved for production and detect any alteration of the firmware or even the configuration file used by a device. The registration of log files in a blockchain can help us to prevent malicious users from tampering or removing part of these logs to erase their traces. It also allows an exhaustive and trustworthy forensic analysis in case of any security incident.

- **Data sovereignty**: blockchain can allow us to control the access and access methods to data and information, register any interaction with such data securely and reliably, helping to comply with the data access and consumption policies. In the near future we will even be able to allow third parties to offer services over our data without having to share the raw data with those third parties, simply by allowing a Smart Contact (containing the algorithm) to run on our data, but not the company that offers that service.

- **IoT security**: blockchain allows peer to peer communications between devices, guaranteeing their integrity and non-repudiation. In addition, it does not require a central node which usually represent a Single Point of Failure (SPoF). Finally, it should be considered that blockchain offers an opportunity for the standardization of identity and secure authentication of IoT devices where currently are different silos and black boxes both in the industrial (IIoT) and consumer markets.

- **Cyber Threat Intelligence**: blockchain is a perfect tool for secure synchronization between different information systems allowing us to create a common network of security related information enhancing and fostering cyber threat information sharing and responsible disclosures.

- **Traceability and transparency of processes**: the inalterability of blockchain together with the non-repudiation of its operations makes it the ideal technology to guarantee the traceability of the processes of any domain of application. In addition, if it is desired to offer transparency of these processes, it is possible to give visibility to third parties (consumers, other members of a supply chain, etc.) of this reliable information.

- **Secure payments**: Addressing cybersecurity challenges in the context of heavily regulated sectors including finance and banking.

Table 1: Summary of impact of Blockchain on verticals

Vertical sector	Specific relevance of Blockchain and challenges
Industry	• Traceability of goods • Certification processes • Agrifood origin
Energy	• Traceability and certification of the origin of the energy • Authentication and authorization in smart grids • Create a secure peer-to-peer energy trade environment • Neighbourhood electricity trading, flexible grid management, architecture for managing grids, and energy trading • Carbon credits and renewable energy
Consumer IoT	• Machine identity • Machine economy
Government	• Public Registers • Interoperability of IT Systems
Healthcare	• Controlling Access to Health Information and data sharing • Identity management of networked medical devices • Data verification and EHR/EMR entry validation • Patient data protection, patient safety, and device availability • Drug Development and Supply Chain Integrity • Dynamic inform consent
Finance	• Cryptocurrency • Decentralized services • Transactions and accountability

3.2. Security and privacy in DLT

Blockchain can help mitigating some of the previous cybersecurity threats, also in DDoS, but blockchain is reliant on its code and – as history already showed – the biggest blockchain related thefts were exploiting purely written code or credential stealing.

When talking about the cryptocurrency economy enabled by blockchain, currency exchanges, mining services and other data processors are facing hacking attempts as well as extortion of personnel data and theft. Another cybercrime trend consists of cryptojacking, based on cryptomining malware, which consists of the exploitation of internet users´ bandwidth and their processing power to mine cryptocurrencies.

The privacy is another big fact in the blockchain environment. The needs of users who are increasingly aware of their personal information and the establishment of regulations, such as the GDPR, make privacy and data protection two of the most recurring issues in the application of blockchain technology to different sectors.

Blockchain handles information at different levels, being the data layer the one affecting privacy the most, where the business model information is located, containing the current state of the record and its history. The way in which each network is managed makes the design of smart contracts – where appropriate – for the treatment of sensitive information of vital importance.

The services offered for the use and exploration of blockchain solutions are again a possible doorway to privacy losses and attacks on personal information. Even if the blockchain network does not contain personal or sensitive information, service providers must offer trust and security so that the information they hold on their users is not accessed by third parties, as it could be linked to their movements within the network.

Even if it is possible to keep all personal information out of the network and services, it is also worth bearing in mind that cross attacks can occur, based on the observation of movements, such as those based on profiling attacks.

4. Relevant Standardisation Activities

4.1. CEN-CENELEC JTC 19

This committee is tasked prepare, develop, and adopt standards for Blockchains and Distributed Ledger Technologies covering among others the following aspect:

- Organizational frameworks.
- Processes and product evaluation schemes.
- Technical guidelines.

The committee focuses on European requirements, which means understanding how blockchains and DLTs could be made aligned with relevant EU legislation (e.g., eIDAS Regulation, NIS Directive, GDPR, TOOP, MICA Directive), supporting and contributing to the EU Digital Single Market. The JTC will pay special attention to ISO/TC 307 standards.

The JTC has a Working Group (WG) on Decentralised Identity Management, which focus is on processes, roles and practices for decentralised identity management and support functions as provided by DLTs.

4.2. CEN-CENELEC Focus Group on Blockchain and DLT

This informal group advises on European technical requirements relating to Blockchain and DLT, without developing standards. The Focus Group will address the needs of European businesses with a particular focus on SMEs. The group has released a White Paper on ‘Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies.

Participation to this Focus Group is free and does not strictly require the participation to a corresponding national standardization body.

4.3. ETSI ISG PDL

ETSI has set up an Industry Specification Group (ISG) on Permissioned Distributed Ledger (PDL), to provide the foundations for the operation of permissioned distributed ledgers, with the ultimate purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors, fostering the application of these technologies. Several standards have been published, including a system architecture and functional specification for smart contracts.

4.4. ISO/TC 307 Blockchain and distributed ledger technologies

This Technical Committee (TC) deals with the Standardisation of blockchain technologies and distributed ledger technologies. It is structured along several WGs, Study Groups (SGs) and Advisory Groups (AGs). Among them, particularly relevant for ECSO is the Joint WG 4(JWG4) with ISO/IEC JTC 1/SC 27, “Security, privacy and identity for Blockchain and DLT”.

This TC has published a standard on vocabulary (ISO 22739:2020), a taxonomy (ISO/TS 23258:2021) and some Technical Reports (TRs) on Privacy and Personally Identifiable information protection, an overview of interactions between smart contracts in blockchains, and on the security management of digital asset custodians.

Many other standards are coming, including a reference architecture, guidelines for governance, an overview of DL systems for identity management.

4.5. ITU-T Study Groups

Several ITU-T Study Groups (SGs) have been dealt with blockchains and DLTs. Among them:

- SG20 (Internet of Things) proposed the recommendation “Framework of blockchain of things as decentralized service platform”.
- SG17 (Security) proposed the recommendations, “Terms and definitions for distributed ledger technology”, “Assessment criteria for distributed ledger technologies” and “Security framework for distributed ledger technology”.
- SG16 proposed the recommendation “Reference framework for distributed ledger technologies”.

4.6. ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT)

FG DLT was established in May 2017 to identify and analyse DLT-based applications and services, draw up best practices and guidance and propose a way forward for related standardization work.

The FG concluded its work in 2019 with the publication of several TRs and Technical Specifications (TSs).

4.7. W3CBlockchain Community Group

W3C Blockchain Community Group formulated to generate message format standards of Blockchain based on ISO20022 (electronic data interchange for financial institutions) and the generation of guidelines for usage of storage including torrent, public/private blockchain, side chain and content distribution networks.

4.8. IEEE Blockchain

This group will be the hub for all IEEE Blockchain projects and activities. The group encompasses a comprehensive set of projects and activities supported by the following core subcommittees: Pre/Standards, Education, Conferences and Events, Community Development and Outreach, Publications, and Special Projects.

5. Implications of legislations and regulations

Legal and regulatory issues are the main obstacle that governments see in applying blockchain, followed by other obstacles such as immature technology, lack of executive buy in or insufficient skills. For example, the application of the General Data Protection Regulation (GDPR) on Blockchain technologies is a complex procedure and still under examination. Even though significant effort should be performed for satisfying GDPR requirements in Blockchain/DLT infrastructures, some implications can be identified. These include the storage of the personal data on the distributed network, the role of Blockchain full nodes as data controllers and data processors and deletion of data stored on Blockchain.

The definition of specific legal frameworks, including domain-specific regulatory sandboxes, will be even more crucial in heavily regulated sectors, like finance, banking, healthcare.

The **European Strategy for Data** (COM (2020) 66 final) pays attention to tools for individuals "to decide at a granular level what is done with their data". Example of those tools are "consent management tools, personal information management apps, including fully decentralised solutions building on blockchain, as well as personal data cooperatives or trusts acting as novel neutral intermediaries in the personal data economy". Specifically, on blockchain, the document states that "New decentralised digital technologies such as blockchain offer a further possibility for both individuals and companies to manage data flows and usage, based on individual free choice and self-determination. Such technologies will make dynamic data portability in real time possible for individuals and companies, along with various compensation models.". Lastly, the Strategy also states that "Currently such tools are still in their infancy, although they have significant potential and need a supportive environment."

The **eIDAS Regulation** 910/2014 concerning electronic identification and trust services for electronic transactions in the internal market is now under revision. The proposed revision - European Digital Identity (EUID) - among other elements extends the current regulatory framework of trust services to include electronic ledgers, a more general and technology neutral concept than blockchains or distributed ledgers. An electronic ledger is defined as "tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering". An electronic ledger could also be qualified, enjoying "the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger."

The proposed EUID Regulation also redesigns the cross-border authentication to online services as provided by the original one, which is extended to public and private services, and it is defined following a self-sovereign identity (SSI) approach. In a typical SSI approach, digital identities are managed in a decentralized manner, and subjects have full control of their identities without relying on central authorities or store of data. It is worth noting that an SSI approach could or could not be implemented with an underlying blockchain technology and that in the EU context, every digital identity has a root of trust based on nationally issued electronic identities.

In the financial sector, the proposal **Digital Operational Resilience Act (DORA)** briefly addresses blockchain technology in the context of crypto-assets, as one of its applications, but refers to the relevant policies addressing blockchain to facilitate its promotion throughout Europe.

In fact, Digital Operational Resilience Act (DORA) Regulation applies also to the crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens (Article 2.1e). However, DORA does not specifically deal with crypto assets, which are regulated in MiCA (Markets in Crypto-Assets Regulation) proposal.

MiCA (Markets in Crypto-Assets Regulation) proposal: the European Union intervened to regulate all cryptocurrencies not covered by existing EU financial services regulations and proposed MiCA regulation for digital currencies. It establishes a set of uniform guiding principles for cryptocurrencies and crypto assets. These guidelines involve transparency, authorization, supervision, organizational and governance measures, consumer protection and market abuse prevention. MiCA regulation proposal wants to push innovation and, on the other side, to address financial stability and monetary policy risks that could arise from a wide use of crypto-assets and DLT-based solutions in financial markets, guaranteeing investor protection, through rules that provide clarity and legal certainty to issuers and suppliers of crypto-assets.

6. Recommendations and future directions

Blockchain capacities have opened a huge variety of potential use cases in different sectors such as industry, finance, energy, insurance, health, logistics and public sector. In the public sector, it is possible to identify several potential use cases. According to data from Moody's Investors Service, some of the experimentations are focused on: recording and identity management, voting, taxes, government and non-profit transparency, legislation, compliance and regulatory oversight.

Financial Institutions	Corporates	Governments	Cross-industry
International payments	Supply chain management	Record management	Financial management & accounting
Capital markets	Healthcare	Identity management	Shareholders' voting
Trade finance	Real estate	Voting	Record management
Regulatory compliance & audit	Media	Taxes	Cybersecurity
Anti-money laundering & know your customer	Energy	Government & non-profit transparency	Big data
Insurance		Legislation, compliance & regulatory oversight	Data storage
Peer-to-peer transactions			Internet of Things

Source: Moody's Investors Service

Figure 1: Selected Potential Use Cases [8]

Technical" use cases could be defined, i.e., defining how the Blockchain can help facing challenges discussed in Section 3.

- Use blockchain as a security enabler, promote its usage in projects, but not forgetting that it isn't a silver bullet solving all the issues.
- Provide funds for the human aspects: education and trainings for secure coding, awareness and related fields as we need skilled and aware people creating and using such technologies.
- Provide funds for industry-government/public-academia cocreation of EU Cyber Centre addressing the following challenge: governments and organisations operate in silos while the internet is an integrated system of computers, algorithms and networks, acting as a horizontal layer, hence destroying the traditional barriers (jurisdictions of agencies, authorities and nations). There is a need for a profound and holistic approach for policy making and the creation of a single framework, which cannot solve all the threats and issues, but there needs to be one single framework applicable for all computers (and as everything is becoming a computer it will impact everything). By placing such a cooperation in effect EU would have a huge step towards digital autonomy and global cyber safety: as software manufactures are using usually one software version globally if they would like to operate in the EU, they would need to comply to the framework hence making the whole world a safer place.

[8] https://bravenewcoin.com/news/moodys-new-report-identifies-25-top-blockchain-use-cases-from-a-list-of-120/

Acknowledgments

The European Cybersecurity Organisation's (ECSO) WG6 aims to contribute to define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem. From the analysis of the challenges of digitalisation of the society and industrial sectors this WG identifies what are the capacities and capabilities to sustain EU digital autonomy by developing and fostering trusted technologies.

The following is a special acknowledgement of the active contributions in various capacities from ECSO WG6 Members.

EXPERT CONTRIBUTIONS: Ana Ayerbe (TECNALIA), Csaba Virag (Talegen), Elia Vimercati (Intesa San Paolo), Gürkan Gür (ZHAW), Ivan Gutierrez Agüero (TECNALIA), Kimmo Halunen (VTT), Konstantinos Votis (CERTH/ITI), Marc Vauclair (NXP), Mara Sorlini (Intesa San Paolo), Oscar Lage (TECNALIA), Paolo Campegiani (Bit4Id), Roberto Cascella (ECSO)