



SME Guide on Blockchain and Distributed Ledger Technology



Experts:

Andrea Caccia

Paolo Campegiani

Antonio La Marra

Donato Russo

Daniele Tumietto

Coordinator:

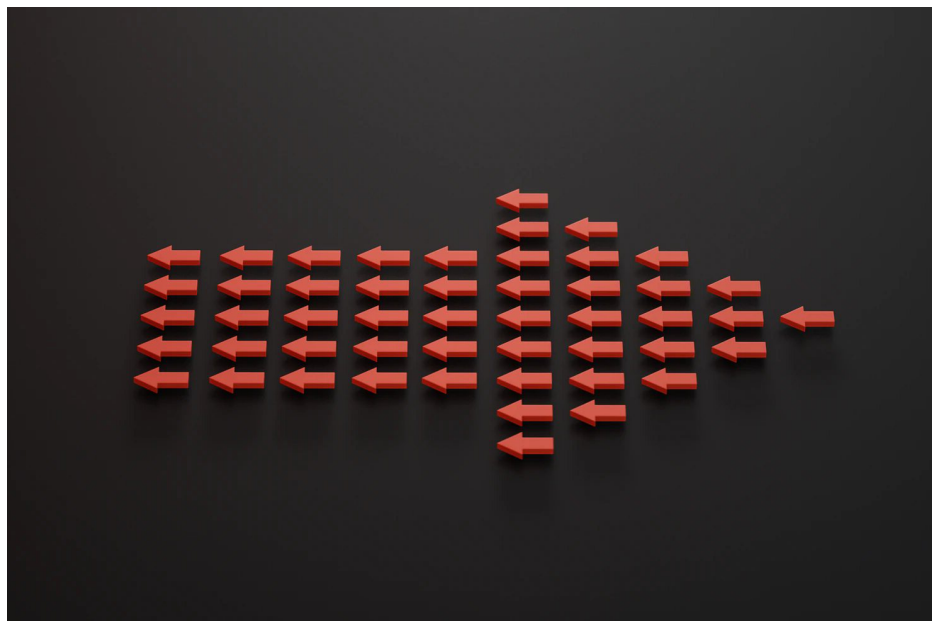
Omar Dhaher

Published:
December 2022

ABOUT THIS GUIDE

Small Business Standards (SBS) is the association representing European small and medium-sized enterprises' (SMEs) interests in standardisation at the European and international levels. Its main goals are derived from Regulation 1025/2012 on European standardisation. SBS aims to increase SMEs' awareness and influence in standardisation. It does this by facilitating the uptake of standards by SMEs, representing their interests, and motivating them to engage in the standardisation process.

The European DIGITAL SME Alliance (DIGITAL SME) is a member of SBS. It is the continent's largest network of ICT SMEs, representing around 45,000 digital SMEs.



In its efforts to raise awareness and help SMEs adopt and use blockchain standards, SBS has developed this guide on blockchain and Distributed Ledger Technology (DLT).

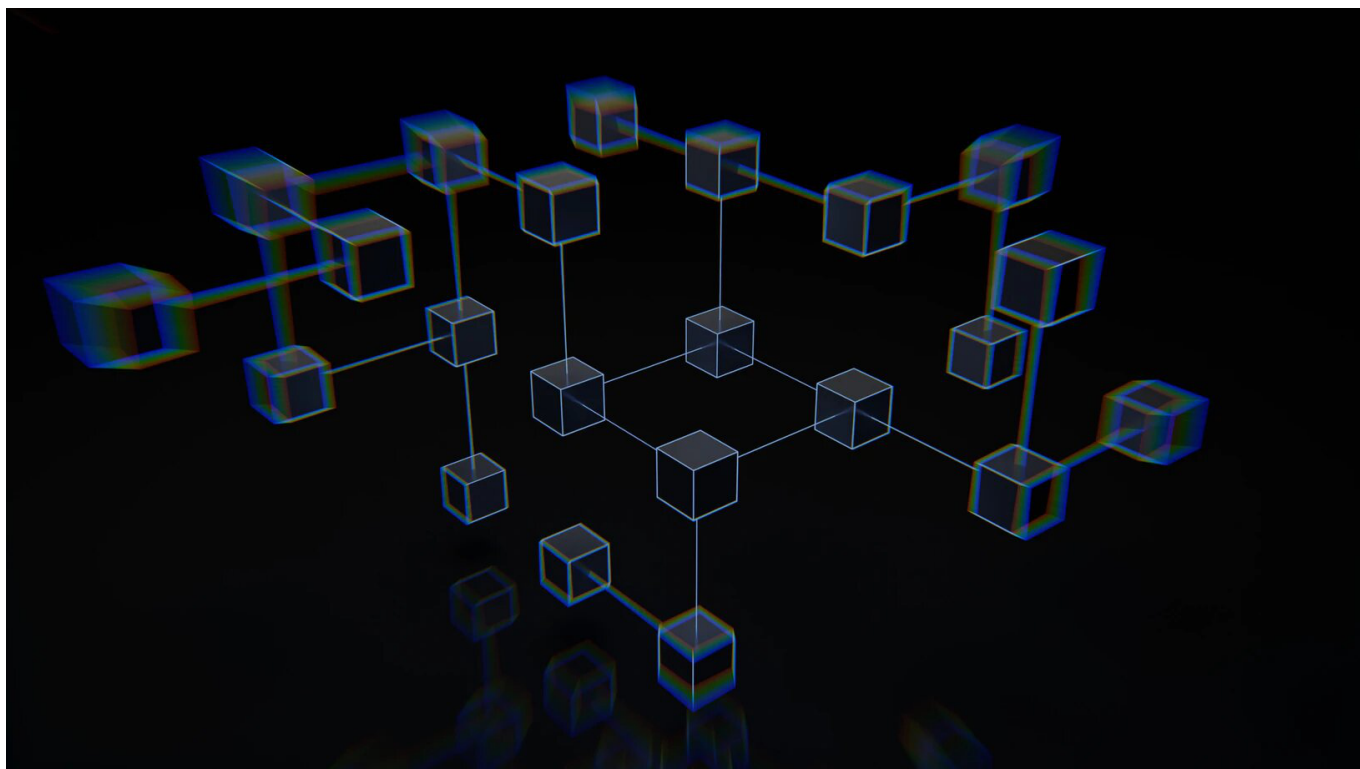
SBS is the sole proprietor of this free and publicly available guide.

List of Acronyms

AML	Anti-Money Laundering
API	Application Programming Interface
BFT	Byzantine Fault Tolerance
DAO	Decentralized Autonomous Organisation
DApps	Distributed applications
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
eHDSI	eHealth Digital Services Infrastructure
eID:	Electronic IDentification
eIDAS	electronic IDentification, Authentication, and trust Services
ESOs	European Standardisation Organisations
ESSIF	European Self-Sovereign Identity Framework
EUDI	European Digital Identity
GDPR	General Data Protection Regulation
IoT	Internet of Things
KYC	Know Your Customer
MiCA	Markets in Crypto-Assets Regulation
NFT	Non-Fungible Token
PoS	Proof of Stake
PoW	Proof of Work
SBS	Small Business Standards
SDOs	Standards Developing Organisations
UI	User Interface
ZK Rollup	Zero-Knowledge Rollup

TABLE OF CONTENTS

INTRODUCTION	5
1. INTRODUCTION TO BLOCKCHAIN AND DLT	6
1.1 What is Blockchain and DLT?	6
1.2 Motivation for using Blockchain	10
2. CHARACTERISTICS OF THE BLOCKCHAIN AND DLT	11
2.1 Security	11
2.2 Identities of People, organisations, things, and Data	13
2.3 Authentication and permissions	14
2.4 Governance	15
3. USE CASES TO SUPPORT STANDARDISATION, SUSTAINABILITY, AND STRATEGIC AUTONOMY	15
Case 1: The civil registry	16
Case 2: The certification process in the construction industry	18
Case 3: Digitising Textile Industrial Districts	22
Case 4: The Huawei backdoor case in IoT networking equipment – The European approach	28
4. BLOCKCHAIN POLICY PRIORITIES	30
4.1 European policy towards Blockchain	30
4.2 China's policy on blockchain and its impact on European SMEs	34
5. STANDARDS FOR BLOCKCHAIN	35
5.1 Blockchain Standardisation landscape in Europe – link to policy priorities	35
5.2 Standardisation needs	35
5.3 Different standardisation organisations involved in blockchain	36
CONCLUSION	39
BIBLIOGRAPHY	40
ABOUT THE EXPERTS	41



During the past years, SBS has published SME Guides to raise the awareness of SMEs for enabling technologies such as the [Internet of Things](#) or guide them through the implementation of specific standards such as the cybersecurity standards [ISO/IEC 27001](#) and [27002](#).

This year, SBS developed a guide on blockchain and DLT. As an enabling technology, blockchain is helping several sectors to become more efficient. Sectors such as agriculture, textiles, construction, ICT and finance use blockchain to share and authenticate transactions in a faster and decentralised way or enhance the transparency of the supply chain, which combats fraud and strengthens the sustainability of raw materials. Section 3 provides four use cases showing how blockchain can strengthen sustainability in the textile industry, help the construction sector in certifications, ensure authentication and trust in identification, and strengthens policy response to geopolitical issues.

On the policy level, blockchain has also many applications. For example, the EU plans to use blockchain to strengthen the identification of persons and things through the eIDAS regulation and reduce contractual disputes (especially in the data economy) through smart contracts.

Standards are essential in the functioning of electronic identification and smart contracts. They are also essential to the functioning of blockchain as a whole, considering that blockchain depends on decentralised databases' structure for which standards for storage, data exchanges, security, and other issues, are required.

SBS publishes this guide with the aim to raise SMEs' awareness of the technology and its role in supporting the EU goal of leading the way for the digital transformation and green transition. The guide targets SMEs' management to provide a basic introduction to blockchain technology, its characteristics, and areas where blockchain can help with their daily operations.

1. INTRODUCTION TO BLOCKCHAIN AND DLT

1.1 What is Blockchain and DLT?

Blockchain and Distributed Ledger Technology are a systematic and technological approach to the problem of having different parties agree on some facts. To understand the problem, consider a social setting where a group of friends has to decide how to spend the evening: they could go to the cinema or go to the restaurant. Any of these choices has some different options: which movie are they going to see? Which restaurant would satisfy everyone?

A lot of us could agree that this kind of decision is time-consuming and finding a solution that is acceptable and welcomed by the majority of people can be very challenging. This problem is a specific instance of a much more general problem: the construction of consensus (consensus-building) between different parties.

Construction of consensus gets more complicated as we move from our social setting to the more rigorous formal world of distributed systems, which is comprised of autonomous systems, very often managed by different organisations and subject to different organisations.

In a normal setting, such consensus is reached through a central authority. For example, the central bank offers trust for the currency people use. But such central authority is usually bureaucratic, resulting in slower transactions and risk of lack of transparency. Consequently, this increases the risk of fraud, such as money laundering. This fraud is magnified if the central authority is not independent, having being captured by one stakeholder to serve its interests, rather than the society's.

Blockchain was the answer to the flaws of a centralised systems. Its main premise is a consensus-building mechanism through decentralised system, where it is impossible for all participants to collude and agree on something against the rules, enhancing transparency, combating fraud, and resulting in more democratic societies.

To achieve that technically, blockchain and DLT are defined as “a type of database that is decentralised in nature, eliminating the need for an intermediary to process, validate or authenticate transactions”¹.

The invention of Bitcoin in 2009 by the group of people collectively called Satoshi Nakamoto, has revolutionised the approach of consensus-building to allow it to be reached between an almost arbitrary number of systems. The system is based on a game theory approach. The different parties (distributed systems) are assumed to be in a conflict of interest, and a set of incentive mechanisms is designed to help them quickly reach a consensus.

The consensus is about some transactions, i.e. transfers of virtual money (called “bitcoin” with the lower initial when we refer to the currency) between different parties. While we do not discuss here the details of the transactions or how these parties are identified in the system and could properly move money between them, we highlight that there is a clear conflict of interest between them.

If A has to give some bitcoin to B (as part of a larger transaction, like to pay for some of B's services or products), A would be very happy not to pay B (while receiving the goods), while B, if it could choose, prefers to receive the bitcoin without giving anything in return. This means that both A and B need a protocol, a set of rules that could find a reasonable compromise between them. This problem in the digital world mimics is what happens in the real world, where typically A pays B by giving it some physical money, in exchange for some goods. Many mechanisms, both of social, technical, and legal nature, are

¹ <https://www.mas.gov.sg/development/fintech/technologies---blockchain-and-dlt>

built around this exchange to make it sufficiently secure for both parties.

In the digital world, the problem lays in the fact that we cannot rely only on A or B as there is a conflict of interest, and before Satoshi Nakamoto's invention, we had to apply a primitive consensus algorithm known as [BFT algorithms](#). But, if we have many transactions happening together (e.g. A has a transaction with B and another with C, then there is a transaction between D and E, ...), these algorithms are not effective as they do not scale well.

Bitcoin solves this problem by grouping all these possible transactions in blocks and then poses a challenge to anyone interested in solving it: finding a solution to a mathematical problem, which requires identifying a parameter that puts in a specific point in the block with all the transactions, make this "enlarged" block become a solution to the problem. The solution is very complex to find (essentially, it requires checking for all the possible values of the parameter, until a satisfying solution is found), but it is very simple to verify.

To avoid any forgery of the blocks, on top of having all the transactions and this parameter, each block contains some synthetic information on the immediately preceding block in this list. Assuming that the list of blocks is composed of B1, B2, B3, B4 ..., the block B3 contains synthetic information (a cryptographic link) to B2, so if B2 is changed after the appending of B3 to the chain, B3 would no longer be a valid block, and this effect will also propagate on B4 and all successive blocks.

This approach is essentially probabilistic. A very powerful opponent that does not like how the B3 block is structured (because, as an example, it contains a transaction that the opponent does not like) is free to calculate a different B3 block (deleting the disliked transaction from it) and then provide alternatives (B4, B5, etc.) blocks.

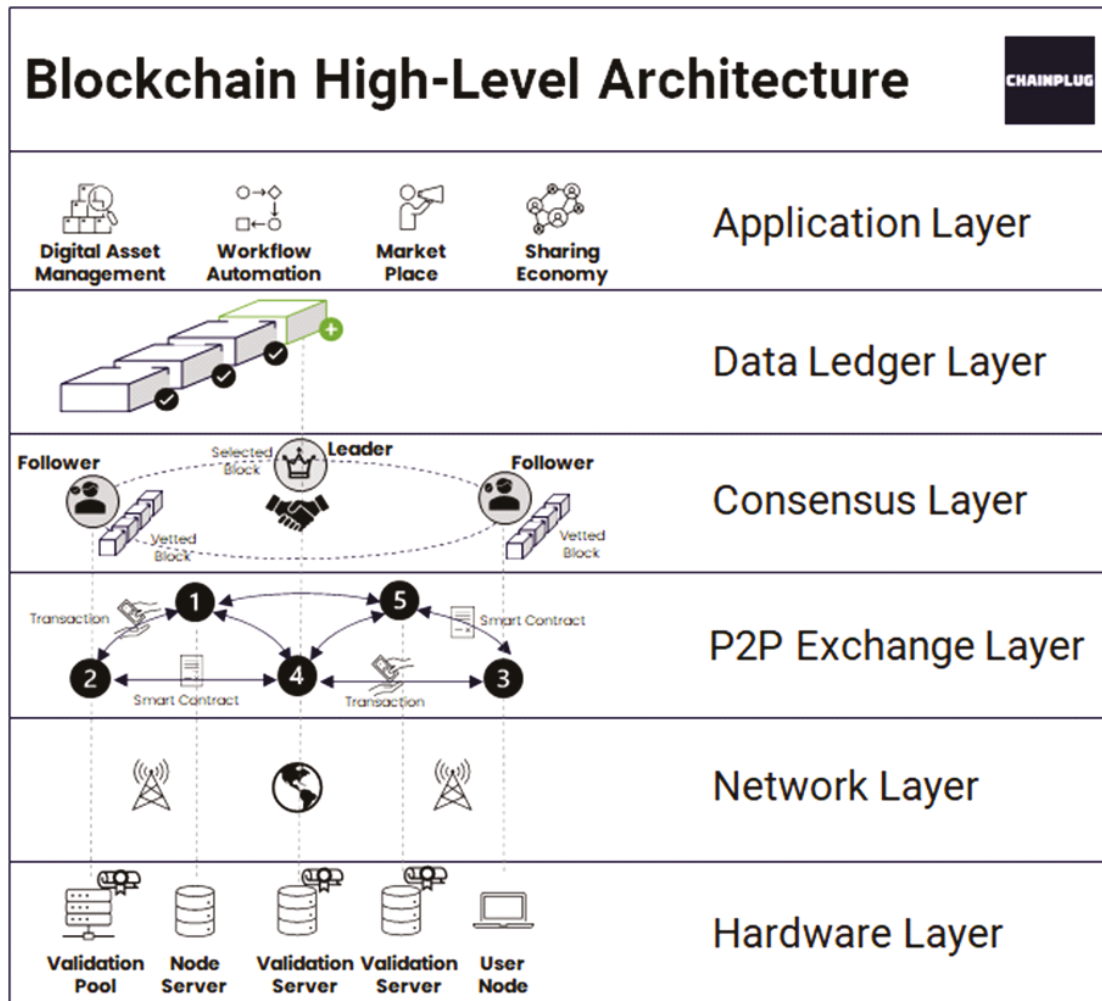
We discuss the properties of a blockchain system in the following paragraphs. To recap the qualifying element of a context that is conducive for the successful adoption of a blockchain system:

1. There is a large number of different parties. If the number of parties is very limited (less than twenty), there is no need for a blockchain system as BFT algorithms will be faster;
2. These parties are peer entities, so there is not a party that has more power than the others on deciding what is true and what is not. As an example, a bank will need to use a blockchain system to keep track of the movements of its customers as the bank has more power in certifying the movements in a saving account than its owner. On the contrary, the bank could choose to use a blockchain system for its interactions with other banks, as all banks are almost equal;
3. There must be some kind of latent or possible conflict of interest between all the parties. If all the parties are willing to give one of them a role of coordination or guide, then this leader could decide on the disputed transactions.

In summary, blockchains and more generally distributed ledgers are a way to create a consensus between peer entities (entities on the same level, so no one has more intrinsic authority than the others) where it is not possible to assume that all participants are acting in good faith.

1.1.1 The layers of blockchain

The following diagram illustrates the high-level architecture blockchain.



This architecture can be represented by 4 layers of blockchain:

1.1.1.1 Layer 0: Data transfer and Miners

This is the ground floor, where the internet, hardware, and connections exist that allow layer 1s like Bitcoin to run smoothly. Layer 0 is the basement that you never see, but it is as important as the building itself and can be considered a bridge between the Internet, the physical world and the blockchain.

In blockchain technology, there is not only software but there is also a physical network infrastructure that allows a complex technology (the blockchain) to work.

Layer 0 allows several things to happen:

Blockchains can interact with each other (interoperability)

- [Cosmos](#) is an excellent example. It creates an ecosystem of interoperable blockchains thanks to an Inter-Blockchain Communication protocol that is called [Tendermint IBC](#). Other examples of this layer are [Polkadot](#), [Cardano](#) and [Avalanche](#).
- For the developers, this is huge. If a decentralised application can run on one blockchain, it can

automatically run on other blockchains if they are built using the same level 0.

No need to invest more time and resources to build the same app on another chain.

Fast and cheap transactions

- With the Inter-Blockchain Communication protocol, Proof of Stake (PoS) consensus can be reached on several chains, thus allowing the expected result to be achieved almost immediately. The functional purpose is to have a block approved so that it can no longer be withdrawn and is therefore considered irreversible.

The result is faster and cheaper transactions on cross-chain exchanges.

Infrastructure for developers

- Finally, developers do not need to start from the ground up to build their blockchain. This is possible because many features of blockchains are pre-built and ready to be implemented immediately.

1.1.1.2 Layer 1: blockchains

Layer 1s are blockchains ([Bitcoin](#) and [Ethereum](#)) that process and finalise transactions on their own blockchain. This is where things like consensus ([PoW](#), [PoS](#)) and all the technical details like block time and dispute resolution take place.

It is responsible for protocols, consensus mechanisms and anything else that ensures the basic level functionality of a blockchain and its associated cryptocurrency (if any). It is also called Implementation Layer, alluding to the possibilities of development.

The three most important aspects of blockchains are conquering the blockchain trilemma²: decentralisation, security, and scalability. Still, no single blockchain has met the three criteria. Other examples of this layer are [Binance](#), [Solana](#), [Celo](#) and [Algorand](#).

A new kind of Layer 1 Proof-of-Stake blockchain like [NEAR](#) Protocol, is sustainable by design with its carbon-neutral footprint. With scalability (100k Transactions per second), low fees (<\$0.01), a privacy shard (Calimero) and an easy, onboarding experience which gives users a familiar Web2 browser experience, NEAR is rapidly taking over the market.

1.1.1.3 Layer 2: speed and scale

A point that is not always clear and a source of discussion is what Layer 2 is. The not-so-common definition comes from the consideration that different projects use Layer 2 for different activities. Let us consider, for example, the [Lightning Network](#) (a bitcoin scalability upgrade). It functions as a secondary implementation layer to Layer 1.

After all, smart contracts, which are a central feature of [Ethereum](#) and many other Layer 1 protocols,

²The problem is known as the Trilemma (as termed by Ethereum's founders Vitalik Buterin) and consists of the fact that major Blockchains, such as Bitcoin and Ethereum, cannot simultaneously (as they are designed) have the characteristics of: decentralisation, security, and scalability.

Generally, decentralisation and security are features that all Blockchains have. Whereas, with regard to scalability, which is the ability of a Blockchain to adapt to the constant growth in the number of nodes and users to which they are subjected, that is, to support high transactional capacity and future growth without performance being affected, the situation is the opposite.

One of the main problems of the most famous permissionless blockchains is precisely that of poor scalability. Various Blockchain developers have come up with various solutions and new Second Layers Protocols (Second Layers Protocol) with the aim of solving the problems of the lower protocols, thus coping with scalability, but the solutions do not represent true solutions of the Trilemma. To date, only Agorand, the Blockchain devised by Silvio Micali, is the only one that has solved the Trilemma at the first protocol layer (First Layers Protocol).

are applications built directly on the Implementation Layer. Let us imagine that Layer 2 represents the layer where additional updates and generalised applications produced in Layer 1 are developed.

Currently, Layer 2 is the area where there is most interest. Ever since Ethereum showed the possibility of using a generalised blockchain to develop narrow and specific applications, a lot of developers and investors have jumped in.

Layer 2s is considered as the scalability layer, and the third-party integrations are used in conjunction with Layer 1s to increase scalability and transactions per second.

- When you hear zero-knowledge rollups or ZK-rollup³, side chains⁴, or anything to do with speeding up transaction throughput, it is likely to be Layer 2.
- Examples of this layer are [Polygon](#), [Starknet](#), [Arbitrum](#) and [Optimism](#).

1.1.1.4 Layer 3: applications

Layer 3 may become the most successful layer in the future, even though it is currently experiencing a low level of appreciation. Layer 3 is the place where generic applications, developed on Layer 2, can be used to develop specific solutions. Using technologies such as smart contracts, atomic swaps or APIs, developers can integrate solutions and create applications that perform extremely vertical functions. Typical cases in this area are [DeFi](#) solutions or NFTs.

Summarising the concept as much as possible, Layer 3 is considered to be interoperability and is the user interface (UI) that we as consumers actually interact with.

1.2 Motivation for using Blockchain

Today, the first motivation to use blockchain is the transfer of value (crypto currencies). It has grown exponentially due to Bitcoin. The second motivation is recording transactions with a tamper-proof method not managed/certified by any third party designated authority.

In reality, the scope of using blockchain will be much broader in the medium-long term as it will remove intermediaries in trust management. This point will not only have a huge economic impact as it will allow faster interactions, reduce costs, and support certified information, but it could also deeply re-organise how our societies will be ruled in the future.

Because enabling trusted transactions directly between two or more parties, authenticated by mass collaboration and powered by collective self-interests shall limit trust intermediaries (individuals, companies, governments) that can bias the value of things, the perception of reality (fake information), or even limiting individuals' freedoms. By removing intermediaries to some extent, it will also promote strong interoperability supporting new interaction models that are strongly limited by conflicts of interest today.

Private vs public blockchains

The main difference between public and private blockchains is based on whether information can be registered freely.

³ A [ZK-rollup](#) is a Layer-2 blockchain protocol that processes transactions, performs computations, and stores data off-chain while holding assets in an on-chain smart contract. Naturally, traditional Layer-1 blockchain solutions like Ethereum validate blocks and transactions on-chain.

⁴ A [sidechain](#) is a separate blockchain network that connects to another blockchain – called a parent blockchain or mainnet – via a two-way peg.

A blockchain is public, so-called permissionless, when no authorisation is required to access the recorded data, to perform transactions or to participate in the validation of transactions and the creation of new blocks. Public blockchains do not have any filtering regarding operating mechanisms and participation in transaction stipulation, as it is the case with the better-known Bitcoin and Ethereum.

In the private, so-called “permissioned” blockchain model, only the participants identified and authorised by the initiator of the blockchain are authorised to write data and validate transactions, while the information is visible to everyone, even if it cannot always be deciphered and used. The private blockchain type is created by a creator entity that identifies the participants and determines the limits of the transactions that can be recorded on that blockchain.

The consensus formation process (as the Blockchain consortium) is controlled by a pre-selected set of nodes (so-called partially decentralised blockchains): this hierarchy between nodes prevents the loss of business intelligence information. When information is added, the approval system is not bound by the majority of participants but by a small number.

The system seems ideal for institutions or large companies that have to manage supply chains with a number of actors, businesses, suppliers or sub-suppliers. It guarantees a higher level of privacy, as no access or reading permissions are granted. Nodes are well connected to each other, and any malfunctions and errors can be easily remedied. Transactions are cheaper as they are verified by a few nodes with high processing power.

The most relevant difference between the two types of blockchains is the authenticity of the information which determines the consequences between the content of the transaction and its effect. In private blockchains, this causes difficulties for the user who must ascertain the veracity of a recorded piece of information.

2. CHARACTERISTICS OF THE BLOCKCHAIN AND DLT

2.1 Security

The term blockchain has often been used in strong relationship with that of cybersecurity. These two terms are not completely unrelated: to keep a consistent, unchangeable, and distributed ledger several technologies such as digital signature, hash functions have been used. It is also true that blockchain technology has been used in some products to improve security, especially in terms of logging.

However, it is a mistake to consider blockchains and their derived applications secure by default. In recent times, as it happens for most widespread technologies, some novel attacks on blockchain applications (especially to crypto markets) have been developed. Such attacks had a significant impact on personal wallets, resulting in people losing invested money and very little was possible to recover the situation.

On the other hand, cryptocurrencies, such as Bitcoins have been widely used by ransomware⁵ and cryptolockers and novel attacks have been developed in an attempt of exploiting victims’ hardware to mine cryptocurrencies such as Monero and Bitcoin as well.

2.1.1 Organisational security

Blockchain technology is seldom used to guarantee specific aspects of security in the context of extended

⁵ A malware that freezes your system by encrypting files and the hacker promises to give you access back after having paid a ransom. Refer to [SBS Guide on Information Security Controls](#) for more information on malware.

organisation. Whenever you need to trace goods or there is the lack of mutual trust between different actors or you need a ledger that can be always verified, then blockchain suits this need. There are some relevant blockchain projects especially in the agrifood sector that, thanks to blockchain, allow consumers to trace their goods up to their origin. This results in an increase of trust between customers and suppliers.

Information security typically means the set of technologies, means and procedures that guarantee three key characteristics of information: **confidentiality**, i.e. only the recipient can read the message; **integrity**, i.e. there is no possibility to tamper the message without the recipient recognising the change; **availability**, i.e. the recipient is free to choose when to read the message.

Blockchain technologies and applications are used specially to guarantee integrity in the sense of non-repudiation: since the blocks are concatenated there is no possibility for an attacker to alter a message without the system recognising the change. Blockchain algorithms can protect integrity well. Since there is no central point of trust and nodes are seldomly distributed in different parts of the world, it is of utmost importance to guarantee that, if one of the nodes is compromised it cannot do any damage. Blockchain technologies are also very useful to guarantee availability of information: since a blockchain node can be run in different parts of the network, you may obtain more proximity than a classical cloud system. The price to pay is of course performance because inserting information takes more time than with a classical cloud system.

To guarantee the integrity of information, blockchain technology leverage on so-called secure hash functions that guarantee that the content cannot be changed. One can imagine a hash function as a digital summary of the text. Altering the text has a severe impact on the resulting summary.

2.1.2 Cybersecurity

Blockchain security needs a different approach with respect to traditional security. This is due to some reasons:

1. There is no mutual trust between peers and systems in a blockchain environment. Therefore, everyone can be a malicious actor trying to pursue his/her own interests. Thus, every piece of the software and every system running that software needs to be scrutinised.
2. The type of blockchain used will influence the attack vectors deployed. For example, cryptocurrencies may be subject to Ponzi schemes⁶, or investors may lose everything (it happened with so-called Squid Game meme coins) because once people get money they can cash out and close.
3. Algorithms used to evaluate trust or to generate trust can have bugs or vulnerabilities that may make them easily hackable.
4. Having to use a significant number of resources to verify that a transaction can be executed, limits the number of actors.
5. Identity checking is a key factor. In fact, if one is able to create many fake identities, they can manipulate the market in order to promote one algorithm or the other showing a fake increase of projects using a specific algorithm.
6. Influencers can manipulate the market quite easily. For example, Elon Musk's tweets that boosted [Shiba Coin](#).

Even though some of these reasons are not directly related to cyber-attacks from some perspective, they are still related to cybersecurity because people may lose money, reputation or be hurt in their real lives

⁶ According to investopedia.com, a Ponzi scheme is a "fraudulent investing scam which generates returns for earlier investors with money taken from later investors."

because of misinformation or misbehaviour. Moreover, blockchain technology is way too often seen as a silver bullet for cybersecurity. Unfortunately, people seem too attracted to easy solutions to complex problems. The hard truth is that complex problems, like cybersecurity, require simple solutions and a careful approach.

Expert Angle

Recently, a company named Halborn has released a specific version of Kali Linux to perform Vulnerability Assessment and Penetration Testing on blockchain. If blockchain is so secure that no additional test is required, do you think a company would have spent money and effort to create their own Linux Distribution?

2.2 Identities of People, organisations, things, and Data

The verification of identities of different nature (people, organisations, things, and data) is a problem as old as the internet itself. During the past years, several solutions have been implemented: in particular, authentication systems based on authentication means assigned to people's identities. Similar technologies can be used for organisations' identification as it is in general possible to link an organisation with human roles to which identification means are assigned. These authentication means are based on the use of authentication factors such as usernames and passwords for the basic levels of assurance with additional factors (typically physical and biometric) to support substantial and high levels of assurance.

To increase security of (personal) information and data, complex passwords have been created. Still, copied or cracked passwords have not solved the problem of giving access to a huge amount of data. Additional factors are an effective means to The Internet of Things (IoT) where physical objects retrieve, generate and transfer data, poses new challenges to the identification of objects connected to the internet and the data they consume and generate.

The European Union, by means of the eIDAS (electronic IDentification, Authentication, and trust Services) Regulation, has provided a legal framework on electronic identification and trust services for electronic transactions in support of the European Single Market.

Another key initiative is the European Self-Sovereign Identity Framework (ESSIF), part of the European blockchain service infrastructure (EBSI) which is a joint initiative of the European Commission and the European Blockchain Partnership (EBP). It is an approach to digital identity that gives individuals control over the information and data they use to prove who they are to websites, services, and applications across the web, in line with the approach taken in the context of the revision of the eIDAS Regulation (known as eIDAS2) with the European Digital Identity (EUDI) Wallet.

However, both eIDAS2 and ESSIF refer to the identities of people and organisations. For example, wallets for natural and legal persons, eIDs and IoT devices linked to a natural or legal person identity. Identities of things and data, in current data sharing scenarios, cannot be autonomously managed as objects: at present stage, there is a lack of automatically certified and trustful identity of things.

The concept of digital twin can help provide a digital representation of the relevant characteristics of physical objects in a digital model representing their relationships and dependencies between each other and with native digital objects, people, and organisations.

Blockchain technology could overcome the lack of capacity of said objects to interact in a different way

at each different transaction. More in general, the need is to support proper, seamless and decentralised identification of people, organisations, things, and data as a foundational element that enables a whole series of applications.

For example, it is foreseeable that “Things” - such as industrial and commercial robots - once uniquely identified would be able to pay or be paid at completion of a certain assigned job.

Another example can be found in the context of the digital product passport (DPP), the key element supporting the proposal for a Regulation on for Ecodesign for Sustainable Products⁷ in the context of the Commission initiatives to make sustainable products the norm⁸. It should be possible to disclose product information in the DPP under the control of the product owner in a way that is similar to the personal information in self sovereign identity for humans.

Another policy initiative where blockchain has a clear role is the Data Act where Smart Contracts are the means foreseen to support the exchange of data and their remuneration, based on the concept of Data Spaces.

Blockchain smart contracts coupled to objects’ identities and wallets could therefore autonomously perform payment transactions related to the performed services and enabling to converge towards a unique solution for identification of people, organisations, things, and data.

2.3 Authentication and permissions

Blockchains and distributed ledgers could either be permissionless or permissioned, according to how (and if) users have to be recognised by the system before actually interacting with it.

In a permissionless system, the only requirement for a user to create a transaction with the system is to adhere to some technical specifications. As an example, in the Bitcoin protocol, a user could interact with the system if they have a private key. This key, akin to the private key that is required for a digital signature system, could be generated by the user autonomously. It is the only possible way for the user to transact with the others and allows for the full disposition of user’s assets inside the system. Once a user is equipped with such key, they could sign transactions on the Bitcoin blockchain. This bottom-up approach has a clear drawback: if the users lost their key, there is no intrinsic way for them to recover it, so all digital assets associated with that key (like crypto-assets) would be lost.

The opposite approach for blockchains is the permissioned one. In this case, users of the system have an identity before actually interacting with the system, and they have to authenticate before using it. This is very similar to a traditional online service, where the user authenticates and then access their assets (e.g. email), managing them as they wish. This approach has the benefit of allowing users to be more protected against the loss of their access data, as it would usually be possible to recover them (similar to the recover password feature provided by an online service).

We highlight that this distinction between permissioned and permissionless system is at the protocol level. Although Bitcoin is permissionless, nowadays it would be very difficult for a user to be completely anonymous while transacting over it. Typically, the user will transact through some specialised intermediaries called exchanges that have to identify people according to the Anti-Money Laundering (AML) or Know Your Customer (KYC) regulations. Even if the users put together the infrastructure for a direct access to the Bitcoin infrastructure, they still need someone to transact with, and the other party

⁷ https://environment.ec.europa.eu/publications/proposal-ecodesign-sustainable-products-regulation_en

⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0140>

could be forced to identify the corresponding party. Thus, the anonymity of the transaction is only at the protocol level and not at the user interface level. This problem is often referred to the centralisation of blockchains, which blockchain's critics often point to as a missing promise.

2.4 Governance

Distributed governance in blockchains is missing nowadays and is as important that decentralisation in transactions certification. Without decentralised governance, a limited number of partners will fix the rules at the beginning. Hence, it is very difficult to scale up blockchains for new users that might have totally different needs and expectations. Furthermore, accepting these rules might even be highly damaging to the users on the medium to long run in a way that is very difficult to predict at the beginning or the governments might rule out that they are not acceptable/lawful after the introduction of new standards and rules. This also implies that each blockchain will have its own architecture/code and hence no standards can be defined and agreed by a large group of users to achieve interoperability. Decentralisation versus centralisation?

3. USE CASES TO SUPPORT STANDARDISATION, SUSTAINABILITY, AND STRATEGIC AUTONOMY

The distribution chain (supply chain) today constitutes the terrain of choice for the application of blockchain technology.

The OECD, whose main mission is to support and guide governments to cooperate for a fairer, stronger, and cleaner global economy, had already highlighted alarming data, according to which the value of international trade in counterfeit goods amounted to USD 461 billion. The information, compiled in cooperation with customs authorities, showed that counterfeiting accounted for 2.5% of the total value of world trade (including food counterfeits).

For a manufacturer, it is essential to be able to reconstruct the origin of raw materials, semi-finished products, and the place and method of processing of products, in order to avoid heavy criminal as well as administrative penalties.

Therefore, the introduction of the new blockchain technology can represent, for the entrepreneur, not only a guarantee of protection and a tool to prevent counterfeiting, but also a means to increase the sustainability of the reference market, as well as an undoubted reflection on the reputational value.

Operational aspects and advantages in blockchain traceability

- Decentralisation: distribution among multiple nodes of information to ensure its cybersecurity and resilience. Traceability of transfers: the exact origin of each piece of information can be traced.
- Disintermediation: transactions are handled without intermediaries, i.e. in the absence of trusted central entities.
- Transparency and verifiability: the immutability of the register: i.e. the data recorded cannot be modified without the consent of all participants.
- Programmability of transfers: the possibility of scheduling certain actions, upon the occurrence of certain conditions.

It should be noted that the impossibility of modifying the information entered in the blocks prevents any subsequent tampering. The technological infrastructure is reinforced by the time certification system (date and time at which the data is consolidated), in accordance with the eIDAS "Electronic Identification and Trust Services Regulation".

Advantages

Traceability, transparency, sustainability: these are the advantages for a producer who allows his consumer to freely orientate their purchasing choices.

Authenticity

This strengthens the link between the brand and the consumer, who can verify not only the authenticity of the product, but also the processing steps themselves.

Waste reduction

Tracking food can generate greater efficiency in supply chain processes, with effects on improving stock management, reducing food waste, and strengthening supply chain relationships.

The following use cases explain how blockchain offers solutions to existing problems and help to drive forward innovation in many sectors with focus on sustainability.

Case 1: The civil registry

Description

In a third world country, due to complex historical and cultural processes, there are multiple different versions of the civil registry that are managed by different authorities. When a person is born, their parents choose a name, and this person grows up with this name (let's call this person Jake). Parents do not directly register this name with the local branch of the civil registry, as this is mediated by another person, like a doctor, a midwife or a tribal leader. Jake is known with this name by the local police authority, which manages a copy of the civil registry for their purposes.

The problem

One day, Jake decides to ask for a passport, as he wants to make a trip abroad. The problem is that, during the background check, the data in the police copy of the civil registry confirm that his name is Jake, but the data in the health council copy of the civil registry tells a different story: the midwife registered him as John, because she thought that was better or because there was some miscommunication with Jake's parents.

The problem for Jake is that these two sources of data consider themselves both authoritative, they are not aligned, and the problem just experienced with the passport could happen again in the future, when Jake asks for other documents from his country of birth or is involved in processes that require the information.

The solution

Blockchains and DLTs could be effective in managing this kind of discrepancies when different parties, each one with some authority over a specific matter, must make an agreement on a shared view of the world.

In Jake's case, the different copies of the civil registries, managed by many different authorities at national, regional, or local level, could empower a blockchain or a DLT to attest their agreement on Jake's name. A very high level of this approach would comprise a couple of steps: in the first, these different data holders make an agreement on Jake's name (so, they all agree that the name of this person is, actually, Jake: this could happen with a specific business process whose details are not of interest here) and each one of them, in the second step, provides for a transaction which states something like "for me, the person that I call Jake/John/... he's actually Jake". Each one of these registries does not have to change its data, but it would need to be equipped with a conformance layer, that allows one to attest (notarise) that such an agreement was made. Each one of these registries participates in the blockchain, which in this case is a private permissioned system, and having a copy of the blockchain allows each party (civil registry holder) to monitor what is happening. Writing a transaction in the blockchain, which is composed of all these different agreements about Jake's name, certifies that all the parties have agreed on that.

Now Jake could simply ask the local health council for his health record. Thanks to the new conformance layer, when the system sees a request for Jake, it understands that Jake is known as John for the local health council, and it retrieves information for him under this different name.

Generalisation

The reader could think that Jake's name problem could be more effectively solved by simply modifying Jake's data inside some systems. This could be or could not be possible, according to the current technology status of these systems. If one considers a broader generalisation, like at an international level, the approach based on blockchains and DLTs is more appreciable.

As an example, EU Member States are part of the eHealth Digital Services Infrastructure (eHDSI) which allows for two Member States to exchange some eHealth data when, as an example, a person born in country A needs medical services in country B. These two countries have, thanks to eHDSI, a working connection. However, the entire process of requesting patient's data could fail because the country of origin is unable to provide such data in a timely manner, and this would result in a possible degradation of the healthcare services as provided by country B. Each one of these countries is a sovereign state, so they also need to be capable of proving that this data has been requested and that it has been provided. The solution could be the creation of a blockchain shared by all EU Member States, where these two countries could store the requests of data and the provisions of data (not the actual data, just the requests and the answers). As this blockchain is shared by all EU Member States, if a conflict arises between A and B, a quick look at the ledger makes it clear if data have been provided or not⁹.

Other possible generalisations are in the carbon credit management schemas. Each country in the world has an allotted amount of CO2 emissions and it could pollute more by buying credits from cleaner countries. Again, as there is a need to ensure that this exchange will not be repudiated in the future, a global blockchain could be a solution.

We proposed a generalisation at the international level only because it makes clearer that different organisations could have different process to be integrated in a global system. In more local systems, there could be the need to make this kind of agreements between different parties such as local social welfare systems, local energy communities, and similar.

⁹ Interested readers could refer to Castaldo, L., Cinque, V. (2018)

Case 2: The certification process in the construction industry

In today's international marketplace, organisations want to be known for adhering to quality assurance and manufacturing standards. As an example, International Organization for Standardization (ISO) certification and other organisations establish credibility and trust within consumers, stakeholders, and other business partners. In fact, an ISO-level certification guarantees the applicant meets global standards for business, especially in trade situations.

The construction industry, like many other industries, needs to certify certain aspects of the production: from Quality Management to Health & Safety Management on building sites, and more. Certification is therefore a key part of the construction process. Here is what applying for ISO certification means:

1. The applicant should select the type of ISO certification needed for his/her construction industries.
2. He/she must select a recognised and credible ISO certification body (ISO Registrar).
3. He/she must make an application in the prescribed form which should include liability issues, confidentiality, and access rights.
4. The ISO certification body will review all the documents related to various policies and procedures being followed in the organisation. If there are any existing gaps, the applicant must prepare an action plan to eliminate these gaps.
5. Then, the ISO Registrar will conduct a physical on-site inspection to audit the changes made in the organisation.
6. As soon as the certifying body approves the applicant's management system, he/she will be awarded the required ISO standard.

A. The problem

A construction contractor, applying for a request-approval process to obtain a certification, faced a long, expensive, and time-consuming effort. ISO certifications and the like, do not meet any new and upcoming digitalised standard. A lot of time is spent on retrieving documents and managing them back and forth: certifications are mostly carried out by means of paper, emails, and PDF-files.

Not only did the lack of technology prolonged the time needed by the contractor to achieve the certification, it also potentially endangered its activity. The contractor could not see a seamless way to promote ISO certification among certifying bodies, authorities, public authorities and customers.

This process has led to frustration; therefore, the contractor decides to do something.

Traditional Model

How Construction Authority currently releases ISO certification

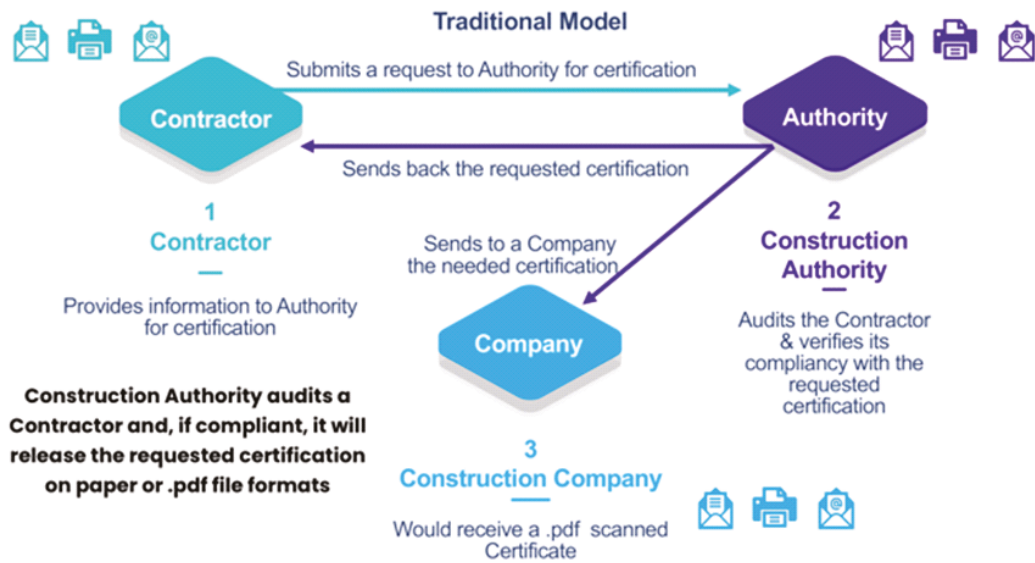


Figure 1- Traditional Certification process

B. The solution

The contractor contacts a software company (another SME) that specialises in blockchain applications, looking for an improvement of the certification process. For the contractor, sustainability is an important factor, having heard that blockchain technology is energy demanding.

Therefore, the company chooses a Layer 1 blockchain, sustainable by design. The technology to be developed integrates both with contractor's existing technology and interface with the certifying body in charge of the certification. Both integrations have to be made via Application Protocol Interface (API).

Proposed High-level Model

How Construction Authority will release ISO certification

CHAINPLUG

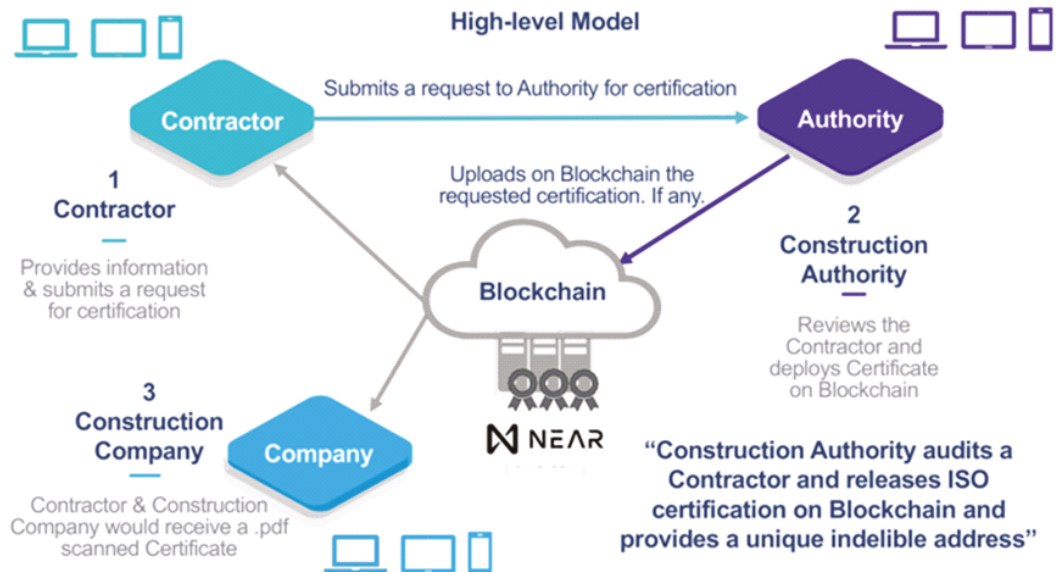


Figure 2- High-level Certification Model (Courtesy of Chainplug and NEAR Protocol)

The company in charge of developing the technology creates a blockchain collaborative platform where the request-approval process is created by means of a decentralised application (DApp).

With this technology, the certification process is managed via an application running on both PCs and mobile devices: a significant technological improvement.

Furthermore, the process of exchanging documents between the parts becomes more agile and efficient: the notarised workflow makes it possible to keep track of who-made-what-when and easily retrieves any document at any time.

- The contractor sends a request for certification to the chosen certification body.
- The certification body receives the request and internally assigns it to the account in charge of the task.
- The account accepts the new certification request and starts working on it.
- All the documents related to the various policies and procedures involved in the certification process are exchanged and notarised via the DApp.
- The various steps of the request-approval workflow progress are time-stamped and visible to both parts.
- The ongoing process ends either with an approbation and deployment of the certificate on blockchain or with a rejection deployed on blockchain as well or it is simply cancelled.



Figure 3 – Certification request-approval workflow

Courtesy of Chainplug

As a result of the implementation of this technology:

- The contractor is able to sensibly reduce both the time, the cost, and massively simplify the management of its certifications enabling its SME to benefit of the higher values of privacy, transparency and automation provided by blockchain technology: all this, without impacting on the environment.
- The certifying body experience the same with the advantage of having now the possibility to offer the collaborative process to all its clients thus making its certification processes a better, cheaper, faster experience.
- Being managed by smart contracts, the process is also able to pre-set remedies in case of litigation between the parts, thus reducing/limiting legal costs.
- As an additional bonus, information on the issued certifications was made available by the contractor to regulatory and control bodies, authorities and therefore, ready for any type of auditing, by providing a digital key to those interested in accessing the certifications published on blockchain.

C. Generalisation

The case of the construction contractor is of course very specific but also representative of many similar instances of digital innovation based on blockchain technologies.

What is the common ground?

Many productions and industrial workflows involve:

- Certification processes like the one here outlined in the construction industry are very common and apply to a large number of production environments and supply-chains.
- Certifications which are not possible to achieve for many companies, especially SMEs, given mainly their lack of resources and knowledge.
- Audits by clients, suppliers, and authorities.

These characteristics are typically not found in traditional processes involving certification, which are still mainly managed by means of paper, mail and PDF files.

In such cases, the adoption of blockchain technologies allows for a more effective data collection capability from the point of view of costs, speed, and scalability. Notable differences include:

- the ability to enhance the degree of privacy, transparency, automation, and sustainability of certification processes;

- the democratisation of the certification process by enabling a larger number of companies, notably SMEs, to provide their workers with more secure working environments and their clients with better products and services without impacting on the environment;
- the ability of blockchain technology to integrate both the Internet of Things (IoT) and Artificial Intelligence to constantly monitor their workflows also by predicting events.

Offering a collaborative and sustainable platform is the foundation of modern Web3 blockchain-based certification processes thus enhancing trust in any industry while protecting the environment.

Case 3: Digitising Textile Industrial Districts

The case concerns several Italian SMEs belonging to a textile district and, since centuries, transforming raw materials into yarns. What they produce is the basis of the creation of fabrics according to obsolete processes. The process to manufacture them is quite simple: different actors and steps work seamlessly in the final production. The raw material comes in the form of fibres that are spun (spinning is a twisting technique), to form yarn. The fibre intended is drawn out, twisted, and wound onto a bobbin. Then, fabrics are produced and transformed into cloths and garments.

The essential purpose of spinning is to obtain a final product as homogeneous as possible, that is, with uniform characteristics of strength, count, colour, cleanliness, and elasticity. In essence, spinning is a set of operations that transform a raw fibre into a yarn. Spinning requires processing phases of the materials indispensable for their preparation, which differ according to the fibres used. It starts from the preparation and carding to reach the spinning which can be followed by structural or aesthetic finishes such as Binatura¹⁰, washing, and dyeing.

The textile district presented in this case has a rather large number of SMEs (more than 7.000 companies) which, each in a specific step of the yarn-making process, concur to the production of cloths and garments.

A. The problem

Considering the emerging Web3 technologies (blockchain, IoT and artificial intelligence), SMEs in the district finds it difficult to switch, at district level, to a jointed technical-production and management innovation. The causes derive from three fundamental factors. The lack of:

- knowledge of emerging technologies and how to apply them to their industry.
- funds to be allocated to innovation.
- human resources capable of carrying out this digitisation process.

Therefore, they decided to join forces by creating a Decentralized Autonomous Organisation (DAO). A DAO is a kind of technological cooperative, blockchain-enabled, that has no central governing body and whose members share a common goal to act in the best interest of the entity.

In this case, the common goal was defined in the collaborative digitisation of the Textile District. The main benefits expected by the SMEs belonging to the DAO involves the possibility to collectively come

¹⁰ The doubling (binatura) is used to couple multiple threads (from a minimum of two to a maximum of 12 on a single reel before twisting the yarns, as a preparation for the next stage of processing: twisting. This process is carried out on the doublers. All doubling machines are of the latest generation with electronic control, for high-quality standards. Twisting is the heart of processing. Twisting provides that the coupled coils are loaded on the twisters which twist the threads from 2 to 12 strands altogether, to obtain a single thread made up of several threads. The yarns thus obtained can subsequently be used in the most diverse fields of application.

together, according to a predefined governance, from around the work to:

- share their problems.
- find the related technological solutions.
- finance their development.
- adopt the technologies.

therefore, jointly digitising their district while acting as a single entity.

Also, with the help of research by the Italian Ministry of Economic Development, in collaboration with IBM, some major challenges of the specific ecosystem were identified:

1. the difficulty of digitising, in a collaborative way, the district's technical-productive apparatus of the existing and future supply chains.
2. the quality control of both internal and external products & processes (2a), and the automation of the management of complex processes (2b).
3. the promotion of the well-being of personnel (3a) and the environment (3b), as well as predictive maintenance of machinery (3c).
4. the integration and control of the production part with that of storage (4a), and the outsourcing of workflows (4b).
5. the simplification of transaction validation processes, both inside and outside the textile district.

These difficulties seemed insurmountable enough that they decided that something had to be done.

B. The solution

The SMEs in question contacted a company (another SME) that specialises in collaborative blockchain technology and digital innovation. The company introduced them to the concept of business technological network enabled by blockchains and DLTs: a technological blockchain consortium or DAO.

The company's starting point was the analysis of the context and the problems of the textile sector. The process was a collaborative approach to identify needs and priorities. The result was the production of technological solutions satisfying both the single company and the district, as a whole.

By collectively adopting and/or integrating, via API, blockchain technology onto their existing ones, the SMEs were enabled to manage on a single platform the request-approval of certifications and transactions thus shifting their approach from the perspective of a single company to a holistic approach to the textile supply chain.

The company was able to develop and easily integrate the applications for the digitisation of the textile district by developing:

1. a blockchain peer-to-peer collaborative platform, punctually integrating both IoT and AI as well as other software and technologies.
2. the quality control of both internal and external products & processes (Figure: Solution 2a), and the automation of the management of complex processes (Figure: Solution 2b).
3. the promotion of the well-being of personnel (Figure: Solution 3a) and the environment (Figure: Solution 3b), as well as predictive maintenance of machinery (Figure: Solution 3c).

4. the integration and control of the production part with that of storage (Figure: Solution 4a), and the outsourcing of workflows (Figure: Solution 4b).
5. the simplification of transaction validation processes, both inside and outside the textile district.

Furthermore, the blockchain-hybrid collaborative platform, integrating the Internet of Things (IoT) and Artificial Intelligence (AI), allowed them to seamlessly adopt those emerging technologies laying the foundations for Web3, Metaverses and the creation of new value. That is facilitating their integration and collaboration on a single platform and providing them with a tool to make the SMEs competitive both within the local textile district and even towards large international value chains.


In the following¹¹, the solutions to be implemented for the benefit of the Textile District DAO.

Solution 1: District digitization of the technical-production apparatus of the existing textile supply chain

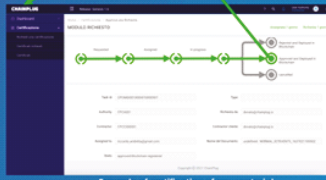
CHAINPLUG

It is implemented, peer-to-peer in blockchain, through Chainplug's collaborative platform: it punctually integrates both IoT and AI e allows sharing in maximum data-privacy & transparency, as well as enabling the creation of predefined supply chain workflows. Among other things, it enables:

- the digitization, both of business and supply chain processes, through the onboarding on Chainplug of the various actors of the specific production and / or distribution processes;
- the certification of products, processes and data-flows, as well as their automation also through the use of IoT and AI, both in the analytical and predictive phase;
- the creation of the certified ecosystem of the textile district;
- the integration, via API, onto blockchain, not only of each of their existing (and future) technologies: also with those of customers, suppliers and public and auditing Bodies.



Courtesy of MISE & IBM



Example of certification of raw material

5

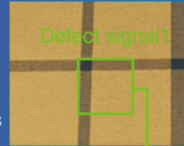
Solution 2a: quality control of both internal and external products and processes

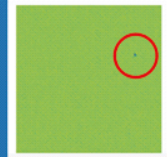
CHAINPLUG

To make quality control the most efficient, simple, reliable and economical, we have created a system that uses cameras, deep learning and blockchain for a rapid and reliable certified error detection.


- The customization of Machine Learning models allows us to manage and certify the different stages of textile production..
- The integration of artificial vision and sensors to detect events allows us to analyze and certify data capable of generating intelligent automation during production.
- Quality control of textile materials can also be done at the level of suppliers, both of raw materials and fabrics.

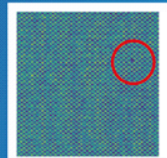
Defect signal!





Blockchain





Courtesy of KÓONE & BINÓOCLE

7

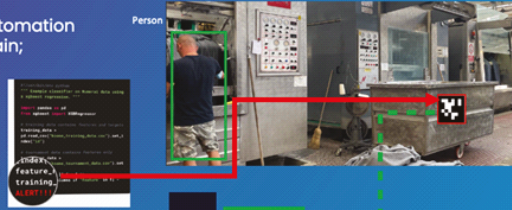
¹¹ Courtesy of Chainplug

Solution 2b: automation of the management of complex processes

CHAINPLUG

With the help of IoT and AI sensors, we have integrated into Chainplug a system that uses, in real time, artificial vision, sensors and tags to:

- detect and certify significant events in production processes in blockchain;
- generate intelligent and certified automation on the timeline of the production chain;
- automate the blockchain certification of both production processes and products;
- interface the Industry 4.0 technologies of customers, suppliers and Authorities with those belonging to the companies within the district.



CHAINPLUG Blockchain

Courtesy of KÓONE & BINÓOCLE

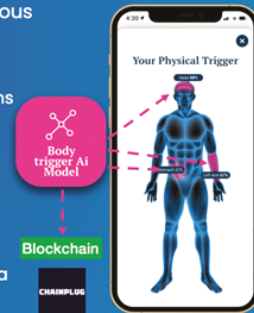
9

Solution 3a: promotion of staff well-being

CHAINPLUG

Thanks to AI models, integrated in Chainplug, it is possible to provide your employees and their families with an anonymous and certified system that:

- involves them in monitoring their psycho-physical well-being through interactions with the platform, also suggesting solutions to these problems with exercises to be done;
- allows the employer to assign their employee to tasks in line with their certified psycho-physical state;
- significantly reduces the risk of accidents at work and the liability of the employer and, possibly, to renegotiate the insurance premium at work;
- allows the creation of a sustainable work environment, also at a social level.



Courtesy of MIRRÓÓR & BINÓOCLE

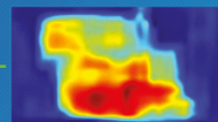
11

Solution 3b: promoting the well-being of the environment

CHAINPLUG

We have created, by integrating artificial vision and intelligence, a system that quantifies, specifies and certifies the waste material.

- The dedicated software generates certified data on the quantity and quality of waste.
- It allows, through the integration of sensors and AI, to certify both the materials and their disposal.
- The experimentation of integrating, within the yarn together with the raw material, of particular RFID antennas to produce traceable fabrics is being studied: from their "birth", to their "reuse", up to the "end of life".



Blockchain

CHAINPLUG

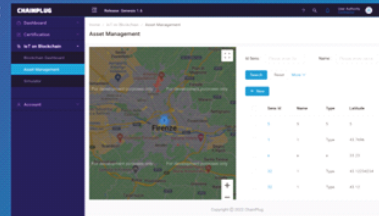
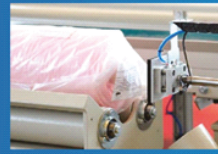
13

Solution 3c: predictive maintenance of machinery

CHAINPLUG

It is based on the integration of IoT, IIoT and IoRT in Chainplug's IoT platform for sensor management and on the Chainplug's "Patent pending" process of certifying the identity of things' identities, called KYD, (Know-Your-Device), as well as on the application of machine learning models. The technology allows to:

- > define the identity of the IoT through the blockchain registration of devices in the "Registrar of Things".
- > define in a "Smart Contract" and record in blockchain: identity, SLA, documentation, guarantee and so on of the specific IoT.
- > monitor and certify IoT activity in blockchain.
- > record and certify, in an automated manner and according to predefined alert levels, the correct functioning of: sensors, machines, cobots and robots.
- > in future developments, to autonomously send and receive payments, independently by the IoT, IIoT, IoRT used.



15

Solution 4a: integration and control of the production part with the storage one

CHAINPLUG

A consortium for participation in the KYKLOS 4.0 program of the EU is under construction, is under construction. This will be used to study and experiment, through particular RFID fibres/antennas, the integration and control of the production part with the storage one. This application will allow companies to:

- > intelligently arrange the RFID antennas along the "patch" and certify their production and storage.
- > immediately identify the geo-localization of tissues, using a mobile device camera or augmented reality visor.
- > to allow automated loading/unloading of yarns/fabrics, through the integration with the company's CRM/ERP and by means of RFID detectors;
- > eradicate counterfeiting and theft of yarns and fabrics, as the digital identifier is "intertwined" with the raw material.

NB: The RFID fiber / antenna under study resists pressures up to 60 Pascal and up to 200 industrial washes.



10

Solution 4b: Outsourcing of workflows

CHAINPLUG

Created through Chainplug's collaborative platform and thanks to the joint action of blockchain, IoT and AI through the API of the platform, to integrate it with quality control processes, both internal and external, supply-chains and technologies of various kind. The technology enables:

- > the creation in Chainplug, through dedicated Smart Contracts, of outsourced, predefined and certified workflows.
- > total control over the quality of the outsourced work.
- > the elimination of legal fees related to product non-conformities and various disputes.
- > accurate and certified management of the relationship with subcontractors and the certified maintenance of company's performance control.
- > the ability to maintain effective integration of third party production and / or logistics processes.
- > the certification and auditing of "third parties" and the work outsourced to them.



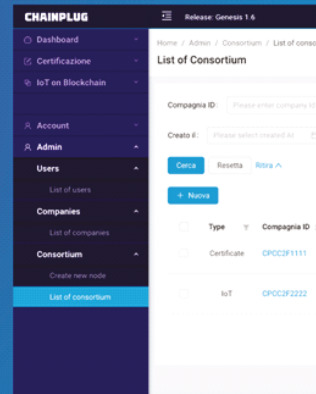
11

Solution 5: Simplification of transaction validation processes

Chainplug allows the creation of various levels of administration and use of the collaborative platform.

Furthermore, thanks to the joint action of blockchain, IoT and AI, it allows, through the platform's API, to integrate it with both internal and external quality control processes and technologies, such as:

- existing and future of Industry 4.0.
- traditional technologies (through IoT and AI).
- those of suppliers, customers, public, certification and auditing bodies.



C. Generalisation

The case of the SMEs of the textile district is of course very specific but also representative of many similar instances of digital innovation based on blockchain.

What is the common ground?

In almost any productive district, SMEs struggle to:

- know and understand blockchain and how to apply it to their business.
- have funds to be allocated to innovation.
- find human resources capable of carrying out this digitisation process.

These characteristics, shared by several SMEs, are not a good starting point for facing the needed digitisation process in any industrial district. Furthermore, SMEs run the risk of digitising their business using obsolescent technologies. Another factor to consider is the cost of the development and implementation of these emerging technologies which is higher than the generally adopted and available ones.

In such cases, the creation of a technological consortium (a DAO):

- allows the creation of shared knowledge, at district level, of the common problems to be solved by means of blockchain technology.
- provides a collaborative blockchain-based ecosystem where transparency, data-privacy, automation of workflows and common governance lay the foundations for new business models and value generation.
- enables the collective development of the needed technologies, thus allowing the SMEs to establish the desired level of privacy for their data and afford innovation.

By adopting collaborative blockchain technology, notable differences with the actual technological “status quo” of any production district include:

- the ability to coordinate heterogeneous companies, at different stages of production, by creating

cross-technological workflows, thus helping to dramatically reduce silos and fragmentation.

- the ability to communicate and transact across factory and enterprise boundaries (very welcome for supply-chain integration).
- the ability to eliminate/reduce litigation costs by defining within smart contracts the remedies in case of breach of either party.
- the ability to automatically validate and certify transactions between parties, also of economical nature.

Offering SMEs and any member of a district (and beyond), a single point of access to a value-governed collaborative platform and technology lays the foundation of modern, transparent, and automated blockchain-based district workflows and operations.

Case 4: The Huawei backdoor case in IoT networking equipment – The European approach

The United States national defence spending bill signed in August 2018 barred the U.S. government from purchasing equipment from Huawei and ZTE (another Chinese IoT producer), due to allegations that the Chinese government was using these companies to spy on other countries.

Several other countries, including Canada, India, and the United Kingdom, have also expressed similar concerns over security and espionage. However, the company has repeatedly denied any involvement with controversial political factions or the allegation that the Chinese government mandates it to include backdoors in the networking equipment it sells.

A. The problem

The Internet of Things (IoT) is a network of physical objects, “things”, embedded with sensors, software, and other technologies. IoTs, using sensors, software, and other technologies connected to the internet, have the purpose to connect and exchange data with other devices and systems over the internet. These devices range from ordinary household objects (home security cameras, wi-fi devices etc.), to sophisticated industrial tools.

Counterfeiting IoTs is a big problem for the industry. Another main concern is that the data IoTs send/receive could be manipulated and forwarded to unwanted third parties, thus generating a big concern about privacy, as in the Huawei [5G antennas’ case](#).

IoT producers and their clients are often faced with:

- counterfeiting of devices.
- loss of privacy and security, due to data thefts.
- potential damage to property and business.

With the industry and organisations gradually embedding “things” like cobots¹² and robots in their workflows, the problem is getting bigger and reaching a State-threatening security level.

¹² [Collaborative robots](#)

Therefore, the United States and other countries decided that something had to be done.

B. The solution

The solution provided by the US and other States was a complete ban on products from the two aforementioned Chinese companies. The European Commission has published a "toolbox" green lighting but restricting the use of higher-risk vendors: through the toolbox, Member States are committing to move forward jointly, based on an objective assessment of identified risks and proportionate mitigating measures.

One important mitigating measure could be provided by establishing trust between IoT producers and users. IoTs' counterfeiting could be eradicated, and trust could be generated either by defining a "thing"'s Self-Sovereign Identity (SSI) using certification provided by blockchain technology or by adopting the EU Digital Product Passport.

When in place, the two above-mentioned solutions could:

- uniquely assess the identity of each IoT.
- forbid the smuggling and counterfeiting of data.
- avoid property damage, intellectual property loss and legal costs.

C. Generalisation

As an example, a wide adoption of wearable healthcare and medical IoTs is on the way. They can be used for various reasons like:

- making an accurate diagnosis.
- building treatment plans.
- improving the security of patients.
- simplifying caregiving.
- continuously monitoring critically ill patients. etc.

Therefore, providing a unique identity to things could protect not only our security as a community and business community but also our personal well-being and health.

4. BLOCKCHAIN POLICY PRIORITIES

4.1 European policy towards Blockchain

4.1.1 European Commission – eIDAS & Smart contracts

The European Commission adopted a legislative proposal for the European Data Act, which specifies essential requirements for smart contracts for data sharing and requires the development of a harmonised standard aiming to facilitate the roll-out of smart contracts to support the cross-border exchange of data and their remuneration.

Smart contracts are a well-known concept implemented within blockchain and Distributed Ledger Technology (DLT). In 2017, ISO set up a new technical committee (ISO/TC 307) to develop standards on blockchain and distributed ledger technologies such as ISO 22739¹⁴, a standard vocabulary now under adoption as a European standard, that includes the technical definitions of all the main blockchain and DLT concepts, including smart contracts.

The technical definition of a smart contract in ISO 22739, also generally accepted by all the standardisation bodies, is:

A computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger.

The smart contract concept in the Data Act proposal is a legal and technologically neutral definition:

A computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger.

ISO 22739 also recognises that “A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction”. Therefore, the use of smart contracts in the context of the Data Act proposal is in line with the possible use of smart contract already well recognised and identified by ISO.

The use of the term “Electronic Ledger” instead of “Distributed Ledger Technology” in the Data Act proposal is a direct link to the eIDAS²¹⁵, the revision of the eIDAS Regulation, that defines an electronic ledger as:

A tamper-proof electronic record of data, providing authenticity and integrity of the data it contains, the accuracy of their date and time, and their chronological ordering.

eIDAS² also places electronic ledgers in the trust service context of eIDAS, defining a new trust service as: “the recording of electronic data into an electronic ledger”.

4.1.2 Shaping the global policy for blockchain?

Blockchain and DLT are key enabling technologies that are experiencing significant growth, especially in the EU. According to [Statista.com](https://www.statista.com), Blockchain market in the EU is expected to generate around €2bn in revenue by 2023, while [Business Market Insights](https://www.businessmarketinsights.com) forecasts a growth of the European blockchain market to around €59bn by 2028. COVID-19 has accelerated the adoption of blockchain solutions as it provides more trust to online transactions. European Banks are investing more in blockchains, while European

¹³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068>

¹⁴ ISO 22739:2020 “Blockchain and distributed ledger technologies — Vocabulary”, see <https://www.iso.org/standard/73771.html>. The standard is de facto available free of charge as preview at the following [link](#).

¹⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281>

Insurance companies are leading the adoption of blockchain technology. In addition, European companies, including SMEs, are showing promising progress in introducing sustainable and green blockchain solutions, while using standards to enhance traceability and transparency. For example, the use of UNECE standards to trace raw materials in the textile sector. COVID-19 has highlighted the challenges and opportunities of digital transformation, accelerating the need for digitalisation in all sectors as a key driver for recovery. Digital transformation for enterprises and public authorities, together with the sustainable green transition – the Twin Transition, became the EU’s two pillars for global leadership.

The enabling role of blockchain as the underlying technology for both digital transformation and the green transition has been identified early on by the EU and is reflected in its policies. Indeed, blockchain has the potential of improving processes in all areas of the economy and public administration, by bringing trust and helping track and trace data, which remains authentic and immutable. On digital transformation, the EC’s Data Strategy as well as the Digital Finance Strategy recognises blockchain’s potential as a decentralised digital technology, which can enable companies and individuals to better control flows and usage of data and enable a financial data space to foster data-driven innovation.

Regarding the green transition, the EU Green Deal, and subsequent proposals such as the revision of the energy package, the Ecodesign, and the Sustainable Product Initiative – including the Digital Product Passport – stress the importance of enabling and converging technologies, such as blockchain, the Internet of Things, and artificial intelligence to lead the green transition among all economic and social actors. For instance, the use of blockchain can enable tracking and reporting of reductions in greenhouse gas emissions along the entire supply chain, including manufacturers, suppliers, distributors, and consumers.

To achieve these goals, the EC has launched the European Blockchain Partnership (EBP) and the European Blockchain Services Infrastructure (EBSI), which will enable a cross sectoral deployment of blockchain through a single digital market for blockchain. However, the evolution of the EBSI infrastructure can only be addressed properly by developing interoperability with other networks that will be provided by the industry.

The EU’s ambitions to become a global leader in blockchain technology are further reflected in its blockchain strategy, aiming to (1) Build a pan-European public services blockchain; (2) Support legal certainty; (3) Bridge the investment gap by funding for research and innovation; (4) Promote blockchain for sustainability; (5) Support interoperability and standards; (6) Support blockchain skills development. In its support for the blockchain strategy, the EC wants to support a “gold standard” for blockchain that embraces European values and includes (1) environmental stability, (2) data protection, (3) digital identity, (4) cybersecurity, and 5 (interoperability).

The current attention on blockchain as a technology that helps the European Union in its pursuit of leadership in the green transition and strengthens Europe’s Digital Sovereignty can be traced to the following legislative proposals:

- General Data Protection Regulation, GDPR
- The Data Act (legislative proposal)
- The Regulation on electronic identification and trust services (EUDI - eIDAS2) (legislative proposal)
- The Markets in Crypto Assets Regulation – MiCA (legislative proposal)

The above legislative proposals (in addition to GDPR) show how the EC is cementing its efforts towards creating a single digital market for blockchain. For example, the Data Act, one of the main legislative proposals for Europe’s general decade emphasises smart contracts, which is based on blockchain and

DLT. The request for smart contract for data centres in the Annual WP 2022 for European Standardisation reflects the relationship between EC's policies and standardisation. The focus on European digital identity (EUDI) through the revision of eIDAS alongside GDPR rules will help manufacturers, retailers, bankers, consumers/citizens, and other players in the supply chains trust Europe's digital assets. In return, Europe's digital transformation and digital sovereignty is strengthened.

Another important aspect of blockchain strategy is the CO2 footprint. One of MiCA's goals is to support crypto mining activities that contribute to climate change mitigation and adaptation. MiCA's proposals for the landscape for crypto service providers and crypto assets in Europe and beyond will also be a game changer towards preserving Europe's digital sovereignty.

4.1.3 GDPR Impact on Blockchain

Creating a coherent and harmonised EU-wide system for the protection of personal data with a new European Data Protection framework is the main goal. Therefore, the European Commission approved the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Regulation (EU) 2016/679 has some new principles of adaptation, integration, and margins of flexibility. With reference to this document, we highlight the principle of Accountability that is an important addition because it introduces the shift from form to substance. Indeed, the data controller is responsible for complying with the principles applicable to the processing of personal data that can prove it.

The characteristics of the DLT as decentralised, unmodifiable and persistent must be assessed and coordinated with the provisions of EU Regulation No. 679/2016 - GDPR, to regulate the hypotheses of centralised processing of the data themselves because it imposes on the data controller a series of obligations that must be identified from time to time. Consequently, any processing of personal data carried out by means of DLT or Blockchain must comply with the fundamental principles established by the GDPR: the principle of lawfulness of processing, the principle of privacy by design, and the principle of privacy by default, which must also be based on the assumptions of lawfulness of processing.

This is because a system based on DLT or Blockchain, which uses personal data, falls within the scope of data protection legislation, must therefore fulfil several legal requirements.

Other critical but very important aspects include the **unmodifiability** of the information entered in the blockchain if personal data relevant to privacy have also been acquired, and linkage with the right to be forgotten, which provides for the possibility of requesting the deletion of data (Article 17 GDPR). It is not an absolute right as it is mitigated by the presence of a public interest or by the occurrence of the cases dictated by paragraph 3 of Article 17 GDPR; guarantee of the right of rectification, pursuant to Article 16 GDPR, of any inaccurate personal data: to be achieved through the request for data correction coming from all the participants in the blockchain and subsequent subscription of the data thus amended.

The **compliance** with the right to data portability (Article 20 GDPR) by making personal data available to the requester in an electronic format interoperable with systems other than the original DLT or blockchain. In any case, knowledge of data protection principles is the rationale behind the *"implementation of appropriate technical and organisational measures"*, bearing in mind that Article 25 GDPR provides for the principles of Privacy by Design and by Default, i.e., *"data protection by design and protection by default"*. This is a general obligation according to which: *"taking into account the state of the art and the cost of implementation, as well as the nature, scope, context and purposes of the processing, and having regard to the risks of varying degrees of likelihood and severity to the rights and freedoms of natural persons represented by the processing, both at the time of determining the means of the processing and at the time of the processing itself"*, the controller *"shall implement appropriate*

technical and organisational measures, such as pseudonymisation, to implement effectively the data protection principles, such as minimisation, and to integrate in the processing the safeguards necessary to meet the requirements of this Regulation and to protect the rights of data subjects”.

In accordance with the principles of **Privacy by Design and by Default**, the data controller must implement *“appropriate technical and organisational measures to ensure that only the personal data necessary for each specific purpose of the processing are processed by default”. In this sense, “this obligation applies to the amount of personal data collected, the scope of the processing, the storage period and accessibility”. This means that these “measures must ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person”.*

The implementation of a DLT or blockchain system cannot therefore disregard, when it contains personal data, the principles of privacy by design from the outset, and the principles that must be considered are:

- purpose limitation: data collected and processed must fulfil a predefined purpose and thus have a specified, explicit, and legitimate purpose, in order to be further processed in a way that is not incompatible with that purpose. Reuse of personal data for a purpose not initially intended is contrary to the purpose limitation principle;
- accuracy: the principle requires data controllers to ensure that personal data are 'accurate and, where necessary, kept up to date'. If not, they must be 'deleted or rectified' without delay. If the only purpose of the application is to document the occurrence of a fact at a certain point in time, by means of a time stamp, there does not seem to be any criticality with regard to the principle of accuracy;
- data minimisation and retention limitation: minimisation consists in collecting and processing a limited amount of data; such data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Data may be minimised at source or reduced to what is strictly necessary if imported from an existing source. Failure to minimise data increases the risk to the rights and freedoms of the data subject. It is therefore recommended that a DLT-based system be designed in such a way that the requirement for data minimisation is considered at the initial design stage, in accordance with the principle of privacy by design;
- confidentiality and integrity: personal data must 'be processed in a way that ensures appropriate security and confidentiality, including in order to prevent unauthorised access or use of personal data and of the equipment used for processing' (Recital 39 of the GDPR). Ensuring this principle requires both the knowledge of which data must not be disclosed to third parties and the application of appropriate technical and organisational measures to safeguard the data from disclosure. In DLT-based systems, potentially all or many nodes could be aware of personal data. Therefore, a balance must be found between the visibility of certain data to keep the system functional and distributed, and the application of technical measures to safeguard personal data from unauthorised access;
- transparency: this is a fundamental principle of data protection since data must be processed fairly and transparently. Data subjects must be fully informed of the relevant aspects of the processing of their data, including the purpose and scope of the data processed on the DLT network.

Additional requirements under the GDPR Regulation that should characterise any processing of personal data include: the right to be forgotten (art.17), the immutability of records: (art.17 (3)), the right of rectification (art.16), the right to data portability (art.20), information to be provided to data subjects (art.13 and 14), automated decision-making (art.22), data minimisation (art.5(1)(c)), data subject's right of access (art.15).

4.2 China's policy on blockchain and its impact on European SMEs

Concerning global initiatives, China has understood very clearly the benefits of blockchain technology and has prepared for its adoption at both national and international levels. This has been expressed at the highest level of the Chinese government when President Xi Jinping stressed that “blockchain technology will play an important role in the new round of technological innovation and industrial transformation” and that blockchain “should be taken as an important breakthrough in independent innovation of core technologies”¹⁶.

To reach this goal, the Chinese initiative established the Blockchain-based Service Network (BSN). As stated on its homepage, BSN is a cross-cloud, cross-portal, and cross-framework global public infrastructure network used to deploy and operate all types of blockchain-distributed applications (DApps). To support and facilitate the adoption of blockchain technologies, the state-controlled company has created two separate departments: National and International one. It is tackling the existing problem of the high cost of developing and deploying blockchain applications by providing blockchain resource environments to developers by greatly reducing costs associated with the development, deployment, maintenance, and interoperability of blockchain applications and accelerating the development and universal adaptation of blockchain technology.

BSN will offer three main services:

- permissioned services;
- permissionless services;
- interchain services.

Permissioned services are already running on the BSN China Portal (not reachable from outside of China). Due to regulations in China, permissionless services will only be available on the BSN International Portal and on international public city nodes (PCNs). Furthermore, the BSN International Portal will allow users around the world access to low-cost blockchain solutions.

In March 2021, blockchain technology was [mentioned for the first time](#) ever in a draft of China's 14th five-year policy plan. Its final version was approved by Chinese lawmakers and advisers at the end of their annual political meeting.

The document laid out China's goals to work toward in the next half-decade: it stressed that technology would play an increasingly important large role in the country's top-down planning. According to the draft, the use of artificial intelligence, big data, cloud computing, and blockchain is expected to contribute to the country's GDP and “transform China into a global leader”.

With its strong central authority, pervading both personal and business activities, the Chinese government has created, teaches, and wants to use blockchain in a different way when compared to decentralisation. As described by [Zhejiang University](#), the Chinese government is creating a blockchain with Chinese characteristics, where only permissioned blockchains are allowed in China. This results in a situation that where the Chinese government has no right to change data, it can delete the whole chain containing such data.

Therefore, the technological “decentralization under centralization” might be a risk for non-Chinese companies wanting to accept the inviting BSN Global blockchain offer.

Some risks that EU SMEs could face by adopting BSN Global Alliance technologies might include:

¹⁶ <https://www.coindesk.com/markets/2019/10/25/president-xi-says-china-should-seize-opportunity-to-adopt-blockchain/>

- Lack of transparency (who has access to data?)
- Loss of data, intellectual property, business secrets and privacy
- Censorship
- Loss of sovereignty.

Next to building its infrastructural supply-chain, China has therefore laid, by means of BSN Global, the foundations for its technological infrastructure supporting the “*New Silk Road*” by means of the “*Chinese blockchain*”.

Despite the attractiveness of the Chinese approach (low cost and quick adoption), it is advisable for European SMEs (and not only), to avoid the abovementioned risks, that is: to choose to develop their technologies by means of blockchains and DLTs where central authorities have access or worse, control, the technologies.

5. STANDARDS FOR BLOCKCHAIN

5.1 Blockchain Standardisation landscape in Europe – link to policy priorities

The European Commission’s Rolling Plan on ICT Standardisation, published annually, provides policy priorities for [blockchain standardisation](#). Although Fintech is the most prominent topic, smart contracts, and electronic identity is gaining traction due to their importance for the Data Act and eIDAS regulation. The Rolling Plan explains that blockchain and DLT have the potential to become the infrastructure for trusted, decentralised, and disintermediated services. In addition, blockchain is considered as a technology for the Single Market. This is because blockchain standards can redefine how transactions are done; therefore, reducing fraud, strengthening compliance, traceability, and trade within supply chains. Blockchain and DLT applications extend to the following sectors:

- eHealth
- Education
- eGovernment and public registries
- Security certification of Internet of Things
- Trusted Artificial Intelligence
- Food safety
- Managing intellectual property rights
- eID management

5.2 Standardisation needs

Interoperability and harmonisation remain the biggest obstacles towards cross-country and cross-sector transactions. Standards would allow a smoother application to cross-country transactions such as the banks/insurance example in section 3.1.2. Interoperability is important to eliminate or reduce vendor lock-in, which is important for SMEs who want to provide blockchain-based services in any sector (See

section 3, above). [The Rolling Plan on ICT Standardisation 2022](#) lists the following gaps:

- Governance and interoperability, organisational frameworks and methodologies, processes, and products evaluation schemes, Blockchain and distributed ledger guidelines, smart technologies, objects, distributed computing devices and data services.
- Identifying use cases which are relevant for the EU (including EU regulatory requirements like GDPR, ePrivacy, eIDAS, TOOP, etc.)
- Identification of actual blockchain/DLT implementations in the EU and assess the need for standardisation, harmonisation and workforce training or adaptation.
- Standardisation of the operation and reference implementation of permissioned distributed ledgers and distributed applications, with the purpose of creating an open ecosystem of industrial interoperable solutions
- A general framework for Governance of the European networks based on DLT should be developed to allow the flow of smart contracts between different networks.
- ESOs to develop the standards needed for the introduction of a programmable Euro (CBDC) and token economy (upcoming MiCA Regulation), in particular to ensure interoperability with smart-contracts, legacy systems, etc.
- SDOs to develop standards to support the eIDAS2 proposal requirements related to DLT.

5.3 Different standardisation organisations involved in blockchain

The following organisations are involved in blockchain standardisation to address the above gaps:

International Organization for Standardization (ISO)	ISO TC 307 works on international standards for blockchain focusing on improving security, privacy, scalability, and Interoperability.
Institute of Electrical and Electronics Engineers (IEEE)	The IEEE Blockchain initiative includes both horizontal and vertical working groups working on Data, Interoperability, Governance, Identity and Smart Contracts (horizontal), Energy, IoT, Healthcare, FinTech, Cryptocurrency and Digital Asset (Vertical).
International Telecommunication Union (ITU)	The ITU-T Focus Group on DLT works on Requirements, Assessment criteria and Reference framework. It covers finance, energy, digital media, e-health, public services, and other vertical applications.
World Wide Web Consortium (W3C)	W3C has recently established a Blockchain Community Group working on use-cases, Decentralised Apps and Digital Assets
CEN / CENELEC	CEN-CLC/JTC 19 focuses on specific standardisation needs to support European legislative and policy requirements in support of the development of the EU Digital Single Market. It gives primacy to international standards setting and develops standards for specific European standardisation needs and/or priorities.
ETSI	ETSI Industry Specification Group (ISG) PDL works on several topics related to blockchain and aims to intent is to address a gap in the landscape of DLT, Blockchain, Cryptocurrency and more to avoid redoing or duplicating existing standards
OASIS	OASIS work is based on open projects. The OriginBX project is a global alliance of organisations working on digital tax and trade attribute attestations for cross-border data transmission using legacy and blockchain platforms. The EEA Community Projects build high quality standards, documentation, for the Ethereum protocol

In addition to the above standardisation work, there is a number of European and global organisations and initiatives on blockchain technology and standardisation including:

A. EBSI – European Blockchain Services Infrastructure

The [European Blockchain Services Infrastructure](#) (EBSI) was established in 2018 when EU Member States, Norway, Liechtenstein, and the European Commission joined forces to create the European Blockchain Partnership (EBP).

While supporting public services at first, EBSI is expected to expand to cooperation with the private sector or private applications. This ambitious initiative of the Commission aims at strengthening EU leadership and autonomy in Blockchain while corresponding with its core values: being GDPR compliant, secure, interoperable and sustainable.

The initial set of EBSI use cases are:

- Traceability: Leveraging the power of blockchain to create trusted digital audit trails, automate compliance checks in time-sensitive processes and prove data integrity;
- Diplomas: Facilitated and trusted exchange of accredited diplomas across Europe, “significantly reducing verification costs and improving authenticity trust”;
- Self-sovereign identity: Deploying a European digital identity, “allowing users to create and control their own identity across borders without relying on centralised authorities, and enabling for compliance with the eIDAS regulatory framework”;
- Trusted data sharing: via blockchain technology data can be shared in a secure and trusted way amongst authorities in the EU, e.g., amongst customs and tax authorities.

Further use cases will be added to EBSI within the next months. The EPB is working on the three following use cases:

- Financing SMEs through blockchain via issuance and trade of SME bonds across Europe;
- Deploying a European social security pass for an easy access to welfare services across Europe;
- Allowing better management of asylum demand processes across Europe.

According to the interviews with European Commission staff, there will be a constant stream of new use cases that will be hopefully added to the EBSI, depending on the demand and the success of the current use cases. Further, around €50 million will be made available via EBSI for sandboxes that will help start-ups to deploy applications they want to sell across Europe, by allowing them to test their applications together with regulators in different areas to clarify the regulatory situation, and to adapt their solutions to make them compatible with the existing regulation.

B. International Association for Trusted Blockchain Applications (INATBA)

The [International Association for Trusted Blockchain Applications](#) (INATBA) was founded in 2019 and has currently around 170 members. INATBA offers developers and users of blockchain and distributed ledger technologies (DLT) a global forum. INATBA solidifies its international portfolio as a representative of the major blockchain stakeholders to provide more in-depth policy analysis and needs. Leverage their WGs to create a wider discussion and expand its network, INATBA is one of the focal points to connecting European experts with international blockchain standardisation initiatives. INATBA’s Committee of Standards works on channelling EBSI standardisation requirements and keeps INATBA on top of policy and standardisation developments.

C. ITU global blockchain initiative

The ITU-T Focus Group on the Application of Distributed Ledger Technology (FG DLT) analysed DLT-based applications and services that can be standardised by the ITU-T Focus Groups, identifying best practices and guidelines that can support the implementation of such applications and services on a global scale. They also identified a path for the ITU-T Standards Groups to study in order to meet urgent market needs. The group developed security standardisation documents for DLT-based interoperable services taking into account the activities undertaken by the various relevant groups, Standards Development Organisations (SDOs) and forums, writing a standards toolkit that can be used by national policy makers and regulators of ITU member states.

To support the development of baseline documentation for global standards for DLT-based applications and services, the objectives of the focus group were to:

- Establish links and relationships with other organisations that could contribute to DLT-based standardisation activities,
- Describe the ecosystem for DLT-based applications and services, and identify the respective roles and responsibilities of stakeholders in the ecosystem,
- Identify successful use cases for the implementation of DLT-based applications and services.

In addition, recommendations were made for future ITU-T study articles and related actions for various ITU-T study groups on:

- Concepts, coverage, vision and use cases of DLT-based services.
- Features and requirements for DLT-based services.
- Architectural framework and communication technologies of DLT-based services.
- Analysing and assessing the current state of DLT and its maturity.
- Researching the security and privacy aspects of DLT-based applications and services.
- Examining the means to extend online trust using DLT.
- Providing a platform for sharing findings and dialogue on policy and regulatory implications of DLT between companies working on DLT applications and regulators from various industry/economic sectors. Identifying stakeholders with whom ITU-T could further collaborate and potential collective actions and specific next steps.

CONCLUSION

Using enabling technologies to innovate, produce, and provide solutions is becoming increasingly part of every SME's business and naturally corresponds to the long-term goal of digital transformation and green transition, the so-called twin transition. SMEs are integrated into the global supply chains. Blockchain and DLT provide great solutions to existing problems regarding authenticity and the sustainability of raw materials. As such, it significantly increases trust and contributes to greening production.

This guide has provided SMEs with basic principles of blockchain and DLT. It explained how blockchain can help SMEs in strengthening the transparency and sustainability of operations.

Blockchain standardisation is important for scaling up solutions and reducing costs for SMEs as shown in the use cases for construction and textiles. Standards ensure trust as well and enable all stakeholders to conclude transactions in a safer environment. The geopolitical aspect of blockchain standardisation is also important and SMEs need to find a balance between affordable blockchain solutions and applying European values, while remaining open to global trade as the Huawei use case illustrated.

The European Union's policy towards blockchain and its work on standardisation to achieve these objectives set the landscape scene for SMEs in relation to the expectations of blockchain role in the European economy in contrast to other global markets.

BIBLIOGRAPHY

European Commission. (2022). Proposal for a Regulation establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC. Brussels: European Commission. https://environment.ec.europa.eu/publications/proposal-ecodesign-sustainable-products-regulation_en (Retrieved November 15, 2022).

European Commission. (2022). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS On making sustainable products the norm. Brussels: European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0140> (Retrieved November 15, 2022).

European Commission. (2022). PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HARMONISED RULES ON FAIR ACCESS TO AND USE OF DATA (DATA ACT). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068> (Retrieved November 15, 2022).

European Commission. (2021). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281> (Retrieved November 15, 2022).

International Organization for Standardization. (2021, December 21). ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary. International Organization for Standardization. <https://www.iso.org/standard/73771.html> (Retrieved November 15, 2022).

Small Business Standards (SBS). (2022). SME Guide on Information Security Controls. Brussels: SBS. Retrieved from <https://www.sbs-sme.eu/news/sbs-publishes-sme-guide-smes-information-security-controls>

Small Business Standards (SBS). (2021). SME Guide for Industrial Internet of Things (IIOT) – Special Focus on Security. Brussels: SBS. Retrieved from <https://www.sbs-sme.eu/news/new-sme-guide-industrial-internet-things-helping-smes-through-digital-transformation>

Castaldo, L., Cinque, V. (2018). Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe. In: et al. Security in Computer and Information Sciences. Euro-CYBERSEC 2018. Communications in Computer and Information Science, vol 821. Springer, Cham. https://doi.org/10.1007/978-3-319-95189-8_5

Small Business Standards (SBS). (2017). SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management. Brussels: SBS. Retrieved from <https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management.pdf>

Regulation (EU) 2016/679. The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Parliament, Council of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (Retrieved November 15, 2022).

ABOUT THE EXPERTS

Andrea Caccia

Senior Consultant, Project Manager, Standard and regulation compliance, product development coordinator on:

- Trust Services, and all related product and technologies, e.g., eSignature, eSeal, eDelivery
- electronic Invoicing and archiving
- blockchain & DLT

Andrea participates in the most important European Standardisation activities (ETSI, CEN, ISO, UNI/ UNINFO, OASIS).

Paolo Campegiani

Digital identity and blockchain expert, head of strategy and innovation for Bit4id, a European digital identity provider. company representative in many organisations, including INATBA, ECSO, EEMA, CEN CENELEC, ISO. Project leader of ISO Technical Report on blockchain and digital identity TR23249.

Omar Dhafer

Senior Technology Manager at DIGITAL SME. Coordinator of DIGITAL SME WG Standards and WG SBS Digitalisation. Member of the Task Force Rolling Plan of EC's Multi Stakeholders Platform on ICT Standardisation. Experienced in ICT, industrial policy with reference to Telecommunications Regulatory Frameworks, entrepreneurship, work-based learning, digital skills, research, and standardisation.

Antonio La Mara

Antonio La Marra is the CEO and founder of Security Forge. Security Forge is a startup that tackles the problem of secure data sharing and data sovereignty via a data security platform named GUARDA. GUARDA is powered by data usage control technology. Antonio has a solid technological background having spent more than three years as Research Assistant at IIT-CNR where he had the opportunity to work with awesome tech such as usage control, malware analysis, car hacking among the others.

Donato Russo

Blockchain Pioneer, European, innovative, multidimensional, dyslexic thinker: a digital transformation leader at the forefront of change, leading and managing cutting-edge digital solutions and complex global delivery to support sustainable IT transformation, smarter commerce, application innovation and the rise of Web3, DAOs and Metaverses. By helping companies and organisations in defining, spreading and monetizing on Values, leverages subject matter expertise and exemplary leadership to deliver the operational and shared growth of sustainable business in any-verse. Forward-thinking and tenacious. Extinction Rebel. Encouraging others to build consensus.

Daniele Tumietto

Independent consultant, senior advisor, innovation manager. Daniele is also an adjunct professor at the Link Campus University in Rome (Italy), POLIMI Graduate School of Management of Milan and O.M. Beketov University in Kharkiv (Ukraine).

Member of several Standard technical committees (UNI/UNINFO, CEN, ISO, ITU, UN/CEFACT) in Sustainability, ESG and Circular Economy, e-invoicing, e-procurement, eBusiness and financial services, eIDAS, GDPR and personal data protection, Blockchain & DLT, Industry 4.0, Artificial intelligence and Quantum technologies.



Co-financed by the European Union and EFTA



This guide only reflects Small Business Standards' views. The European Union and the EFTA Member States are not responsible for any use that may be made of the information it contains.