



# The Use of Blockchains: Application-Driven Analysis of Applicability

**Bruno Rodrigues, Thomas Bocek, Burkhard Stiller**

Communication Systems Group (CSG), Department of Informatics (IfI), Universität Zürich (UZH),  
Zürich, Switzerland

## Contents

|                                     |     |
|-------------------------------------|-----|
| 1. Introduction                     | 164 |
| 2. Blockchain Application Areas     | 165 |
| 2.1 Why Blockchain?                 | 166 |
| 2.2 Application Areas and Use Cases | 172 |
| 3. Research Directions              | 193 |
| 3.1 Initial Coins Offering          | 193 |
| 3.2 Blockchain Interoperability     | 194 |
| 3.3 Blockchain Governance           | 194 |
| 4. Conclusions                      | 194 |
| References                          | 195 |
| Further Reading                     | 197 |
| About the Authors                   | 197 |

## Abstract

Bitcoin paved the way for a highly successful FinTech (Financial Technology) application on the basis of a newer technology termed blockchain. As this technology has evolved very recently beyond the financial market, gaining more public attention, other promising blockchain applications areas and use cases are emerging. However, it is still not a straightforward in which application areas and use cases blockchains do provide an advantage beyond distributed databases and decentralized systems. Through a decentralized and immutable data storage blockchains enable the enforcement and verification of exchange assets, while disrupting potentially existing business models by promoting the disintermediation of processes involving multiple stakeholders. While having no mediator or a third party controlling the operation, less operational costs and a higher business agility are targeted at. However, the adoption of blockchains requires not only overcoming its technical challenges, but it also implies to reach the ability to

understand and handle the impact on existing business models, processes, and legal compliances. This chapter will overview the main blockchain application areas by providing examples and by discussing from the technical perspective on how and under which conditions the use of blockchains can be useful for a successful use case.



## 1. INTRODUCTION

While blockchains have started with FinTech applications [1], many other application areas, use cases, and specific blockchain types are emerging with the growth of public attention around the blockchain technology. The capacity to provide a trustworthy, decentralized, and publicly available data storage makes blockchains an interesting opportunity for organizations to increase business agility and reduce costs by removing intermediaries in distributed applications (i.e., by involving multiple and initially nontrusted stakeholders). It is precisely the powerful characteristic to disintermediate trust, which arouses interest in the use of blockchains in applications areas beyond FinTech, such as fraud detection, global access or ownership rights, contracting, and identity management [2,3]. It allows, for example, two parties to conduct an exchange upon an agreement without requiring the presence of a third-party acting as the (trusted) intermediary. Also, the ability to run program code managed and executed in a blockchain extends the possibilities for the development of new application areas on the blockchain [4].

Computer programs running within the blockchain are referred to as smart contracts (SCs), which define formal algorithms, following Turing-complete capabilities, comprising the agreements between stakeholders involved [5]. SCs are automatically enforced, verified, and replicated by nodes composing the blockchain to ensure its permanent storage and high obstacles to manipulate the contract's content. As SCs are executed on transaction data received by the blockchain, the contract is automatically enforced and records of this transaction are permanently added to the blockchain. When new blocks of records are appended to the chain, all other nodes are simultaneously updated, and there is no need for third-party intermediaries to verify or transfer ownership of these digital assets. Furthermore, the blockchain is agnostic concerning the type of data, which makes it applicable to a wide range of application areas where disintermediation of trust makes sense.

While short-term expectations of emerging technologies are usually overestimated, ignoring its long-term effects, the blockchain technology

is foreseen as an evolutionary rather than revolutionary technology. The reason is that blockchains offer a radical change for a large variety of industries not only on the technical side but also disrupting existing business models, the operation of processes, and existing legal compliances. Shifting the *modus-operandi* of existing business models affecting its laws and regulations, regardless of its technology requirements, usually takes a longer time to be in place in a political sphere. Thus, it is important not only to combine the knowledge of a specific application area or use case with the blockchain knowledge but also to understand the long-term blockchain impact on existing business models, processes, and compliances specific to an application area to estimate the success of a case.

Foretelling the success of blockchains in a long term is not a straightforward task, in particular when considering that blockchains are still subject to active research and development by governments, industries, and academia. However, it is possible to identify key positive characteristics in its fundamental concepts that may influence a long-term adoption, such as disintermediation and automation that may lead to a reduction of costs. For the successful development of a blockchain-based application, one must also consider negative aspects that may be associated with business paradigm shifts and technical challenges that technology must overcome to establish itself in practice [6]. In this sense, based on blockchain fundamental concepts and characteristics, an analysis of existing application areas and use cases can facilitate the understanding of barriers of this technology's application and guide a successful long-term development and application of blockchain.

This chapter overviews the blockchain application areas providing examples of use cases and discussing how and under which conditions the use of blockchain can be useful for a successful use case. As usual with scientific work, references are utilized to refer to existing work, which, however, does not necessarily always be either complete or proven due to the young development stages of blockchains in general.



## 2. BLOCKCHAIN APPLICATION AREAS

In its purest form, a blockchain acts like a shared, replicated, append-only database where participants can depending on the type of blockchain, share write access, and participate in the validation process. While many blockchains implementations are typically designed to contain financial transactions (e.g., Bitcoin), it can also be designed to contain a general type

of data (e.g., Ethereum). As a result, a complete overview of all application areas and use cases is impossible due to the variety of data that could potentially be stored, verified, and processed including the range of its application areas being as wide and as diverse as human activities themselves [7]. Thus, before investing in a blockchain start-up or using a blockchain product or service, it is extremely relevant to evaluate whether a blockchain application (i.e., use case) makes sense or not to avoid potential losses. Such discussion is conducted in Section 2.1 presenting arguments to guide the decision on whether to adopt blockchain or not and being fundamental to establish parameters to analyze blockchain application areas as well as their use cases.

## 2.1 Why Blockchain?

There is no general formula to determine whether a blockchain makes sense or not without a detailed analysis of the different blockchain properties and types, the requirements and goals of its potential participants, and the particular characteristics of the application itself. Each use case presents its complexity with different properties to be satisfied, and, similarly, each participant involved might have different requirements and goals. This decision-making problem has been discussed in Refs. [3,8] where the authors aim to determine whether a blockchain makes sense or not by defining a methodology or conditions that helps to answer why a blockchain is needed in a case-by-case analysis. For example, in Ref. [3] the authors present a flowchart to guide the decision-making process considering whether it is needed to store data for cases involving one or multiple entities that may not trust, or know each other. It is also considered whether a trusted third party exists and whether public verifiability is required among these entities to decide if a blockchain is necessary. The output of this decision process not only helps to decide if a blockchain is not needed at all but also helps to determine the type of blockchain to be used for a particular application in a positive case.

The authors in Ref. [3] state that a blockchain is not necessary if there is no need to store data or there is only a single entity involved in the use case. However, it is worth to note that even for a single entity that is large enough there might be a lack of trust between its departments or operations in different countries [8], and thus a necessity to validate its operations. Similarly, a blockchain is not recommended if it is possible to trust a third party or all involved parties are known and trusted to each other. For cases where a third party can be trusted, or there is no need at all for disintermediation, a blockchain-based solution might become a stepping-stone

for data confidentiality and performance of transactions. Thus, when parties are known and trusted, a traditional database with shared access is likely to be the most suitable option to address these issues.

Conversely, for all cases that data needs to be stored and multiple entities that do not know to each other are involved, a permissionless (i.e., open and decentralized) blockchain is recommended when it is not possible to trust a central third party. In these cases, goods and services can be exchanged and verified publicly without a central entity managing the membership of these parties. Otherwise, a public-permissioned blockchain is necessary when public verifiability is required, but only some predefined parties can be trusted. For these cases, a central entity manages, the membership of participants, is responsible for granting or denying permissions to a set of participants to read or write in the blockchain. Lastly, a private blockchain is recommended for cases when data is stored by multiple known and trusted parties, and there is no need for public verifiability among them. For example, this type of blockchain could be deployed in a large company that seeks greater transparency and auditability in its internal processes, but do not want to expose these processes to general public.

Similarly, the author of Ref. [8] guides the decision process describing conditions, as in a checklist, that a particular use case or application should fulfill to justify the adoption of blockchains. Five (5) main conditions are described as essential, and three (3) conditions derived from these are described as recommendations. These conditions are [8]:

- i. *Database*: need to store data.
- ii. *Multiple writers*: blockchain is a shared database with multiple writers.
- iii. *Absence of trust*: there needs to be a degree of mistrust between the multiple writers.
- iv. *Disintermediation*: remove intermediaries by enabling databases with multiple nontrusting writers to be modified directly.
- v. *Transaction interaction*: transactions created by different writers often depend on one other. For example, in transference of funds, allowing one to use the new funds.

Three (3) conditions derived from these are described as recommendations. These conditions are [8]:

- i. *Set the rules*: the database should contain embedded rules restricting the transactions as the data recorded in the blockchain is not always reliable. Therefore, it is necessary to carefully design and control the order of data transfer to records in the blockchain.

**ii.** *Pick validators*: refers to the choice of trustable miners and the consensus protocol defined in the blockchain.

**iii.** *Back assets*: translation of nontangible assets to real-world assets.

As the authors in Ref. [3], the first two conditions described in Ref. [8] are straightforward concerning the need of a shared database, expressing, in the first place, the need to have a database (i) involving multiple writers (ii). Blockchains are, in principle, a shared structured repository of information and thus, there is a need to store data and have more than one party including information in this structure. However, there is the fact that most parties may not be known or trusted among themselves, which is described in the by their following condition. The capacity to provide trustworthy environment among nontrusted parties (iii) is one of the major blockchain characteristics, and cases involving one or multiple parties that requires a certain degree of trust, or do not trust each other at all, are essential to justify the adoption of the blockchain.

A blockchain application not only can provide trust over multiple nontrusted parties, but it also provides disintermediation (iv) enabling data to be directly shared across boundaries of trust in case there is no need for or absence of trust in the central third party. For cases which a central authority is not required to validate transactions between one or more parties, transactions can be independently verified and processed by every node with the blockchain acting as a consensus mechanism to ensure these nodes are synchronized. However, removing an intermediary might present drawbacks regarding performance and data confidentiality, and the adoption decision is a critical factor to the success of a use case. Some organizations have earned their trust over the years, and for use cases where confidentiality or performances are key factors, a trusted third party is naturally the best choice.

The next key condition described in Ref. [8] is the transaction interaction (v), which is similar to the public verifiability described in Ref. [3]. The author state that the true value of blockchain rises when there are interactions between transactions created by multiple writers and these transactions depend on each other. For example, in a supply chain process involving multiple stakeholders, a final party can only deliver goods or services when all transactions in the supply chain were submitted and validated, or a simple transference of funds between two parties, allowing one of these parties to use the new funds. This means that transactions submitted by nontrusted parties can be validated without exposing themselves to risk, allowing the delivery vs payment settlement to be safely performed over the blockchain without a trusted intermediary. While transaction interaction is similar to

public verifiability, the author in Ref. [8] describes this condition as fundamental toward the blockchain adoption in a use case and authors of Ref. [3] state this requirement as a conditional to decide between public, in case verifiability is required, and private-permissioned blockchains otherwise.

The last conditions are derived from the previous ones and seen as recommendations rather than mandatory for the blockchain adoption. Thus, according to the authors in Ref. [8] when a use case fulfills the previous conditions is necessary to set the rules, select the validators, and back the assets in the blockchain. Set the rules is a consequence of the previous five conditions that are related to embedding rules restricting the transactions in the blockchain. These rules are fundamentally the logic behind the use case being typically described using SCs in a blockchain application. Next, is necessary to select the validators, which refers to the choice of miners and the consensus protocol defined in the blockchain to avoid conflict between transactions and thus multiple chains, transaction censorship, and biased conflict resolution. The choice of the consensus protocol is closely related to the needs of a particular use case and the involved parties, whether it requires transparency and disintermediation, or privacy and performance, among other requirements. Lastly, back the assets (viii) is related to the translation of a nontangible asset to a real world, physical asset, e.g., what is the ballast of some virtual tokens defined in a blockchain converted into some assets in the real world. This concern stems from the nature of the blockchain environment typically composed by multiple nontrusted parties that may attempt to create digital assets to obtain physical assets maliciously.

As mentioned earlier, there is no general formula to determine whether a blockchain solution makes sense or not for a particular use case. However, based on Refs. [3,8] it is possible to draw essential characteristics that a use case should fulfill to decide whether to adopt blockchain and make efficient use of blockchains. Furthermore, application requirements such as transparency, confidentiality, performance, fault tolerance, and disintermediation should be seriously accounted onto such decision. Thus, main requirements to adopt a blockchain, regardless of defining its characteristics, are summarized herein as follows:

- *Database*: first and foremost, to adopt a blockchain solution should exist the need to store data in a structured fashion.
- *Multiple writers*: may or not involve multiple parties, but should include multiple writers that may not know or trust each other.
- *Disintermediation*: required when a trusted third party is not available, or it is not needed nor desired for a particular use case.

- *Sequential transactions*: condition for uses cases where the order of transactions impacts further transactions, i.e., data is sequentially concatenated. The transaction model can be either UTXO (unspent transaction output) or SC based. Whereas the former is used in Bitcoin [1] and suited for the transfer and tracking of assets, the latter is used in Ethereum [4], and arbitrary logic can be defined, executed, and verified.

It is mandatory that these conditions should be fulfilled (i.e., a use case should need these characteristics) to answer if a blockchain solution is ideal or not for a particular use case. If one or more conditions are not satisfied, then another type of data storage structure should be considered. However, this is just an indicator that blockchain can be a good solution to the use case, case all conditions mentioned earlier are satisfied, it is also necessary to discuss the use case requirements and the trade-offs between them. These requirements are summarized as follows:

- *Performance*: blockchains are naturally slower than any centralized database. Besides of the regular operations performed in a traditional database, a blockchain should perform extra procedures to ensure that transactions are correctly recognized, propagated, and verified. Also, traditional databases have been deployed, tested, and optimized through decades of development.
- *Distributed or centralized control*: it is closely related to the disintermediation blockchain characteristic. The question to be answered is whether the use case requires to be centrally managed or not. The core value of blockchain stems from its power of disintermediation, ensuring that nontrustable parties be able to interact in a trustworthy environment.
- *Privacy and confidentiality*: users and data in a blockchain are visible to all nodes (with reading permission) participant in the blockchain. For use cases where a user and data transparency are desired, blockchain is the choice to verify and process every transaction transparently independently. However, if privacy and confidentiality are required, and there is a trusted third party, a blockchain poses no advantage over a centralized database. However, it is still possible to hide confidential information on a blockchain, but hiding critical information requires lots of cryptographic efforts for the nodes in the network.
- *Robustness or reliability*: it is related to the dependability of the database. Blockchains are typically fault tolerant due to its built-in redundancy, which means that transactions are replicated within the blockchain network and permanently recorded. Some trusted third parties can also provide fault tolerance offering replication techniques, but blockchains can provide high redundancy by default.

Not only these use case requirements should be evaluated solely by its own to decide which type of database is necessary, but also the trade-offs between them. For example, as mentioned in Ref. [8], if disintermediation and robustness are more important than performance and confidentiality, then a blockchain-based solution seems to be the natural choice for the use case. Alternatively, if performance and confidentiality are required then other types of data storage such as a centralized database or a distributed master-slave replication structure might be more adequate.

Although confidentiality is typically the most relevant criteria and despite some attempts to provide privacy in blockchains (e.g., zero-knowledge proofs, side channels, and encryption), blockchains are not meant to store sensitive information, and thus off-chain centralized solutions can be combined with the blockchain network to fill this gap. Furthermore, any combination of these requirements is valid and should be carefully considered. For instance, taking requirements which are not always on the same side of the road in a single storage solution, such as performance and robustness or confidentiality and distributed control, it may not be straightforward to determine which whether a blockchain is necessary. Thus, in these cases is not only essential to observe the use case requirements to decide whether to use blockchain but also to check whether the use case complies with the blockchain characteristics.

Also, answering these trade-offs is helpful to guide the decision on which type of blockchain to deploy, in addition to the steps discussed in Refs. [3,8]. A permissionless blockchain is a fully decentralized approach removing any intermediary certifying transactions between parties, and it is a determinant factor is when the participants are not known or trusted to each other. Possible downsides for use cases implemented in a permissionless blockchain are performance and confidentiality once all data in the chain is open and publicly verifiable, and it requires a consensus mechanism to maintain the chain order. When participants are known but not trusted, write permissions may be distributed according to trust criteria in a public-permissioned blockchain (i.e., consortium) and data within the chain could be verified by all members. The difference between a public and a private-permissioned blockchain is that read and write permissions are managed centralized, avoiding public readability and increasing the blockchain confidentiality. However, it is commonly argued [9] if a private-permissioned blockchain is merely a traditional centralized system with a degree of cryptographic auditability attached with no reasons to belief that cryptographic authentication based on hash-chained blocks containing Merkle tree roots is an optimal format of audibility. Also, it does not prevent single (large)

entities managing read and write permissions to perform fraudulent actions on the data by freely changing rules.

In summary, it is not only difficult to determine whether a blockchain infrastructure is necessary or not but also and in case it is needed, which type of blockchain to be deployed. A decision should be based on the features offered by each type of blockchain (and conceptual differences among traditional databases schemes and blockchain), and application requirements and its trade-offs.

## 2.2 Application Areas and Use Cases

Blockchain moves the control of daily interactions from centralized entities, redistributing it among users in a decentralized and transparent way. The ability to remove intermediaries creating a secure bridge between two parties is a factor that modifies how some use cases are currently made. However, the ability to operate over any data makes that extends its application areas making it as diverse as the human activities themselves—as long as some conditions were observed to ensure its necessity and efficiency. Still, one of the most useful ways to understand and determine whether blockchains are been able to improve the efficiency of a use case is observing its successful application areas and use cases. Therefore, this section presents selected blockchain application areas and use cases, analyzing the reasons for and against the use of blockchain in these areas.

### 2.2.1 Supply Chain

Goods all over the world are produced and distributed across a vast network of producers, retailers, distributors, transporters, and vendors in a complex arrangement of processes. The availability of standardization and certification bodies has done a remarkable work improving the producers quality and consumers awareness, but actual processes remain costly and unreliable, especially in regions with high levels of corruption, as reported in Ref. [10]. Blockchains counter these shortcomings providing:

- *Transparency*: every asset inserted in the blockchain can be tracked and traced by all participants of the supply chain.
- *Trust*: since the whole system is running transparently and every transaction is signed and traced back to its owner, it is easier to check malicious behaviors. Also, there is no need to trust a third party which could manipulate the data.

- *Interoperability*: single, transparent, and trusted source of data that is shared between different systems in the supply chain. Therefore, instead of many systems individually managing databases, the visibility of data is limited.
- *Reduced costs*: costs associated with all kinds of manual paperwork, legal documentation processing, duplicate entries, and mismatches can be reduced with digital processes.

While costs can be reduced by removing intermediaries and costs associated with legal documentation processing, risks can be eliminated by the inherent data transparency and the use of cryptographic primitives to ensure ownership of each step registered in the supply chain ecosystem. For example, when something goes wrong within a vehicle or aircraft that are systems composed of various subsystems, it is important to know the origin of each subsystem to collect details like manufacturer, production date, how it was transported, and other relevant pieces of information. Thus, it is essential not only that information is available to all participants, but also that no central authority owns the data of multiple steps in the supply chain, so as its origin can be tracked to a single entity.

The author of Ref. [11] states that the scale and complexity of the involved systems often lead to high transactional costs, mismatches, and errors in manual paperwork. Thus, digitalizing information and making it available to all members of the supply chain can optimize the time-to-market of products and increasing end-to-end transparency. Therefore, with a blockchain-based solution reducing the amount manual paperwork, which is more prone to error than digital documents, everyone has access to the same, up-to-date information. Furthermore, blockchain can be used not only for registering, certifying, and tracking goods but also to trigger automatic payment systems and other procedures through SCs. However, as detailed in Ref. [12], as the entire process typically involves many entities with different organizational processes, well-designed interfaces and data-models should be defined to enable this transfer of information to occur smoothly.

Although reduced time to market is a common objective, performance requirements are not as relevant as other features like transparency, trust. It is not important whether a supplier is fast if the goods are not registered or delivered correctly. Thus, a reliable and transparent supplier is more important to a wholesaler than a fast one. Also, while disintermediation is naturally obtained by deploying a blockchain solution, transparency is achieved by defining a public or private-permissioned blockchain, depending on the

use case. For example, reading permissions of internal steps of a supply chain may not be exposed to general public (e.g., industrial confidentiality), but only to its internal members to increase the overall process efficiency. Similarly, writing permissions shall be given only to those who take part in the system.

Notable use cases stem from the logistics sector, responsible for the transport of goods both overseas and land. For example, IBM and Maersk [13] announced in 2017 the creation of a network of shippers, freight forwarders, ocean carriers, ports, and customs authorities. The goal is to reduce the costs associated with paper-based trade documentation processing and administration, which are estimated to be up to one-fifth the actual physical transportation costs. In 2014, Maersk found that just a simple shipment of refrigerated goods from East Africa to Europe can go through nearly 30 people and organizations, including several interactions and communications, as reported in Ref. [13]. The solution, based on the IBM Hyperledger blockchain, is intended to enable real-time exchange of events (e.g., when a good is shipped or received) and documents (e.g., trade reports) reducing errors and delays in the process. For authorities, it will also provide traceability as goods advance and enters in countries for border inspection as the solution can give real-time visibility, significantly improving the information available for risk analysis and targeting, eventually leading to increased safety and security as well as greater efficiency.

Other relevant use cases appear in the food supply chain, which had seen a big change over the years with the fast increase of population in urban areas, with more than half of the world's population living in these areas [14]. As a result of the need to provide more food in a decreasing time, more cases of fraud appear through the entire food chain, being not enough to avoid fraud even if each country has an organization body defining minimal sanitary conditions for production, transport, storage, and sales of food. These cases directly affect not only the health of consumers, but it also creates economical and trusts losses throughout the entire supply chain. Among the main requirements to avoid frauds in the food sector are [14]: (i) traceability of food producers and transporters; (ii) transparency to track and trace the parties involved in the supply of fragmented foods (e.g., hamburger); and (iii) trust among entities. Also, even if a blockchain-based solution does not solve all fraudulent actions in the sector, it does comply with these main requirements.

An example comes from Switzerland focused on the agricultural sector, whereas the Swiss Federal Constitution provides incentives in the form of

subsidies to encourage farmers whose productions comply with environmental and animal-friendly regulations. Based on this, the University of Zurich developed a blockchain-based system to demonstrate how such system can increase transparency and automate interactions in the agricultural sector [15]. Once a farmer creates a new request for *Direktzahlungen* (subsidy paid by the government), the farm has to be inspected and periodically checked. Then, a SC is deployed to the blockchain containing all relevant information such as the type of animal and their living conditions to calculate the subsidy amount. These conditions are verified by government agents during inspection visits on the farms. Then, the payout is accomplished through a transfer of ERC20<sup>a</sup> tokens to the farmers. However, the downside of the system requires an exchange platform which guarantees that farmers can exchange their tokens into real currency.

Another use case appears in the pharmaceutical supply chain with the transport of medicinal products for human use. The new European Union regulation for distribution of medicinal products, GDP 2013/C 343/01 [16], states that it is an obligation to report any deviation on the transport (such as temperature and humidity) as well as to monitor parcels at all times, to the distributor and the reception of these products. In this regard, a modum.io AG developed a blockchain-based solution combined with IoTs (Internet of Things) sensors to monitor all necessary data during transport [2]. From a business perspective, blockchain allows reducing the number of intermediaries and SCs can ensure compliance with GDP regulations verifying data collected by IoT sensors during transport.

From a practical point of view, valuable lessons were presented in Ref. [2], which are summarized as:

- *Connectivity*: most warehouses have poor or no Internet connectivity which has an impact on the design of sensors (to store data offline) and to create SCs to register a new shipment.
- *Simplicity*: a key in all aspects of the system design because, in most cases, the solution will replace manual paper-based documentation, and workers do not have the technical knowledge to operate devices and digital processes. The use of blockchain has to be as transparent as possible to a system user.

In a nutshell, blockchain has the potential to be game changing in the supply chain sector for several reasons that ranges from the digitalization and automation of process to the increase of trust in its members.

---

<sup>a</sup> ERC20 standard: [https://theethereum.wiki/w/index.php/ERC20\\_Token\\_Standard](https://theethereum.wiki/w/index.php/ERC20_Token_Standard).

However, even if data transparency in every step of the supply chain is a desired feature, this information should not be publicly accessible due to some industrial reasons. Thus, reading and writing permissions should be carefully managed in a permissioned type of blockchain. Also, as discussed in Ref. [2], many places and workers are still not ready for digitalization of processes, with many warehouses with poor or without connectivity and workers without knowledge to operate these processes. Lastly, it is important to consider that humans are the source of information and, as an immutable database, erroneous entries in the chain will be a source of inconvenience for the other participants.

### **2.2.2 Health Care Industry**

Not only the supply chain is a difficult task for the health care industry, but it is an extremely complex system on its own. In 2015, the Office of the National Coordinator for Health Information Technology (ONC) published the Shared Nationwide Interoperability Roadmap [17], defining a path to improve interoperability for the next 10 years. Besides of recognizing that many advances were made in precision medicine, telehealth (the use of telecommunications and virtual technology to deliver health care outside of traditional facilities), and adoption of electronic health records and big data analytics, there is still progress to be made. The ONC established a roadmap to improve interoperability between different sectors and entities of the industry, which includes standards for identity, authorization and access data formats, data transmission, longitudinal health information, and provider workflows.

The industry has multiple interconnected entities which not always act in predictable ways to deliver health care services to patients. Actions and duties of these entities are regulated by governments and standardization bodies, such as the ONC, to ensure that effective patient care becomes the focus of health care delivery. However, due to the complexity of the sector, some key challenges are found [17,18]: (i) number of fragmented data maintained individually by these entities; (ii) patient data security; (iii) system interoperability; (iv) cost and time effectiveness. Blockchain can help to overcome most, if not all these challenges, depending on the use case-specific requirements. Also, existing health care systems do not need to be completely rebuilt to use a blockchain solution, being necessary only the way how these systems interact. The main benefits of blockchain in the sector are:

- *Transparency*: in general, the way how data is shared across the health care network is extremely important and using blockchain, it can eliminate

duplicate entries, errors, and fragmented data that can happen in an individually managed database.

- *Trust*: this single view on shared medical records and increase trust and interoperability among these systems. However, it should be noted that patient records cannot be fully exchanged or exposed in the blockchain and, therefore, read and write permissions need to be carefully managed. SCs could create an efficient method for accessing and analyzing patient records that can be permissioned to selected entities. In the end, by reducing inconsistency, transaction costs, eliminating third-party applications, and providing a single view of patient data selectively shared across the chain, can increase the cost-effectiveness in the health care industry. Several initiatives in and between the private and public sectors have been undertaken to develop blockchain-based solutions for the health care industry. One use case is MedRec [19], a project between MIT Media Lab and Beth Israel Deaconess Medical Center. The use of blockchain in this scenario is intended to give patients the ability to decide who can access their health care data and use these permissions to create an automated approach to data sharing for clinical and research use. The solution itself does not store patients' health records, it stores the record's signature (i.e., a hash of the data) on a blockchain, and this signature may assure that data's unaltered copy is obtained.

While the permissions, data storage location, and audit logs are maintained in the blockchain, all health care information remains in health records systems and requires additional software components to enable interoperability [18]. The project has been tested as a concept prototype with medication data, and the developers are looking to enhance the project's scope by adding more data types, data contributors, and users. As shown by this proof of concept, biomedical and outcomes research may significantly benefit from the application of blockchain to provide fast, secure access to research data.

A second use case was developed by Guardtime [20], a data security company that uses blockchain technology to promote public and private data security, which in partnership with the government of Estonia, created a blockchain-based framework to validate patient health records. All citizens have issued a smart card, which links their health records with their blockchain-based identity. Therefore, all updates in these health records are seen as a regular transaction with an assigned hash and registered in the blockchain framework. This approach ensures that data within the health records contains an immutable audit trail and that records cannot be maliciously modified. For example, in an appointment scheduling, it is assigned

a time stamp and cryptographically signed in a block and these records could be verifiable using the blockchain guaranteeing system, process, and operational integrity.

The health care industry is a complex sector with several interconnected entities maintaining similar records of patient data in individually managed databases. Besides of the lack of interoperability, this creates a high-level fragmentation and mismatches between of patient data. Blockchain can significantly simplify interoperability among these entities as long as patients provide permission of its data to be shared, as shown in MedRec [19]. However, efforts from standardization bodies and perhaps, government's incentives, are also required to create a common data model and APIs so as the different systems from these entities can interact over the blockchain (a concern also outlined by ONC in its roadmap for interoperability [17]). In this regard, the government of Estonia gave the first step toward the blockchain adoption [20], creating a nationwide system integrating data from Estonia's different health care providers to create a common record that every patient can access online.

It is important to note, however, that interoperability cannot be solely achieved only through a blockchain solution where all entities share data. Even if transparency is a desired feature to avoid fragmented data, there are different companies competing in similar areas (e.g., multiple health insurance companies) which may not wish to store information in a blockchain where competitors may read. Therefore, confidentiality is one of the main requirements that have to be addressed not only to secure private patient data but also to protect information that could provide a competitive advantage. An alternative in this sense is that companies could share a hash of data in the blockchain, and this hash could be verified only by an authorized entity (e.g., government or patient), but not to other competitors. Ultimately, the future will tell if all or only parts of that blockchain technically available characteristics and advantages can be practically exploited in the health care industry.

### **2.2.3 Internet of Things**

IoT is an interconnected network of devices ranging from small sensors and actuators to vehicles and other large appliances, stationary or portable, that can automatically transfer data without requiring human intervention [21]. In this regard, these devices can be deployed as an enabler in a broad range of blockchain-based use cases, such as smart vehicles, tracking temperature during transport of medicinal [2] or food shipments [15], or sense patient data [19]. As detailed in Ref. [22], both manufacturers and

customers can benefit from this combination. Manufacturers can reduce their maintenance costs by, for example, deploying a public-permissioned blockchain network of its devices to identify and maintain devices. Thus, whenever a new system update is released, identified devices can retrieve, from a predefined SC address, a hash-based link and download the update.

The SC can use, for instance, a distributed file system, such as IPFS<sup>b</sup> to distribute these binaries over the network and, instead of using a central system to perform updates on several devices, these binaries can be spread over the network automating and optimizing system's update tasks. From a customer perspective, it is also important to have devices registered in the blockchain. It means that messages signed by registered devices can have its authenticity confirmed, and these devices can interact through SC functions which then model the agreement between the parties. Therefore, not only a trustworthy device-to-device model can operate transparently but also in an autonomous way without a central authority.

The blockchain also provides a financial layer that can be used to create a marketplace of services between devices, as outlined in Ref. [22]. For example, a smart fridge could sense its interior and automatically reorder new items whenever required. Also, in the case above where devices can serve a copy of binaries for system updates, storage space, and API calls can be monetized to sustain infrastructure costs (e.g., storage, bandwidth). Therefore, every device or group of devices behind a sink can use cryptocurrencies accounts to expose its resources to other devices or users in an "as-a-service" basis and get a financial reward for it. All these interactions can happen automatically, without human intervention.

As IoT devices can be used to sense, store, and process data in many different environments, combining blockchain and IoT creates a vast possibilities of use cases. The combination IoT and blockchain can provide the following benefits:

- *Automation*: blockchain and SCs help to optimize and automate business processes through IoT.
- *Marketplace*: blockchain facilitates the sharing of services and resources leading to the creation of a marketplace of services between devices.
- *Trust and transparency*: greater levels of trust and transparency are provided by blockchains. While devices can automatically sense and process data for a particular use case, blockchains and SCs can provide a transparent and verifiable communication.

---

<sup>b</sup> IPFS: <https://ipfs.io>.

However, as there are different types of blockchains and devices, it is necessary to observe which combination of blockchain and devices is better suited to a use case. For cases where a public blockchain (and proof-of-work based) is required, the following challenges need to be addressed [21]:

- *Resources restriction*: mining is expensive, and the majority of devices is resource constrained.
- *Performance*: mining blocks consume time, while for most cases, low latency is desired.
- *Scalability*: blockchain scales poorly as the network size increases.
- *Security*: blockchain can create significant overhead traffic, which may be undesired for most constrained devices. Additionally, reaching confidentiality is extremely difficult since the content of every transaction is exposed to every blockchain node and methods to that allows confidential transactions (e.g., zero-knowledge proof, homomorphic encryption) are resource intensive and thus, not applicable to resource-constrained devices.

In private networks where participants are known but not trusted, a permissioned blockchain can be used with other protocols to reach a consensus which requires fewer CPU computations. This would reduce or eliminate the need for powerful devices, but privacy (i.e., identifying a device) and confidentiality (i.e., identifying the data) would still not be straightforward to be reached. However, it is worth to note that despite these considerations, the combination of blockchain technology and IoT devices can be very powerful to automate time-consuming tasks in a trustworthy and verifiable manner, and potentially creating a new ecosystem where devices can seamlessly communicate with each other and offer services.

Ultimately, blockchain and IoT are part of a revolution that modifies how platforms are currently defined and used, passing from technical infrastructure to an ecosystem enabler, and creating the foundation for new business models. Therefore, entities within this ecosystem should not only be aware of the technical challenges of this combination but also to redefine their business strategies to build cost-efficient solutions that take into account autonomy and privacy. On a business level, it is needed to redesign processes and agreements around traditional definitions of data and to define legal responsibilities and actions.

#### **2.2.4 Identity Management**

Digital identity is a growing issue on the Internet not only due to an increasing number of users and devices but also because of the user complexity to

create, use, store, and verify these identities in many services fragmented across traditional centralized databases. This results in insecure systems where people often use the same combination of username and password for many services [23]. Also, the security of these identities is just as strong as the security of the database where they are stored, which makes large identity providers like Google and Facebook a valuable target for hackers to attempt to crack. Also, information taken from this large pool of identities can be a valuable source of information for market-oriented publicity.

Blockchain-based identity systems reduce this risk by decentralizing the ownership of data and bringing the responsibility of managing identities back to the user. Thus, in addition to the password security being the sole responsibility of the user, it becomes less economically valuable for hackers to crack many individual identities one by one. Also, the use of SCs may include sophisticated logic that helps with key verification, revocation, and recovery, lessening the key management burden for the end user. In summary, three main benefits could be observed in a blockchain-based identity service [23,24]:

- *Data ownership*: being the digital identity a reflection of a real physical person, the attributes of identity, or group of identities becomes valuable information for market-oriented publicity. In a blockchain-based identity, the information is decentralized, and users are the owners of their data being able to monetize according to its will.
- *Reduced risk of data breach*: well-established public–private key pair schemes (e.g., Elliptic Curve Digital Signature Algorithm—ECDSA) are commonly used to represent identities. Also, it becomes difficult for hackers to steal a large number of identities on a peer-to-peer basis.
- *Immutability and transparency*: blockchain algorithms and SCs are open and transparent, being independent of a single entity to manage and update. Moreover, it enables quick auditing of identities through the immutable chain.

However, besides these positive characteristics, it is necessary to evaluate the requirements of each use case since the identity service can, in most cases, provide access to a critical service to the user (e.g., online banking). Also, as pointed by the author in Ref. [25], some aspects are not favorable of the blockchain adoption:

- *Immutability myth*: while most authors state that blockchain is immutable, others say that data immutability is not a guaranteed condition. The immutability discussion refers to the 51% attack, where an actor, which controls 51% or more of the mining power of the network, would have

enough economic power to reach more mining capacity than the remainder of the network and to subvert the network. Therefore, immutability is based on the assumption that is economically difficult to undermine the network, but for some entities (e.g., governments), this cost is still not high enough.

- *Lack of trust*: related with the lack of confidence (which, in its turn, is associated with immutability myth) and knowledge of individuals and companies in new technology and the absence of a legal framework to control liability are aspects that affect the trust in blockchain-based identities.
- *Synthetic identity and identity verification*: while synthetic identity is related to creating real and unique identities, the verification involves checking whether the user claiming an identity is a rightful owner.

Despite the author in Ref. [25] describes synthetic identity and identity verification as blockchain-related issues, these issues are not only related to blockchains but to all digital identity services. Similarly, the author describes a demographic issue, which is related to the problem of issuing strong digital credentials at scale for different groups of people. However, these aspects are related to the design decisions and how an application layer, that uses the blockchain as a storage back end, is implemented and not the blockchain itself. In this regard, many companies are investing in blockchain-based solutions to authenticate their users. Blockstack [26], for example, provides identities, naming, storage, and authentication services for decentralized apps using the Bitcoin blockchain as a back end to secure identity data [1]. The solution is built following three main principles: (i) decentralized naming and discovery service where users register and discover resources in a human-readable way; (ii) decentralized storage where users place their identity without revealing to the third party; and (iii) performance comparable to a traditional centralized service.

Blockstack contains a network of nodes with the global registry of identities, public keys, and other metadata, and operations are represented in the Bitcoin blockchain to provide a name registration service binding public keys to their names. These names are resolved into a new DNS (domain name system) built on top of the Bitcoin layer and every time a Blockstack node joins the Bitcoin network, it can synchronize its registry via the Bitcoin blockchain. For data storage, a DHT (distributed hash table) is used to store key-value pairs, where the integrity of the values can be verified in the Bitcoin blockchain. The solution not only simplifies the maintenance of

the keys using a DNS service but also decentralizes the identities using the Bitcoin blockchain as back end.

Another blockchain-based digital identity is VALID [24], which based on a new European privacy regulation called the General Data Protection Regulation (GDPR), aims to connect people as physical identity owners with data consumers, such as product and service providers, brands, researchers, and advertisers [24]. The goal of VALID is to let the users be responsible for their data by granting permissions or monetizing their data through a marketplace. Thus, the company offers a platform consisting of a mobile wallet and a web application for users to manage their data and permissions, and a blockchain-based marketplace for consumers to buy and access consumer's data. Then, agreements between consumers and users are defined via SCs in the marketplace back end.

The company provides an example of how to take advantage of a new regulatory incentive to combine with new technology. Blockchains are used as a platform to record the trade of user data, where the user may sell the use of its data based on SCs, and to store a user data. Thus, a public-permissioned blockchain is combined with a permissionless blockchain, to tracking user data modifications of the former and recording these changes on the latter. Therefore, the permissionless blockchain acts as a notary for data modifications by checking whether and when they occurred. Ultimately, when users are the sole owners of their data on purchases, online browsing history, or mobile data, they can choose whether or not to monetize their data.

There is no doubt that Blockchain has a fundamental impact on existing digital identity methods, bringing back to the user the ownership and of digital identities data by centralized entities. However, some aspects need to be considered before adopting a blockchain-based identity service. The use of new technology based on cryptographic primitives may be less unintuitive for most people, impacting the adoption of blockchain-based services. Also, the performance is a restricting factor and, as in any fully distributed network, it is hard to tell which nodes contain what information, so the search has to go through the whole network to find specific data. Also, the more nodes are added to the network; the more difficult the information lookup becomes because it is unclear which nodes contain what information.

### **2.2.5 Government Services**

Governments strive to be as open, transparent, and collaborative as possible, creating projects and actions that aim to promote transparency, fight against

corruption, and increase social participation through the development of new technologies. A significant advantage for blockchains in public services stems from the disintermediation, which uses the decentralization of information as a safety measure to increase transparency and avoid frauds. Thus, information about finances, people, real estate, certificates, and other documents can be not only virtually unchanged once stored on the blockchain but also transparent and accessible to everyone. Also, blockchains can be used as a governmental platform to increase interoperability between the different governmental bodies, for example, reducing the risk of fraud or irregularities in the payment of social benefits.

The most prominent example of an open and transparent digitalized government stems from Estonia, which is a pioneer country in the adoption of new technologies by both the market and the government. The “e-Estonia” movement reflects a trend of modernization and adoption of technology by the Estonian government since the early 1990s, and in the last years, Estonia has offered a wide range of blockchain-based services, being the most famous the e-Residency [27]. Created in 2014, the system allows the creation of a unique digital identity that gives them access to various Estonian public services, including the e-Health service [20]. For example, Estonian citizens can log into their e-Health service using their e-Residency identity, which is verified in the blockchain, and then check their medical records and which medical professionals have done the same and when.

However, it is important to understand how these public services are connected with the blockchain to obtain its benefits fully. In Ref. [28], the author describes how the Estonian services are implemented and connected to the blockchain. The blockchain uses the Keyless Signature Infrastructure (KSI) from Guardtime [20], which generates and maintains the blockchain containing the distributed ledger. The KSI blockchain has been integrated into key government registries, such as the e-Residency, and other services, such as business registry, property registry, and official announcements, being are used for both internal and external processes to provide a signature service [28]. Also, it ensures the integrity of data enabling the efficient detection of both intentional and unintentional modifications of data because records and associated metadata are chained to previous records. Therefore, when the customer transmits the asset’s hash (e.g., the hash of medical document), a token is received in return, which proves the existence of the document.

The system interacting with the blockchain is named X-Road. It acts as an interoperability platform connecting different governmental institutions to multiple databases. Thus, the role of the KSI blockchain in the Estonian

government is to ensure the integrity of data recorded in the X-Road by providing a chronological proof-of-existence mechanism, which ensures the detection of changes in these registries [28]. Also, it enables an audit log (or transaction log) containing entries such as a time stamp, user login information, and accessed and modified resources are written to the KSI blockchain together with the hashes of the database records. As only hashes are stored in the KSI blockchain, there is a preservation of citizen's privacy, and it enables the transparent auditability and makes records impossible to delete without detection.

Another promising use case for blockchains in government services is electronic voting. In many countries, votes are manually cast, stored, counted, and verified by a central authority. This process is prone to error due to the manual verification of votes, and there are no reliable ways of auditing a completed election because it is done via a central authority. A blockchain-based voting would empower voters to do these tasks themselves, by allowing them to hold a copy of the voting record and recount votes if required [29]. However, there is the challenge to solve regarding the secrecy of the vote, which is related to the coercion of voters [3]. Thus, it is necessary to inhibit voter coercion procedures by third parties and the marketing of votes. In this case, pseudoanonymity is often considered a crucial requirement in the voting process, meaning that it should not be possible to track and prove the relationship between voter and his vote. Also, the nodes in a blockchain-based voting system should be connected to each other being susceptible to cyber security issues and threats.

In general, the use of blockchain in public services and governmental affairs offers many benefits. From a technical perspective, it enables simple and transparent methods to efficiently audit public services, and also as an interoperability platform. The main benefits of blockchains in government services are:

- *Transparency*: it is a key requirement for democratic governments and also a fundamental characteristic of the blockchain. Every data stored in the network is replicated to all nodes that take part of it, making the data or a hash (i.e., a pointer linking to the data as a proof of existence) of it, being transparent to the public.
- *Interoperability*: once different governmental systems maintain a single view on given information (e.g., financial expenses report of deputies), it can be automatically accounted on different systems without duplicates.
- *Auditability*: once data is stored, it provides a permanent record that serves as a constant auditable trail to the population.

However, there are many challenges to be solved. While transparency is desired for many public services (e.g., public expenses), it is still needed to maintain privacy in services provided to citizens (e.g., health care, identities, vote). While blockchain technology can preserve the integrity and confidentiality of records using cryptographic methods, as shown in the Estonian use cases, it is also necessary to understand the security guarantees provided by the overall system, which include the integration between blockchain and other centralized systems. Also, to fully take advantage of all blockchains benefits, it is not only necessary to understand the deployment model (i.e., public or private permissioned) verifying which entities and how decentralized are the nodes responsible for the network, but also the security of the centralized bodies which insert data in the blockchain. Although there is still the possibility of manipulation or errors on the input of the data, it is important to highlight that technology is, in general, an excellent tool for improving the transparency and interoperability of public services.

### **2.2.6 Computer Science**

Many computer science applications can benefit from the decentralization leveraged by blockchains. Besides the IoT-based applications, other cases can be seen in literature taking advantage of the blockchain capabilities. For example, in the context of a distributed denial-of-service (DDoS) defense, blockchain could be used as a platform to exchange mitigation services in a cooperative network defense (i.e., service providers cooperating toward a global network defense). A cooperative network defense has many benefits, for instance, by utilizing other organization's resources the burden of the protection can be shared, and defense capabilities can be extended through the different protection systems participating in the distributed defense. Thus, blockchain would serve as an immutable platform for the exchange of mitigation services expressed in SCs.

The Blockchain Signaling System (BloSS) [4] is one example that leverages blockchain capabilities to define individual agreements or conditions in a SC to perform a mitigation service in a cooperative network defense. Conditions service are described in an individual SC which expresses the networks managed by a peer and the conditions (e.g., cost to operate the infrastructure) to perform a mitigation service. In a mitigation request, service and validation time-outs are agreed between the peers to establish deadlines for mitigation service completion and the payout of the reward (cost) upon the submission of a mitigation proof.

In BloSS, SCs and decentralized applications are the main components. While SCs describe how information is exchanged among autonomous system (AS), the applications contain the parameters that define how an AS interacts with a network management system. An AS creates a blockchain account (wallet) and notifies a central contract that holds information on IP networks being operated by each AS, the address of their wallet, and the address of their contract. Operating IP networks and the token price could be modified in the central contract. Individual SCs implement a method to retrieve addresses reported by others ASes and to be aware of addresses of other domains, ASes can query the central SC to maintain a local lookup table. With the knowledge of IP networks maintained and, possibly, the token prices of other participants, ASes may request protection submitting a transaction to their SC with a list of IP addresses. Subsequently, requested ASes may accept or deny requests based on their security policies or service level agreements.

In this case, blockchain becomes a useful tool not only to propagate attack information, replacing existing gossip-based protocols but also a tool that allows the exchange of information (e.g., cryptocurrencies) for the enforcement of mitigation services. However, there may be restrictions on the confidentiality of the disclosed data since attacks information can have an economic impact on service providers. This makes it necessary to have a permissioned blockchain, restricting permissions to read and write through a consortium responsible for managing the cooperative defense.

Blockchain can be used as a means of protecting many Internet services typically provided in centralized systems, such as DNS (domain name system). Traditional DNS is vulnerable to a variety of attacks due to protocol flaws and the centralized nature, which is usually target of DDoS attacks. For example, DNS records can be distributed across the blockchain network avoiding the single point of failure and increasing the difficulty of potential attackers to make it unavailable. For example, the identity service Blockstack [26] uses a naming system (termed blockchain name system) operating across different blockchains. As it is built on top of the Bitcoin [1], which cannot store large data such as name-value pair information, and separate logical layer (i.e., virtual chain) is used to organize the naming system regardless of the underlying blockchain. Therefore, not only can Blockstack increase the data storage capacity considerably but also allows the logical layer to improve and extend independently.

Essentially, blockchain technology is a candidate of great promise for the next-generation DNS system in that it inherently possesses the qualities of

ensorship-resistance, security, and resilience. In summary, blockchain-based DNS systems own the required properties for a naming system. They are immune to attacks traditional DNS usually suffers such as protocol attacks and server attacks. Additionally, they can offer privacy protection for the clients as the DNS lookup can be done locally at the chain stored in the nodes. However, while maintaining a complete local copy of DNS entries might impact the performance of DNS lookups positively, it can be costly regarding disk space. For example, Namecoin [30], the blockchain size currently is 5.29 GB, and it is expected that the volume will significantly increase when scaling to millions of users in the future.

Other computer science technologies can also be combined with the blockchain, such as artificial intelligence. For example, AI can be defined in a simple way as a layer on top of blockchain data to analyze data (e.g., looking for irregularities in public services<sup>c</sup>), or to interconnect AIs in a marketplace where different AI can communicate to each other, as described in the project SingularityNET [31]. The goal is to provide an open platform based on blockchain where any AI developer can include modules with specific capabilities, combining all the different knowledge to create a better AI. Therefore, SingularityNET aims to become a standard protocol for networking AI and machine learning tools [31].

Another interesting project is presented in the ScienceMatters project [32]. Currently, scientists must be trusted to provide a true and useful representation of their research results in their final publication; blockchain would make much larger parts of the research cycle open to scientific self-correction. While the current centralized solution solves important issues in academic publishing, a blockchain-based solution can go even further.

Full transparency, where the researcher can see also previous reviews of reviewers, any potential social bias can become visible. Not only the reviewers can be rewarded as in the centralized system (e.g., reward scientists who conduct a timely peer review), also a scheme where a reference to other reviewers can be rewarded. Thus, a ground breaking and often cited paper would be rewarded with more Ethers or Tokens. Trying to achieve the same functionality with the current banking system is much more difficult and error-prone. The same way an author gets Tokens or Ethers for getting cited, this could also be applied for confirmation or contradiction of existing research. For a confirmation, Tokens or Ethers can be added, while for a contradiction Tokens or Ethers may be deducted.

---

<sup>c</sup> A.I. for social control of public administration: <https://serenata.ai/en/>.

Middlemen are no longer needed to decide what is published and what is not. Instead, as long as observations pass the required peer review process they are published and recorded on the blockchain. This ensures scientists' and researchers' discoveries and observations are recorded in a tamper proof way with a time stamp. This has important ramifications for protecting intellectual property. While the blockchain-based solution also solves the same issues as the current ScienceMatters platform: Overreliance on Trust and Lack of Objectivity, Fear of Getting Scooped, Many Scientific Observations Are Not Published, Reluctance To Publish Reproduced Results, the most important argument for using a blockchain is "profits and control." With a blockchain-based system, the traditional publishing middleman will become obsolete.

Among the diverse areas of computer science, blockchain can operate as a large interoperability platform enabling systems that, usually operate in isolation or with limited interoperability, to exchange information without intermediaries in a transparent way. Also, the ability to decentralize information enable services, once centrally provided as a single point of failure, to become more resilient to attacks. Therefore, it is general benefits of blockchains in computer science applications can be summarized (but not limited to) as:

- *Interoperability*: enabling a transparent platform for individual systems to exchange information verifiably. It not only enables new possibilities for collaborative systems but also helps to transform the way existing systems communicate.
- *Decentralization*: transference of information is securely done without intermediaries on a peer-to-peer basis. Therefore, services that were centrally provided can be fully decentralized by extending resilience to denial of service attacks.

However, there are still challenges related with the performance which can reduce or delay the interactivity of cooperative systems. Also, maintaining a local copy of the chain results in a disk space requirement that can restrict use on constrained devices. For example, while it is beneficial to perform a local lookup on the DNS entries, it is also to store the entire chain locally. Therefore, storing and maintaining large blockchain data at every node might not be viable. Moreover, it is necessary to understand the blockchain traffic (i.e., protocol execution, block-generation period, and size) to estimate the computational overhead in the targeted system. In this regard, challenges can be summarized as:

- *Performance and storage requirements*: for some applications latency and communication overhead can become a deciding factor. In this sense,

the evaluation of the blockchain type as well as its consensus algorithm becomes crucial in the decision. As the number of participants and transactions increases, the blockchain also increases, making it costly to store it, which can be a limiting factor for constrained nodes.

- *Privacy and confidentiality*: ensuring privacy and confidentiality remains a challenge. Even being possible to hide information on a blockchain, using well-established cryptographic methods, and instances may spread data sensitive and reveal the behavior and preferences of their owners. Therefore, complete anonymity is not possible, but only pseudoanonymity, evolving toward solutions that reduce the possibility of identifying systems from the identification of patterns in the behavior of the data.

### 2.2.7 Discussion

As the public image of blockchains is slowly disassociated from a cryptocurrencies, especially a Bitcoin view, there is a strong trend to discover new application areas and use cases, where a blockchain can be as disruptive as in the financial sector. Indeed, there are several use cases in which blockchains can reshape the way how entities can interact and trade, providing a trustworthy platform to transact without relying on a third party. However, the decision on whether the application of a blockchain makes sense for new use cases is still not trivial. It requires not only to check if a particular use case fulfills all key blockchain properties, but it also requires an analysis on whether a particular blockchain implementation satisfies such a use case's requirements.

The replacement of an existing ecosystem, consisting of a set of entities, processes, and legacy systems by another logic based on blockchains, requires a large capacity of articulation between these entities. In other words, the use of blockchains needs to create a measurable advantage that could justify the replacement of a working ecosystem by a new one based on blockchains. Otherwise, it is unlikely that the new technology will even be tested. Still, not even a positive disruption can result in the adoption of the technology, once government actors can introduce new laws to monitor and regulate the use of a certain technology or system.

The selected application areas and use cases not only confirm that blockchains can, in general, increase the efficiency of how entities interact, but it also reveals specific technical, institutional, and human challenges that need to be addressed before a successful deployment. While almost all

technical challenges are related to trade-offs between application requirements (e.g., performance vs confidentiality) and what the blockchain can deliver regarding its functionality, institutional and human challenges, respectively, are related to legal and compliance requirements and the lack of knowledge about the technology itself. Lastly, there is the economic aspect regarding the processes of adoption and maintenance of the technology that must also consider the impact in the other aspects.

#### 2.2.7.1 Technological Aspects

Different types of blockchains (permissionless, public/private permissioned) exist, whereas each one is suitable for a scenario. While, on one hand, permissionless blockchains present by design a high level of transparency and redundancy, on the other hand, they show limitations regarding performance and confidentiality requirements. There exist other implementations, where write and reading permissions can be distributed only to those who take part in the system. The challenge is to maintain these blockchain properties of transparency and redundancy, while performance and confidentiality are increased, which often requires a certain level of trust in a centralized entity managing the blockchain. However, the most important technical challenge for blockchains is scalability, which is not a goal to be achieved simply, but considered today a moving target. For example, the main goal of cryptocurrencies is to achieve the same level of transactions per second as a centralized system can do, while key blockchain properties are maintained. Therefore, the difficulty encountered in the system is intrinsically related to preserving such qualities, in addition to not impair its appreciation as a currency.

#### 2.2.7.2 Institutional Aspects

Most governments have not defined rules regulating cryptocurrencies or other blockchain applications or these rules may be conflicting across state lines, creating a suitable or limiting environment for innovative blockchain-based start-ups. On one hand, start-ups are free to innovate, but on the other hand, more established companies hesitate to adopt the technology until they know exactly how it will be governed and especially how much risk will be involved. For example, if an error occurs in the execution of a SC in a permissionless blockchain, it is not easy to determine who will be legally responsible. However, government agencies and international organizations already started preliminary work to regulate the technology

(mostly with respect to cryptocurrencies). For example, Japan recognizes Bitcoin as a legal currency being definitely legalized in 2017 [33], and the World Economic Forum (WEF) published a long study on the likely impact of various methods of blockchain governance [34]. Also, changes in regulation can create opportunities, as seen in the cases of modum.io [2] and VALID [24]. Both companies explored changes on European Union regulations to control the distribution of medicinal products [2] and ownership of digital user data [24].

#### 2.2.7.3 Human Aspects

From a practical point of view, many people and places are not ready for a digital transformation. As described in the supply chain area [2], most of the personnel working in warehouses are very well used to paper-based processes, and replacing these processes by digital ones (e.g., an app in a smartphone to create shipments) may require lots of effort on the user experience of these digital processes. Also, most warehouses do not provide network connectivity, which impacts on the hardware design's side of sensors the use of long-range protocols (e.g., LoRaWAN). Also, it is important to note that a blockchain is only responsible for ensuring the information, but the accuracy of the information relies on the input of data, e.g., the sensors applied. Other examples are found within the financial sector, where the user experiences the secure key management for cryptocurrencies. Instead of focusing only in the functionality, such software solutions should also focus on user experience to ease the operation of these features by non-technical persons.

#### 2.2.7.4 Economic Aspects

Blockchain can facilitate, simplify, and improve business and processes, be applying to several areas and cases where multiple entities are involved. Thus, not only the costs associated with manual paperwork, legal documentation processing, duplicate entries, and mismatches can be reduced with digital processes, but it also enables a transparent platform for centralized systems to exchange information verifiably, which also reduces costs. However, it is necessary to evaluate impacts of the blockchain adoption process on the mentioned areas (technological, human, and legal) and their associated costs before beginning the transition process. Also, blockchain is still a technology in the process of evolution and maturation, which may, therefore, require time for the totality or even a portion of its benefits to be fully obtained.



### 3. RESEARCH DIRECTIONS

While the majority of blockchain research focuses on revealing and improving technical limitations of blockchains, such as *scalability*, *privacy*, and *security* requirements, other aspects are becoming equally important. Among these technical requirements, scalability is the main concern of both industry and academia, seeking solutions to increase the number of transactions per second (especially for a public blockchain), while the consensus over the chain and current blockchain properties are to be maintained unchanged. In addition, other research directions, which may pave the way for more use cases being applicable, are not to be forgotten, thus, they are discussed here.

With the rise of attention in the blockchain technology and the lack of regulations in many sectors, many blockchain-based start-ups are using their own blockchain platform to raise funds through an initial coin offering (ICO). Also, different blockchains for different application areas and use cases will create the need for a blockchain interoperability and new processes of distributed governance to organize the interactions of many entities using many blockchains.

#### 3.1 Initial Coins Offering

Among the various potential applications of a blockchain, one of the most promising ones and a very frequently adopted one is an ICO—initial offers of currencies (similar to traditional initial public offerings—IPOs). ICOs can be considered as a new way to raise funds to finance project development. So far, ICOs were used primarily by small businesses and start-ups for creating and issuing a token through the blockchain for an initial fundraising campaign. Sometimes, the new token is offered to the public in exchange of existing cryptocurrencies (e.g., Ether or Bitcoin), but this is not always the case. Tokens issued in ICOs may also offer rights in a company, i.e., voting and capital rights, or even access to different services and applications, which could be enabled through SCs.

Cryptocurrencies and ICOs are increasingly subject to inspection by public agencies. They are starting to publish their interpretations and rules to be applied from a governmental regulation perspective. In Switzerland, for example, even if ICOs are not officially regulated by Swiss legislation, the independent financial markets regulator (FINMA) published guidelines defining how it intends to apply financial market legislation in handling

inquiries from ICO organizers [35]. The goal of this document is to create transparency in how an ICO is conducted, protecting both the organizers and investors from fraudulent activities (such as money laundering).

### 3.2 Blockchain Interoperability

In the future, assets and information are predicted to be spread in different blockchains of different companies (e.g., financial information or digital information), revolving a similar problem of current traditional databases. In this regard, the blockchain interoperability or federation has the goal to collect data from multiple parallel blockchains, while retaining each of their security properties. Thus, it means that users could access a wide range of blockchain features that are native to each chain without the need to download large blockchain files for every chain they want to use [36]. Currently, interoperability can be handled off-chain with developers handling different SC languages or third-party tools, but it requires a standardization effort toward a common SC language across all blockchains. In addition, the handling of information off-chain can create inconsistencies in case of network failures or longer-term lacks of access.

### 3.3 Blockchain Governance

For the first time in history, communities can now reach consensus and coordination at a global level through cryptographically verified peer-to-peer procedures to provide governance services in a more efficient and decentralized way, without the intermediation of a third party. However, blockchains still require a set of common rules by which all participants operate, to ensure its accuracy and trustworthiness, and it is not yet clear what and how the governance process is going to be in the face of the many possible application areas and use cases. For example, despite of interoperability efforts promoted in the health care industry by the Office of the National Coordinator for Health Information Technology (ONC) and the blockchain technology being able to satisfy most requirements, it is still not clear how the governance process can be defined to organize how many entities can cooperate in such complex industry.



## 4. CONCLUSIONS

In overall conclusion, current work on blockchains and SCs does indicate that many fully decentralized actions can be performed reliably in a distributed manner, however, efficiency, security, and legality in a multitude of different

facets—typically determined by the dedicated application area or use case—have to be addressed in an integrated manner in the near future to reach a long-term viable balance of usability and efficiency of major or even all blockchain operations. Thus, the roles of the various use cases discussed earlier, the technological alternatives of blockchains being implemented and used, and technical, regulatory, human, and economic requirements require a thorough evaluation to determine whether a blockchain solution makes sense or not for a particular use case.

## REFERENCES

- [1] N. Satoshi, Bitcoin: A Peer-to-peer Electronic Cash System.: 28, URL: <https://bitcoin.org/bitcoin.pdf>, 2008.
- [2] T. Bocek, B. Rodrigues, T. Strasser, B. Stiller, in: *Blockchains Everywhere—A Use-Case of Blockchains in the Pharma Supply-Chain*, IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2017), 2017, pp. 772–777. Lisbon, Portugal.
- [3] W. Karl, A. Gervais, Do You Need a Blockchain? IACR Cryptology ePrint Archive: 375, 2017. Cryptology ePrint Archive.
- [4] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, Ethereum Project Yellow Paper 151 (2014) 1–32. Chicago.
- [5] T. Bocek, B. Stiller, Smart contracts—blockchains in the wings, in: *Digital Markets Unleashed*, Springer, Heidelberg, Germany, January, 2017, pp. 1–16.
- [6] Z. Zheng, S. Xie, H.N. Dai, H. Wang, *Blockchain Challenges and Opportunities: A Survey*, 2016. Working Paper.
- [7] D. Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, New York, NY, 2017.
- [8] G. Greenspan, Avoiding the Pointless Blockchain Project, URL: <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/>, 2015.
- [9] B. Vitalik, On Public and Private Blockchains, URL: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>, 2015.
- [10] P. Boucher, How Blockchain Technology Could Change Our Lives. European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), 2017. PE 581.948. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS\\_IDA\(2017\)581948\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf).
- [11] M. Iansiti, K.R. Lakhani, The truth about Blockchain, *Harv. Bus. Rev.* 95 (1) (2017) 118–127.
- [12] K. Korpela, J. Hallikas, T. Dahlberg, in: *Digital Supply Chain Transformation Toward Blockchain Integration*, 50th Hawaii International Conference on System Sciences, Hawaii, U.S.A., 2017.
- [13] IBM, Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain, URL: <https://www-03.ibm.com/press/us/en/pressrelease/51712.wss>, 2017.
- [14] S. Dani, *Food Supply Chain Management and Logistics: From Farm to Fork*, Kogan Page Publishers, 2015. URL: [https://www.koganpage.com/media/project\\_kp/document/food-supply-chain-management-and-logistics-sample-chapter.pdf](https://www.koganpage.com/media/project_kp/document/food-supply-chain-management-and-logistics-sample-chapter.pdf).
- [15] M. Schneider, Design and Prototypical Implementation of a Blockchain-Based System for the Agriculture Sector, Universität Zürich, Communication Systems Group, Department of Informatics, Zürich, Switzerland, 2017.
- [16] European Union, Guidelines of 5 November 2013 on Goods Distribution Practice of Medicinal Products for Human Use, URL: [http://ec.europa.eu/health/files/eudralex/vol-1/2013c343\\_01/2013c34301en.pdf](http://ec.europa.eu/health/files/eudralex/vol-1/2013c343_01/2013c34301en.pdf), 2013.

- [17] K.B. DeSalvo, RE: Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, 2015. URL: <https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf>.
- [18] S. Angraal, M.H. Krumholz, W.L. Schulz, Blockchain technology: applications in health care, *Circ. Cardiovasc. Qual. Outcomes* 10 (9) (2017) e003800.
- [19] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data, in: *IEEE Open & Big Data Conference*, 13, 2016, p. 13.
- [20] M. Gault, Increasing Healthcare Security With Blockchain Technology, URL: <https://guardtime.com/blog/increasing-healthcare-security-with-blockchain-technology>, 2017.
- [21] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in Internet of Things: Challenges and Solutions, 2016. arXiv preprint arXiv:1608.05187.
- [22] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, *IEEE Access* 4 (2016) 2292–2303.
- [23] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, Uport: A Platform for Self-Sovereign Identity, Whitepaper. URL: [https://whitepaper.uport.me/uPort\\_whitepaper\\_DRAFT20170221.pdf](https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf), 2017.
- [24] VALID, Your Data Your Asset, Whitepaper. URL: <https://valid.global/static/valid-wp-2.pdf>, 2018.
- [25] B. Hall, 5 Identity Problems That Blockchain Does Not Solve, URL: <https://blog.id.me/identity/fintech/5-identity-problems-blockchain-doesnt-solve/>, 2017.
- [26] M. Ali, J. Nelson, R. Shea, M.J. Freedman, Blockstack: A Global Naming and Storage System Secured by Blockchains, *USENIX Annual Technical Conference*, Denver, CO, 2016.
- [27] E-Resident, Republic of Estonia—e-Residency, URL: <https://e-resident.gov.ee/>, 2018.
- [28] I. Martinovic, Blockchains: Design Principles, Applications, and Case Studies, Working Paper No. 7 (Draft). URL: <http://egov.ee/media/1374/martinovic-blockchains-design-principles-applications-and-case-studies.pdf>, 2017.
- [29] Y. Liu, Q. Wang, An E-Voting Protocol Based on Blockchain, URL: <https://eprint.iacr.org/2017/1043.pdf>, 2017.
- [30] A. Loibl, J. Naab, Namecoin. Seminar Innovative Internettechnologien und Mobilkommunikation SS2014, URL: [https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2014-08-1/NET-2014-08-1\\_14.pdf](https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2014-08-1/NET-2014-08-1_14.pdf), 2014.
- [31] B. Goertzel, S. Giacomelli, D. Hanson, C. Pennachin, M. Argentieri, SingularityNET: A Decentralized, Open Market and Inter-Network for AIs, URL: <https://public.singularitynet.io/whitepaper.pdf>, 2017.
- [32] Science Matters, The Next-Generation Science Publishing Platform, URL: <https://www.sciencematters.io/>, 2018.
- [33] B. Yap, New EU Payment Services Rules Spur New Regulation in Japan, *International Financial Law Review*, 2017. 3/6/2017, p. 7. URL: [https://searchworks.stanford.edu/articles/bah\\_121561457](https://searchworks.stanford.edu/articles/bah_121561457).
- [34] World Economic Forum (WEF), Realizing the Potential of Blockchain. A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies, Whitepaper, 2017. URL: [http://www3.weforum.org/docs/WEF\\_Realizing\\_Potential\\_Blockchain.pdf](http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf).
- [35] FINMA, Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs), URL: <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>, 2018.
- [36] V. Buterin, Chain Interoperability, URL: <http://www.r3cev.com/s/Chain-Interoperability-8g6f.pdf>, 2016.

## FURTHER READING

- [37] B.B. Rodrigues, T. Bocek, B. Stiller, In: *Blockchain Signaling System (BloSS): Enabling a Cooperative and Multi-Domain DDoS Defense*, 42nd Annual IEEE Conference on Local Computer Networks (LCN 2017, Demo Track). Singapore, 2017.

## ABOUT THE AUTHORS



**Bruno Rodrigues:** received the B.Sc. degree in computer science from University of the State of Santa Catarina (UDESC) in 2013 and his M.Sc. degree in Computer Engineering from the Polytechnic School of University of São Paulo in 2016. He joined the Communication Systems Group (CSG) at the University of Zurich (UZH) in September 2016 to obtain his Ph.D. degree.



**Prof. Dr. Thomas Bocek:** received the Doctor of Informatics (Dr. Inform.) degree from the University of Zurich. Dr. Thomas Bocek is currently the head of P2P and distributed systems at the Communication Systems Group at the University of Zurich since 2013. Before that, he worked as a software engineer and technical project manager in the financial sector. Thomas is mainly interested in communication systems and networks, especially focusing on peer-to-peer, distributed systems, and blockchains

including Bitcoin and Ethereum. He is also involved in the blockchain start-up modum.io, which combines IoT sensor devices with blockchains. In 2018, Thomas will join the University of Applied Sciences of Eastern Switzerland as a professor for distributed systems.



**Prof. Dr. Burkhard Stiller:** received the Diplom-Informatiker (M.Sc.) degree in computer science and the Dr. rer.-nat. (PhD) degree from the University of Karlsruhe, Germany. He chairs as a full professor the Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH since 2004. He held previous research positions with the Computer Laboratory, University of Cambridge, UK, the Computer Engineering and Networks Laboratory, ETH Zurich, Switzerland, and

the University of Federal Armed Forces, Munich, Germany. He did coordinate various Swiss and European industrial and research projects, such as AAMAS, DAMMO, SmoothIT, SmartenIT, SESERV, and Econ@Tel, besides participating in others, such as M3I, Akogrimo, ECGIN, EMANICS, FLAMINGO, and ACROSS. His main research interests are published in over 200 research papers and include charging and accounting of Internet services, systems with a fully decentralized control (blockchains, clouds), network and service management, economic management, telecommunication economics, and IoT.