


## **Towards the Adoption of Blockchain to Trustworthy Interoperability in Industry 4.0 Systems: A Case Study**


**Ana Paula Allian**

(University of São Paulo (USP). São Carlos, SP, Brazil)

 <https://orcid.org/0000-0001-9399-0944>, [ana.allian@gmail.com](mailto:ana.allian@gmail.com))


**Frank Schnicke**

(Fraunhofer IESE. Kaiserslautern, Germany)

 <https://orcid.org/0000-0002-4351-4488>, [Frank.Schnicke@iese.fraunhofer.de](mailto:Frank.Schnicke@iese.fraunhofer.de))


**Pablo Oliveira Antonino**

(Fraunhofer IESE. Kaiserslautern, Germany)

 <https://orcid.org/0000-0002-9631-8771>, [pablo.antonino@iese.fraunhofer.de](mailto:pablo.antonino@iese.fraunhofer.de))


**Thomas Kuhn**

(Fraunhofer IESE. Kaiserslautern, Germany)

 <https://orcid.org/0000-0001-9677-9992>, [Thomas.Kuhn@iese.fraunhofer.de](mailto:Thomas.Kuhn@iese.fraunhofer.de))

**Elisa Yumi Nakagawa**

(University of São Paulo (USP). São Carlos, SP, Brazil)

 <https://orcid.org/0000-0002-7754-4298>, [elisa@icmc.usp.br](mailto:elisa@icmc.usp.br))

**Abstract:** The rapid evolution of Industry 4.0 has brought forth transformative changes in manufacturing, accentuating the need for seamless interoperability among heterogeneous systems. However, the geographically distributed and decentralized nature of Industry 4.0 ecosystems presents a pressing challenge: ensuring trustworthy interoperability within a complex web of entities and intermediaries. This paper delves into the pivotal role of blockchain technology in addressing this challenge, aiming to bridge the gap between theoretical promises and practical applications. By examining the feasibility and efficacy of blockchain solutions in fostering trust and enabling interoperability within Industry 4.0 environments, we confront the pressing issue of data security, integrity, and reliability. Through the lens of seven blockchain-based solutions, we navigate the intricate landscape of Industry 4.0, offering insights into the trade-offs, risks, and potentials associated with blockchain adoption. Real-world case studies and practical demonstrations underscore the urgency and relevance of our research, shedding light on pathways for industry stakeholders to navigate the complexities of interoperability. Our findings not only contribute to advancing the discourse on blockchain's role in Industry 4.0 but also provide actionable strategies for addressing the overarching challenge of ensuring trustworthy interoperability in the digital age.

**Keywords:** Industry 4.0, Interoperability, Trustworthy Interoperability, Blockchain, System Architecture, Requirements

**Categories:** D.2, D.2.10, D.2.11, D.2.12

**DOI:** 10.3897/jucs.125714

## 1 Introduction

Industry 4.0 has drastically changed manufacturing processes, making them faster and more efficient, opening opportunities for new businesses, and culminating in the fourth industrial revolution [Antonino et al., 2019, Li and Qiao, 2023]. Interoperability among software systems, robots, devices, services, and many other virtual and physical entities is an essential requirement in Industry 4.0 systems [Kumar et al., 2023]. An important entity in Industry 4.0 systems is the digital twin, which refers to a digital representation of a physical asset [Javaid et al., 2023] and enables simulation of future scenarios for planning and preventive maintenance [Antonino et al., 2019, Uhlemann et al., 2017]. It also allows for easier integration of data analysis, machine learning, and monitoring that can be directly tied to the physical asset. Industry 4.0 systems should also present both horizontal and vertical integration. While horizontal integration refers to the integration of processes at the production floor level, vertical integration refers to the integration of entities from the production floor to the higher-level business process [Antonino et al., 2019, Kuhn et al., 2018]. Connections among these heterogeneous entities are created, undone, and changed at runtime. This results in systems that make it possible to quickly switch suppliers, identify plagiarism, and guarantee the authenticity of products [Kuhn et al., 2018].

Geographically distributed ecosystems, like Industry 4.0 systems, raise concerns related to trustworthy interoperability, as they involve fine-grained entities (e.g., humans, robots, sensors) to coarse-grained decentralized entities (e.g., enterprises and businesses). These ecosystems also rely on many intermediaries (i.e., entities of smart factories or entities from other factories/companies), which potentially increase the risk of unauthorized access to data. Moreover, such intermediaries can increase the risk of intrusions, interruption of production, sabotage, and manipulation of data and services, leading to injuries or even loss of lives [Bicaku et al., 2017]. Hence, trustworthy interoperability becomes an essential requirement for Industry 4.0 systems and is decisive for assuring their success [Horváth and Szabó, 2019].

In the context of this work, “interoperability” can be defined as the ability of two or more entities to exchange meaningful information to achieve shared goals [Bass et al., 2012, ISO/IEC, 2011]. In addition, “trustworthy interoperability” refers to the ability to exchange data in a trusted way within Industry 4.0 ecosystems. Based on other works that discuss trustworthy interoperability in Industry 4.0 [Allian et al., 2021, Li and Qiao, 2023], it can also be understood as the balance between quality aspects (e.g., data privacy, data transparency, ethical concerns, and data protection) in the communication among known entities. These entities should be connected in a transparent and coordinated infrastructure that allows data exchange according to predefined rules for achieving common goals. Recent solutions have addressed trustworthy interoperability in Industry 4.0, but focused on specific concerns related to trust, including security [Bicaku et al., 2017], authentication, access control [Kjersgaard and Eriksena, 2018], and data privacy [Fraile et al., 2018].

At the same time, blockchain has been considered a promising technology for solving trust-related concerns in the interoperability of systems. Blockchain is a distributed database of transactions used to share and replicate data and synchronized across all blockchain partners [S.Perera et al., 2020]. Due to this fact, it can reduce or avoid the need for intermediaries [Christidis and Devetsikiotis, 2016, Lu, 2017, Wang et al., 2018]. Commonly associated with cryptocurrencies, e.g., Bitcoin [Nakamoto, 2009], blockchain has also been more recently applied across a wide variety of industry sectors, including healthcare [Wang et al., 2018], financial [Pazaitis et al., 2017], automotive

[ul Ain Arshad et al., 2023], and Internet of Things [Christidis and Devetsikiotis, 2016]. Blockchain has also increasingly gained acceptance in Industry 4.0 projects as a solution that can assure trust [Anjum et al., 2017, Hawlitschek et al., 2018, ul Ain Arshad et al., 2023], security [Fernandez-Carames and Fraga-Lamas, 2019], and transparency [Ahram et al., 2017]. The Industry 4.0 community has believed blockchain could provide trustworthy interoperability, but there is no scientific evidence that assures blockchain can assure such interoperability. Hence, the main research question that guided this work is: “Do people intend to use blockchain to assure trustworthy interoperability in Industry 4.0 systems?”

The main contribution of this work is a set of seven blockchain-based solutions that could promote trustworthy interoperability in Industry 4.0 systems. To do this, we first elicited and defined a set of architecture drivers that could together assure such interoperability [Allian et al., 2021, Allian, 2021]. In short, architecture drivers refer to key requirements classified as risky, new, and costly that, if not adequately maintained, can seriously affect the architecture design and implementation [Antonino et al., 2019, Knodel and Naab, 2016]. Following, together with highly trained experts in both Industry 4.0 and blockchain, we systematically analyzed whether blockchain is a proper solution for implementing those drivers. We found that blockchain alone cannot be considered a reliable solution for the complicated interoperability situations that occur in Industry 4.0 systems. Hence, based on our experience in Industry 4.0 projects and together with those highly trained experts, we defined the set of blockchain-based solutions that, while they benefit from blockchain, they cover all complementary aspects that need to be addressed together to achieve the so required interoperability. We also provide a discussion about what is favorable or not with blockchain, the pros, cons, risks, and trade-offs of adopting blockchain, besides alternative and/or complementary technologies. We also present a real-world case associated with an automated transport system to move workpieces throughout the shop floor, in which we show how the blockchain-based solutions can be used. By first addressing together the different aspects required to achieve trustworthy interoperability in Industry 4.0 systems, this work can provide direction for the future generation of Industry 4.0 systems, mainly about how to deal with the complicated interoperability of their components.

This paper is structured as follows. Section 2 presents the research method applied in this work. Section 3 details the results as well as the blockchain-based interoperability solutions. Section 4 discusses the main findings of this work and threats to validity, and presents a scenario where our solutions have been used. Section 5 concludes this work.

## 2 Research Method

### 2.1 Architecture Drivers

A set of architecture drivers, also known as essential requirements that can affect the design and implementation for trustworthy interoperability in Industry 4.0 systems, were established in [Allian et al., 2021, Allian, 2021]. These drivers consider the main challenges regarding interoperability in real-case Industry 4.0 projects and observations of real-world industrial projects in the context of BaSys 4.0<sup>1</sup>, the German reference project for Industry 4.0. This project encompasses a consortium with several research institutions and companies, such as Bosch (German multinational company for engineering and

<sup>1</sup> <https://www.basys40.de>

electronics solutions), Kuka (German company for automation solutions), Fortiss GMBH (software-intensive systems and services research institute), SYSGO and Kontron (company related to critical application and security solutions), SMS Group (leading global partner for the metallurgical industry in Germany), ITQ (independent engineering and consulting firm), and ABB (multinational in the areas of robotics, energy, heavy electrical equipment, and automation technology).

## 2.2 Survey Planning

The survey was systematically planned accordingly to [Wohlin et al., 2012]. Participants were required to have extensive experience with Industry 4.0 projects while also being blockchain experts. Eight experts working in Industry 4.0 projects were selected; two of them are also experts in blockchain. Participants had at least three years of experience with Industry 4.0 projects in different roles, including Software Architect (SA) (Interviewees 1 and 4), Project Manager (PM) (Interviewees 2 and 7), Software Engineer (SE) (Interviewees 3, 5, 6, 7, and 8), Researcher (RE) (Interviewees 3 and 4), Quality Manager (QM) (Interviewee 5), and Blockchain Expert (BC) (Interviewees 1 and 2).

Therefore, respondents were well-experienced in software and gave confidence to their answers. A semi-structured interview was conducted [Wohlin et al., 2012] to answer two main questions: *Q1: Can blockchain be considered a solution for realizing each architecture driver? Q2: If blockchain cannot completely the realization of each architecture driver, which are the solutions that could be combined (or not) with blockchain to solve each driver?*

## 2.3 Survey Execution

The interview was conducted individually with each expert and they were free to ask, discuss, and share their experience from real-world Industry 4.0 projects. When an expert did not agree that blockchain could be a proper solution for a given driver, the interviewer asked for other solutions that could cover that driver and if this solution could be combined with blockchain or not. Each interview took around 60 minutes, totaling 9 hours and 20 minutes of audio during the step “*Record interviews in audio*”.

## 2.4 Analysis of Results

Grounded Theory [Strauss and Corbin, 1998] was used to systematically analyze the information collected from interviews and two techniques were applied: (i) *open coding* (which identifies *codes* that are separated into discrete parts for analysis); and (ii) *axial coding* (which handles connections between codes and groups them according to their similarities). The QDA Miner<sup>2</sup> was used to support analysis, as follows:

- **Transcript of interview:** The eight interviews (referred to as I1 to I8) were transcribed into a 59-page text document (32,320 words).
- **Coding:** The text or select portions of the data were manually categorized and assign the relevant codes. Figure 1 depicts an example of pieces of text assigned to different codes that were identified using the QDA Miner tool. The tool supported

<sup>2</sup> <https://provalisresearch.com>

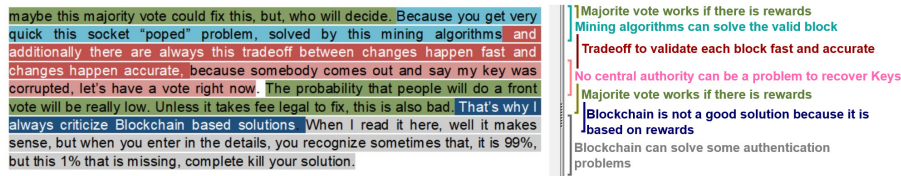


Figure 1: Pieces of text (left side) from interview II about the driver *Authentication to the System* and codes identified with the QDA Miner tool (right side)

the identification of 24 codes related to the driver *Authentication to the System*. For instance, from the pieces of text “*I am not sure if a blockchain-based concept will have any benefit*” and “*...maybe this majority vote could fix this, but, who will decide*”, which were said in I1, the codes “*Blockchain does not bring benefits*” and “*Majority vote is a drawback*” were identified, respectively. These codes were used as a first set to code the interviews of the other respondents, considering the part of the interviews related to this driver. When new codes were identified, they were included in this set. In the end, 125 codes for this driver were identified. The process was repeated for each architecture driver resulting in a total of 678 codes. Table 1 lists the codes from interviews.

- **First categorization of codes:** The transcript was divided into seven categories: *Authentication to the System* (125 codes), *Data Access Control* (90 codes), *Data Privacy to Protect Sensitive Information* (111 codes), *Traceability and Auditability of Data* (106 codes), *Availability of Data* (97 codes), *Availability of Physical Devices* (74 codes), and *Compatibility of Data and Services* (75 codes).
- **Second categorization of codes:** Two other broader categories were defined (“*Blockchain may be a good solution*” and “*Blockchain may not be a good solution*”), which were the main theme of interest during the analysis. Due to space limitations, the pros and cons of blockchain for the driver *Authentication to the System (AS)* are presented as follows: Pros of using blockchain: “*AS.7. Blockchain brings trust because it is a distributed system*”: A decentralized infrastructure would bring more security and reliability for dealing with sensitive and critical data; “*AS.1. Blockchain and public-key infrastructure (PKI) can bring security*”: Blockchain relies on cryptography infrastructure such as PKI, which brings more security for exchanging data; and “*AS.12. Blockchain can help to bring transparency in the whole chain*”: Blockchain would bring more transparency and the ability to automatically define smart contracts for production settings. Cons of using Blockchain: “*AS.5. Blockchain majority vote is difficult to be applied*” and “*AS.19. Blockchain majority vote works if there are rewards*”: These codes describe the concern regarding the use of majority vote, which corresponds to agreed votes from each manufacturer to modify behavior or data inside the blockchain; “*AS.18. Blockchain trade-off is to validate each block in a fast, accurate way with a consensus algorithm*”: The consensus mechanisms describe the agreement among all nodes of the blockchain and can be achieved by implementing a proof of work or proof of stake. In the proof of work, miners are rewarded by solving complex formula equations. In the proof of stake, it is based on the number of coins a person has to mine the block to get a reward [ul Ain Arshad et al., 2023]; and “*AS.2. Blockchain is a risk if you lost the identity keys*” and “*AS.8. Blockchain needs to be combined with a central*

*authority*”: These codes describe security concerns in case credential identities are lost. In a blockchain, it is hard to recover lost IDs. As a result of this categorization, 268 codes were categorized into “*Blockchain may be a good solution*” and 410 codes into “*Blockchain may not be a good solution*”.

- **Merging codes:** Codes with the same meaning were merged together. For instance, once again considering *Authentication to the System*, the codes “*AS.16. blockchain is not mature for authentication*” and “*AS.27. There is still the need for more evaluation of Blockchain*” are similar, so we merged them into the code “*AS.16. Blockchain is not mature technology for authentication*”. Analyzing all 125 codes related to this driver, we found 23 unique codes, of which 12 were in category “Blockchain may be a good solution”, while 11 were in category “Blockchain may not be a good solution”. Table 1 summarizes the unique codes for each driver.

Table 1: Number of codes identified using open coding

Drivers	Interviews (Roles)								Subtotal of codes	Subtotal of unique codes
	I1: SA/BC	I2: PM/BC	I3: SE/RE	I4: SA/RE	I5: SE/QM	I6: SE	I7: PM/SE	I8: SE		
Authentication to the System	24	18	15	12	13	13	15	15	125	23
Data Access Control	13	15	10	7	9	7	9	20	90	22
Data Privacy to Protect Sensitive Information	17	23	10	13	10	13	8	17	111	19
Traceability and Auditability of Data	15	19	12	11	9	8	9	23	106	22
Availability of Data	16	18	8	10	11	9	6	19	97	19
Availability of Physical Devices	10	10	4	12	6	5	8	19	74	17
Compatibility of Data and Services	10	15	8	4	7	7	7	17	75	16

Figure 2 shows the percentage of codes that are favorable and unfavorable to the adoption of blockchain for each architecture driver. While blockchain could be beneficial for the drivers *Data Access Control* and *Traceability and Auditability of Data*, it could not support *Availability of Data*, *Availability of Physical Devices* and *Compatibility of Data and Services*. Each expert’s statement were analysed aiming to identify solutions for the architecture driver. For instance, considering the driver *Authentication to the System* experts declared that “*Maximum security is achieved with blockchain encryption, supporting certified device and users to connect to the production line network.*” This was said in interview I2 and pointed to the adoption of blockchain. This statement enabled us to connect it to another statement in favor of blockchain: “*Blockchain is for distributed systems and ensures no centralized point of failures*”, which was claimed in interview I8. Another example is the statement “*So, from the security point of view, I am not sure if a blockchain-based will have any benefit so only thinking on the security perspective in contrast to a central authority.*”, which was said in interview I1 and was against the adoption of blockchain. Another statement against blockchain was “*Especially in security, there are a lot of solutions, such as PKI. So if you use blockchain, you are going to use PKI anyway, so why blockchain? Why not just public key?*”, which was said in interview I2. Both interviews presented concerns about blockchain and the security aspect on it. Besides, the experts claimed that combining blockchain with traditional

authentication servers could provide great benefits for interoperability in Industry 4.0, such as more transparency in the whole chain, better synchronization among participants, flexibility regarding authentication of distributed systems, and support for compliance with regulations through rules in smart contracts.

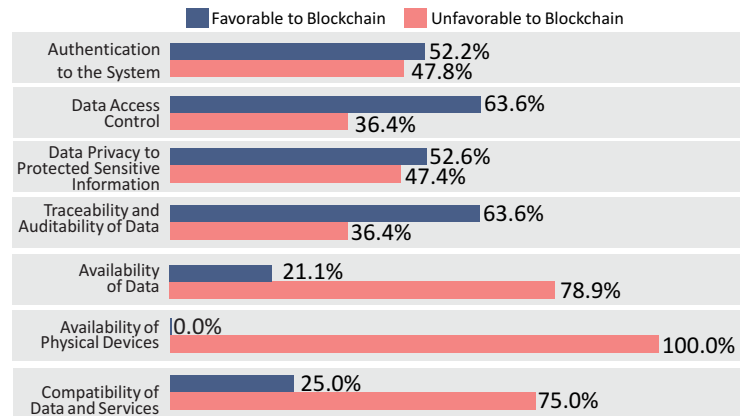


Figure 2: Experts' opinion regarding adoption of blockchain

The analysis used to identify solutions for the other drivers (*Data Access Control*, *Data Privacy to Protect Sensitive Information*, *Traceability and Auditability of Data*, *Availability of Data*, *Availability of Physical Devices*, and *Compatibility of Data and Services*) followed the same procedure as that for *Authentication to the System*. In the context of this work, these solutions refer to claims and assertions made by experts that can be further used for the architecture design and can also be represented by any model or notation [Knodel and Naab, 2016], i.e., they do not refer to models documenting a software architecture solution. In turn, these solutions are represented in terms of: (i) *favorable* or *unfavorable* for blockchain; (ii) *pros* or *cons* of adopting blockchain and associated challenges; (iii) *cons*, *risks*, and *trade-offs* of adopting the solution; and (iv) *alternative* or *complementary technologies*. The resulting solutions related to each driver are presented in the next section.

### 3 Blockchain-based Interoperability Solutions

We defined seven solutions to achieve trustworthy interoperability in Industry 4.0, as described in the next subsections:

#### 3.1 Authentication to the System

This driver describes the scenario where there is an ever-changing system that needs to support the addition and removal of new devices, users, digital twins, and other entities efficiently and transparently.

- **Favorable to blockchain:** Entities (i.e., users, devices) can have more control over their own identity without the need to trust a centralized authority. It guarantees non-discriminatory access to a marketplace operated by a player (e.g., Amazon or eBay). Such players can mediate production orders and enable automated agreement on smart contracts for producing goods. Partners that sign in would participate in the revenues (this would be analogous to Bitcoin).
- **Challenges for adopting blockchain:** The high cost for smaller companies to modify their existing systems as well as the need to create policies that fulfill the security requirements of all partners.
- **Cons & risks:** Partners of a blockchain may face disagreement if they choose to deploy changes unilaterally.
- **Alternatives:** Federated identity, certificate authorities, PKI, and protocols, such as OAuth 2.0, OpenID, or multi-factor authentication (id, password, PIN, email account, token device, and fingerprint).

### 3.2 Data Access Control

This driver describes entities (e.g., users, devices, and digital twins) that depend on access control to manage access. This system makes it possible to protect or prevent the occurrence of illegal access and modification of data generated by devices (e.g., data from an overheated device or data from an overloaded pallet).

- **Favorable to blockchain:** Blockchain provides immutable logs of access and bringing more transparency to the system. Each entity/partner can access and audit data records without the need for a central authority. Blockchain can also be used to document the agreements made by partners via smart contracts regarding how the data will be used.
- **Challenges for adopting blockchain:** Higher cost to change the current authorization control system and the necessity to create common policy requirements to properly define a security authorization mechanism to access production line.
- **Cons & risks:** Vulnerabilities of smart contracts and the need for an off-chain integration database for access policies.
- **Alternatives:** Access Control Lists (ACL) and Access Rules or systems covered by a Role-Based Access Control (RBAC) model that controls individuals' access to the system [Peralta et al., 2019], can also be good solutions for this driver. However, these solutions cannot solve problems regarding the presence of third parties that define the access privileges for each user, resulting in a lack of privacy. Besides that, current access control solutions are static and might be inadequate for the dynamism of Industry 4.0 systems. Hence, a combination of these solutions with blockchain is more suitable.

### 3.3 Data Privacy to Protect Sensitive Information

This driver describes concerns related to protecting intellectual property when information must be shared among different manufacturers in the Industry 4.0 ecosystems. This intellectual property refers to financial data, patents, and private data from companies that are under legal protection.



- **Favorable to blockchain:** Blockchain encrypts sensitive data and separates it into segments that can be accessed by authorized parties at any time using appropriate decryption keys. As blockchain contains a signature of bilaterally exchanged data and not the data itself, partners can check whether a contract was concluded without external parties being able to access the data. This enhances the privacy of data by replacing most identifying fields within a data record with one or more artificial identifiers.
- **Challenges for adopting blockchain:** Difficult to guarantee data privacy in a technology that is based on the principle of transparency and immutability of data.
- **Cons & risks:** When identifiers keys from off-chain databases are deleted, the on-chain data will be anonymized.
- **Alternatives:** Encryption protocol managed by a central server. However, a central administrator is necessary, which makes confidentiality and privacy a challenging problem. Hence, the adoption of blockchain combined with end-to-end encryption to protect sensitive data and a combination to access privileges as described for the driver *Data Access Control* could provide more benefits.

### 3.4 Traceability and Auditability of Data

This driver describes a scenario where the system must record every step in a process chain from raw material to the final product in an immutable way.

- **Favorable to blockchain:** A private blockchain naturally provides a data provenance by recording all transactions.
- **Challenges to adopting blockchain:** The dependency on a database to store data, as blockchain cannot support a large amount of data in the chain.
- **Cons & risks:** Response time to requests may increase as the number of devices increases in the production line.
- **Alternatives:** External service requests by assigning a unique ID. However, these traditional solutions are centralized and not all of them provide end-to-end traceability of data and tamper-resistant records to support stakeholders decision-making. Blockchain solves the issues of data traceability but does not solve the issue of data storage. Hence, every block should include hashes pointing to the data sets stored in databases; in this way, the state of each data set can be tracked securely.

### 3.5 Availability of Data

Industry 4.0 systems encompass many entities that increase the amount of data created, either through applications developed or deployed by the company, third-party systems, customers, or suppliers. This data must be available and manufacturers must document and make available data from the production line process. Representatives of the manufacturing process require verification of data related to a specific technical requirement (e.g., temperature and bombing pressure at a specific time in the production line).

- **Unfavorable to blockchain:** Although blockchain does perfectly store the hash to data, the raw data cannot be saved in the blockchain due to performance reasons.

- **Alternatives:** Backup server, databases, and the use of clouds are recommended alternatives for storing data from the production line. Digital twins can also be used to support the availability of data because they are virtual copies of real-world entities (e.g., data flow, production machine, operational processing status, functionalities, sensors, and robots), and they can synchronize manufacturing data and functions related to the plant design.

### 3.6 Availability of Physical Devices

This driver describes the scenario where many plants are connected and must deliver the information even when a failure occurs in the system.

- **Unfavorable to blockchain:** Blockchain cannot restore systems and, for this reason, it is not a good solution for this driver.
- **Alternatives:** Redundant servers/devices combined with digital twins. While digital twins enable the monitoring of devices identifying possible upfront failures, redundant servers and devices should exist if a nonstop production process is required. Besides, additional security for the whole production with a real-time monitoring and simulation system must be implemented, which can increase the cost to have a backup physical infrastructure.

### 3.7 Compatibility of Data and Services

This driver describes a scenario in which new entities from third parties are added to the current manufacturing process and must be semantically and syntactically compatible to exchange data.

- **Unfavorable to blockchain:** Blockchain cannot be used as a solution for this driver, as compatibility refers to how the systems are prepared for some extension and/or some intelligent mechanism to facilitate changes.
- **Alternatives:** A service-oriented middleware could provide the necessary services to enable compatibility of systems according to protocols that must be agreed by the partners involved in the production line. However, this type of solution makes it hard to ensure real-time compliance among manufacturers' systems and physical communication. In this scenario, we recommend the adoption of solutions that check the compatibility of data and services.

Due to the openness of these solutions, different existing approaches, techniques, and technologies related to alternative solutions can be adopted to implement the set of architecture drivers. When necessary, blockchain must be combined with these solutions. It is worth highlighting these solutions cover different, complementary aspects of trust to fully achieve interoperable Industry 4.0 systems; hence, all solutions must be implemented together.

## 4 Discussions

### 4.1 Main Findings

Achieving trustworthy interoperability in Industry 4.0 systems requires: (i) recognition that these systems are comprised of many heterogeneous entities; and (ii) awareness of how they interact with each other in a cross-layer Industry 4.0 environment. At the same time, trust must be pervasive in Industry 4.0 [Al-Ali et al., 2018, Bicaku et al., 2017], meaning that trust must be well-designed to assure all associated aspects are properly addressed. There are still divergent opinions (from experts directly involved in Industry 4.0 projects) regarding the adoption of blockchain as a solution for revolutionizing the interactions among entities that require a high degree of trustworthy interoperability in Industry 4.0 systems. However, blockchain has its benefits that should be explored in the Industry 4.0 context. Because of the distributed nature of blockchain, the data is transparent, preventing fraudulent behavior from non-trusted parties. In particular, a private blockchain is a good solution when different parties are involved in a production line and must be well-known by the others. Manufacturers, suppliers, and customers sometimes require data assurance, i.e., transactions are tracked and accessed in a transparent manner (cf. solution for *Traceability and Auditability of Data*) or can be protected by cryptography, which prevents sensitive data from being accessed by non-authorized users (cf. solution for *Data Privacy to Protect Sensitive Information*). Hence, blockchain can provide benefits for data protection through a private network [Anjum et al., 2017], which increases *data transparency* and facilitates *data traceability* in Industry 4.0 production lines.

On the other hand, one significant challenge of integrating blockchain in Industry 4.0 is the substantial energy consumption associated with its operations. The computational power required for maintaining the distributed ledger can lead to increased operational costs and a larger carbon footprint. This energy requirement is particularly problematic for industries aiming to enhance sustainability. Additionally, the high energy demand can limit the scalability and efficiency of blockchain-based solutions in industrial applications [Kolahan et al., 2021] [Alghamdi et al., 2024]; hence, it cannot also guarantee data availability for users, but only a hash pointing to the data [Hawlitschek et al., 2018] and, as a consequence, it cannot solve the drivers *Availability of Data*. Moreover, it cannot also solve *Availability of Physical Devices* and *Compatibility of Data and Services*. Additionally, applying blockchain to Industry 4.0 introduces several security risks and vulnerabilities. While blockchain is praised for its robustness, it is not immune to attacks such as the 51% attack, where a single entity gains majority control and manipulates the ledger. Smart contracts, which automate transactions, can contain coding flaws that hackers exploit, leading to significant losses. Additionally, the integration of blockchain with legacy systems can expose new attack surfaces and compatibility issues. Phishing attacks and private key theft remain persistent threats, jeopardizing the security of blockchain-based Industry 4.0 systems [Manasa and Leo Joseph, 2023].

Considering the results of this work, the adoption of blockchain alone does not cover all requirements for trustworthy interoperability in Industry 4.0 systems. Blockchain must be combined with traditional solutions, in particular, to solve *Authentication to the System*, *Data Access Control*, *Traceability and Auditability of Data*, and *Data Privacy to Protect Sensitive Information*. Such combinations decrease the capacity of blockchain by no longer allowing a totally decentralized system. Instead, a central authority provides the control; hence, entities in the blockchain have the assurance that the data is recorded and tracked by all others, avoiding non-repudiation in the chain. Traditional solutions, such as

federated identities, OAuth 2.0, OpenID, Security Assertion Markup Language (SAML) for authentication and authorization [Suresh et al., 2020], cryptography for data privacy [Fernandez-Carames and Fraga-Lamas, 2019], backup/redundancy/duplication of data [Link et al., 2018, Schulte and Colombo, 2017], and many others, cannot implement trustworthy interoperability in Industry 4.0 systems [Fernandez-Carames and Fraga-Lamas, 2019, Link et al., 2018, Peralta et al., 2019, Schulte and Colombo, 2017]. In this respect, blockchain can complement these solutions by encoding rules in smart contracts, which in turn enable users to transparently access records, ensure the privacy of data through cryptography, and store data and transactions in a distributed ledger. Regarding the question that drove this work (*Do the people intend to use blockchain to assure trustworthy interoperability in Industry 4.0 systems?*), blockchain brings not only benefits but also issues that can compromise the whole cost and performance. Blockchain needs to advance in terms of improving scalability, energy efficiency, and security to effectively support the high demands and complexities of Industry 4.0. This includes developing better consensus mechanisms, enhancing smart contract reliability, and ensuring seamless integration with existing industrial systems. For the while, people intend adopting blockchain but combined with other interoperability solutions.

Finally, surveys such as the one conducted in this work can provide high representativeness, increasing the reliability of the results. The main advantage of surveys is the detailed information obtained from experts and their perception regarding a given topic of interest [Molléri et al., 2016], which, in this case, was the use of blockchain as a solution for trustworthy interoperability in Industry 4.0 systems. Moreover, the analysis of data based on coding can lead to further analysis and broad comprehension of the data considering different experts' opinions [Strauss and Corbin, 1998].

#### 4.2 Threats to Validity

Regarding threats to the validity of this work, the results might have been affected by the following threats: *Construct Validity*: This refers to whether it was able to appropriately collect the measures, i.e., the opinions of the experts interviewed in this study. To minimize this threat, a focused open questionnaire for and high-trained industry professionals were selected. *Internal Validity*: This refers to whether the treatment used in this study made any difference in terms of achieving the results presented in this work. To mitigate this threat, the same documentation of the architecture drivers were delivered for the interviewers. *External Validity*: This refers to the generalization of the results of this study. To minimize this threat it was selected professionals with different backgrounds regarding past projects and academic experience, increasing the possibility of generalizing the results. *Conclusion Validity*: This is related to the ability to draw correct conclusions from the results obtained. To mitigate this threat, a systematic procedure was carried on to analyse the data obtained in the interview.

#### 4.3 Perspectives to Use the Proposed Solutions

While the seven architecture drivers can serve as a set of core *requirements* that together assure trustworthy interoperability in Industry 4.0 systems, the interoperability solutions presented in this work go further by directly supporting *architectural decisions*. This section presents the architectural decisions made using our solutions in a real-world system of a partner of BaSyS 4.0 project. The main feature of this system is the digitalization of an automated transport system to move workpieces throughout the shop floor

[Antonino et al., 2019]. This system includes roller conveyors, shift tables, turntables, many sensors that control speed, temperature, position, and shift of the workpieces, as well as high-level systems, i.e., Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM). It also includes a digital twin, which refers to a virtual copy of the entire platform and provides information, such as status of the transport system occupation, status of work pieces, and localization. All parts of this system are interconnected with each other and interoperate with a number of other systems and users inside and outside the production line, including a *third-party robot*, which was added to the production line to make it more efficient. All end-to-end communication crosses multiple levels of the automation pyramid and is made by a virtual automation bus, which bridges the gaps between different communication protocols.

The novelty of this scenario is the need for trustworthy interoperability of the third-party robot with the entities of the automated transport system. Scenarios like this are becoming common in the Industry 4.0<sup>3</sup>. The third-party robot must be compatible with the transport system to properly exchange data and communicate with all entities of this system. This raises requirements related to trustworthy interoperability: **(i)** only authorized users and entities may be allowed to access the system and its components; **(ii)** every step in the production of workpieces must be tracked and protected, including the step in which the workpieces pass through the third-party robot; **(iii)** devices, data, and systems must be available to complete the production of workpieces; and **(iv)** communication among heterogeneous entities inside and outside the production line, including the third-part robot, must be assured.

The requirement “**(i) only authorized users and entities may be allowed to access the system and its components**” describes the situation in which all users and entities, including the third-party robot, must be identified, authenticated, and authorized to access the product line. To solve this issue, blockchain-based interoperability solutions for the drivers *Authentication to the System* and *Data Access Control* are adopted. A good solution for the authentication to the system of the third-party robot is the use of a pair of keys (public and private encrypted keys) randomly created by the product line company. These keys are used to generate identities and credentials with attributes from the product line company and from the third-party robot. These identities are stored in the blockchain and can be tracked to allow data to be revoked or updated. The smart contract then takes the identifiers from the third-party robot and checks if they exist and are valid in the blockchain. If this is the case, the smart contract allows the authentication; otherwise, the request is rejected and forwarded to the service that manages new entities. The smart contract responsible for adding entities only includes new entities if their data matches the pre-loaded data.

The solution for *Data Access Control* takes as input the identities from the third-party robot that contain the attributes used for gaining authorized access to the system. Access rules are employed using Attribute-Based Access Control (ABAC), which contains rules for entities to access the system. These rules are initially defined by the product line company and implemented in smart contracts that are stored in the blockchain. The product line company update and change their policies over time. All changes are time-stamped and logged in the blockchain, thereby enabling traceability. Blockchain combined with the solutions for the two drivers (*Authentication to the System* and *Data Access Control*) enables entities to have more control over their own identity, more security by validating keys stored in the blockchain, and further auditory in the system

<sup>3</sup> An example of smart manufacturing cooperation can be found at <https://www.boschrexroth.com/en/xccompany/press/index2-31616>

by tracking and monitoring each transaction.

The requirement “**(ii) tracking of the production of workpieces**” describes the situation in which each movement performed by the automated transport system and the third-party robot must be tracked by the product line company. At the same time, any information about both parts (production line company and third-party robot) must be protected, e.g., only the robot (i.e., the company responsible for it) must be able to access the internal controllers and energy power consumption of the robot. The solutions for the drivers *Traceability and Auditability of Data* and *Data Privacy to Protect Sensitive Information* can solve this issue. To track the data, blockchain uses a time stamp to add the time to each block stored in the chain and a hash code value, which uniquely identifies the blocks and their parent blocks. These blocks are linked to each other in a linear and chronological order. Any changes in the data within a block also change the hash of a particular block, making it possible to track any modification in the chain. Due to the limitation of storage space in the blockchain, data from the product line is stored in a central database outside the blockchain. To still enable the tracking of data and check whether data was not changed, a cryptography function can be implemented in a database layer; the result is then compared with the hash stored in the blockchain. Hence, if both cryptography keys are the same, the data has not been changed [Chen et al., 2019]. Regarding the protection of data from the third-party robot, sensitive data is encrypted and separated into segments that are accessible only for authorized users and devices. Blockchain provides provenance services by recording evidence of the data’s originality and the operations in the chain that are also accessible only for authorized users and devices. In summary, blockchain can store each step of the workpieces without the intermediation of third parties. However, its main drawback is the limited storage space and the lack of performance to manage a huge amount of data. For these reasons, cryptography functions and off-chain databases must be combined with blockchain.

This transport system also requires that “**(iii) devices, data, and systems, including the third-party robot, must be available to complete the production of workpieces**”. Solutions for the drivers *Availability of Data* and *Availability of Physical Devices* are suitable in this case. Indeed, blockchain is not a good solution to assure data availability due to performance reasons when a large amount of data is in the chain. Besides, blockchain does not guarantee the availability of devices. In this case, a digital twin of the entire automated transport system is adopted to create a virtualized platform. This digital twin provides unified real-time data access regarding the behavior of real-world environment and entities (i.e., data flow, production machine, operational processing status, functionalities, sensors, and also the third-party robot). This twin supports predictive maintenance to diagnose problems and monitor services to quickly identify and remediate anomalies regarding maintenance, such as rules, events, and triggers, to identify issues. In addition, solutions for data recoverability, including redundancy services, storage in the cloud, and backup servers to recover the last data, must also be implemented. The main drawback of these solutions is the cost to have redundant devices and systems available at any time.

The requirement “**(iv) communication among heterogeneous entities inside and outside the production line**” leads to the need of the third-party robot to be compatible with the automated transport system. The implementation of the solution for the driver *Compatibility of Data and Service* is recommended in this case. Blockchain is indeed not suitable because it does not provide automated or intelligent means to translate and map the data exchanged between third-party robot and automated transport system. Hence, a specific communication channel is necessary in which all entities connected to it are typed and have well-defined properties. Additionally, a service-oriented middleware provides the necessary services to enable the data compatibility according to policies and rules,

besides describing the syntactic and semantic communication protocol for exchanging data. The main drawback of this solution is how to ensure real-time compliance among entities when different semantic and syntactic types are identified and need to be translated and mapped to allow proper compatibility. This real-world case study showed us the viability and value of our interoperability solutions by mainly indicating which issues blockchain can or cannot cover, and where alternative solutions or combined solutions are needed to completely achieve the so required trustworthy interoperability.

## **5 Conclusions**

In the era of the fourth industrial revolution, trustworthy interoperability is becoming crucial for the success of Industry 4.0. At the top of the available solutions, blockchain promises to increase the degree of trust, changing the way transactions are done based on the immutability of records and transparent and trustworthy interactions among users and other entities. In this scenario, seven architecture drivers together with their solutions for achieving trustworthy interoperability in Industry 4.0 systems were presented in this work. Founded on the knowledge and experience of highly trained professionals in Industry 4.0 and blockchain, these solutions can guide architectural decision-making when it comes to whether or not to adopt blockchain and, more importantly, in which situations. We conclude that, in most situations, blockchain needs to be combined with traditional technologies/solutions to fully assure trustworthy interoperability. We also claim this work does not intend to provide the best solutions for trustworthy interoperability in Industry 4.0 systems, but rather in supporting software architects and researchers in making better architectural decisions for their projects.

### **5.1 Limitations and Future Work**

Despite the promising potential of blockchain in Industry 4.0, there are several limitations to its current application. The high energy consumption required for blockchain operations poses significant challenges, particularly in terms of sustainability and operational costs. Furthermore, blockchain's inability to store large quantities of data directly within the chain limits its scalability and efficiency. Another limitation is the maturity of blockchain technology itself; it has yet to demonstrate its full potential and value in a wide range of Industry 4.0 applications.

Future work should focus on addressing these limitations by exploring energy-efficient consensus mechanisms and hybrid solutions that combine blockchain with other technologies. There is also a need for extensive real-world testing in various Industry 4.0 environments to gather quantitative data on performance, security, privacy, and other quality attributes. Additionally, research should continue to investigate the compatibility of blockchain with existing systems and its impact on the maintenance and scalability of Industry 4.0 systems.

Finally, the path to mainstream use of blockchain in Industry 4.0 is still long. It includes its use in several real-world Industry 4.0 systems to mainly get evidence about the impact on quality attributes (by getting quantitative data on, for instance, performance, safety, security, privacy, and others), on the maintenance of these systems and their components, and on the availability of technologies and their compatibility. Hence, another takeaway message of this work is that blockchain must still mature in the Industry 4.0 context to further contribute to realizing the fourth industrial revolution.

## Acknowledgements

This work is supported by FAPESP (Grants: 2016/05919-0, 2018/20882-1, 2017/06195-9, 2019/19730-5, 2023/00488-5), and CNPq (Grant: 313245/2021-5). We would like to thank the experts from Fraunhofer IESE for their valuable feedback regarding Industry 4.0. Our special thanks go to Sonnhild Namingha for her excellent proofreading.

## References

- [Ahram et al., 2017] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., and Amaba, B. (2017). Blockchain technology innovations. In *IEEE TEMSCON*, pages 137–141, Santa Clara, CA, USA.
- [Al-Ali et al., 2018] Al-Ali, R., Heinrich, R., Hnetyuka, P., Juan-Verdejo, A., Seifermann, S., and Walter, M. (2018). Modeling of dynamic trust contracts for industry 4.0 systems. In *ECSA*, pages 45:1–45:4, Madrid, Spain.
- [Alghamdi et al., 2024] Alghamdi, Ali, T., Khalid, Rabiya, Javaid, and Nadeem (2024). A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges. *IEEE Access*, 12:79626–79651.
- [Allian, 2021] Allian, A. P. (2021). *A Trustworthy Interoperability Architecture for Industry 4.0*. Tese de doutorado, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos.
- [Allian et al., 2021] Allian, A. P., Schnicke, F., Antonino, P. O., Rombach, D., and Nakagawa, E. Y. (2021). Architecture drivers for trustworthy interoperability in industry 4.0. *IEEE Systems Journal*, 15(4):5454–5463.
- [Anjum et al., 2017] Anjum, A., Sporny, M., and Sill, A. (2017). Blockchain standards for compliance and trust. *IEEE Cloud Computing*, 4(4):84–90.
- [Antonino et al., 2019] Antonino, P. O., Schnicke, F., Zhang, Z., and Kuhn, T. (2019). Blueprints for architecture drivers and architecture solutions for Industry 4.0 shopfloor applications. In *ECSA*, pages 261–268, Paris, France.
- [Bass et al., 2012] Bass, L., Clements, P., and Kazman, R. (2012). *Software Architecture in Practice*. Addison-Wesley, 3 edition.
- [Bicaku et al., 2017] Bicaku, A., Maksuti, S., Palkovits-Rauter, S., Tauber, M., Matischek, R., Schmittner, C., and Mantas, G. (2017). Towards trustworthy end-to-end communication in industry 4.0. In *IEEE INDIN*, pages 889–896, Emden, Germany.
- [Chen et al., 2019] Chen, J., Lv, Z., and Song, H. (2019). Design of personnel big data management system based on blockchain. *Future Generation Computer Systems*, 101:1122 – 1129.
- [Christidis and Devetsikiotis, 2016] Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303.
- [Fernandez-Carames and Fraga-Lamas, 2019] Fernandez-Carames, T. M. and Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access*, 7:45201–45218.
- [Frailé et al., 2018] Frailé, F., Tagawa, T., Poler, R., and Ortiz, A. (2018). Trustworthy industrial IoT gateways for interoperability platforms and ecosystems. *IEEE Internet of Things Journal*, 5(6):4506–4514.
- [Hawliczek et al., 2018] Hawliczek, F., Notheisen, B., and Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, 29:50–63.



- [Horváth and Szabó, 2019] Horváth, D. and Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? *Technological Forecasting and Social Change*, 146:119–132.
- [ISO/IEC, 2011] ISO/IEC (2011). Systems and software quality requirements and evaluation (SQuaRE) – System and software quality models. 1–41.
- [Javaid et al., 2023] Javaid, M., Haleem, A., and Suman, R. (2023). Digital twin applications toward industry 4: A review. *Cognitive Robotics*, 3:71–92.
- [Kjersgaard and Eriksena, 2018] Kjersgaard, J. and Eriksena, M. (2018). Access control for industry 4.0 initial trust with blockchain. Technical report, Aalborg University, Aalborg, Denmark. <https://projekter.aau.dk/projekter/files/281557079> pp. 1–99.
- [Knodel and Naab, 2016] Knodel, J. and Naab, M. (2016). *Pragmatic Evaluation of Software Architectures*. Springer, Germany.
- [Kolahan et al., 2021] Kolahan, A., Maadi, S. R., Teymouri, Z., and Schenone, C. (2021). Blockchain-based solution for energy demand-side management of residential buildings. *Sustainable Cities and Society*, 75:103316.
- [Kuhn et al., 2018] Kuhn, T., Antonino, P. O., Damm, M., Morgenstern, A., Schulz, D., Ziesche, C., and Müller, T. (2018). Industrie 4.0 virtual automation bus. In *ICSE*, pages 121–122, Gothenburg, Sweden.
- [Kumar et al., 2023] Kumar, L., Ajay, Sharma, R. K., and Parveen (2023). *Smart Manufacturing and Industry 4.0: State-of-the-Art Review*, volume 1. Taylor and Francis.
- [Li and Qiao, 2023] Li, Z. and Qiao, G. (2023). Trust building in cross-border e-commerce: A blockchain-based approach for b2b platform interoperability. pages 246–259.
- [Link et al., 2018] Link, J., Waedt, K., Ben Zid, I., and Lou, X. (2018). Current challenges of the joint consideration of functional safety cyber security, their interoperability and impact on organizations: How to manage rams + s (reliability availability maintainability safety + security). In *ICRMS*, pages 185–191, Shanghai, China.
- [Lu, 2017] Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research. *J. of Industrial Information Integration*, 6:1–10.
- [Manasa and Leo Joseph, 2023] Manasa, K. and Leo Joseph, L. M. I. (2023). *IoT Security Vulnerabilities and Defensive Measures in Industry 4.0*, pages 71–112. Springer Nature Singapore, Singapore.
- [Molléri et al., 2016] Molléri, J. S., Petersen, K., and Mendes, E. (2016). Survey guidelines in software engineering: An annotated review. In *ESEM*, pages 58:1–58:6, Ciudad Real, Spain.
- [Nakamoto, 2009] Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Technical report, Bitcoin.org. <https://bitcoin.org/bitcoin.pdf> pp. 1–9.
- [Pazaitis et al., 2017] Pazaitis, A., Filippi, P. D., and Kostakis, V. (2017). Blockchain and value systems in the sharing economy: The illustrative case of backfeed. *Technological Forecasting and Social Change*, 125:105 – 115.
- [Peralta et al., 2019] Peralta, G., Cid-Fuentes, R. G., Bilbao, J., and Crespo, P. M. (2019). Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges. *Electronics*, 8(827):1–14.
- [Schulte and Colombo, 2017] Schulte, D. and Colombo, A. W. (2017). Rami 4.0 based digitalization of an industrial plate extruder system: Technical and infrastructural challenges. In *IECON*, pages 3506–3511, Beijing, China.
- [S.Perera et al., 2020] S.Perera, S.Nanayakkara, M.Rodrigo, S.Senaratne, and Weinand, R. (2020). Blockchain technology: Is it hype or real in the construction industry? *J. of Industrial Information Integration*, 17:100–125.

[Strauss and Corbin, 1998] Strauss, A. L. and Corbin, J. M. (1998). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, 2nd edition.

[Suresh et al., 2020] Suresh, A., Udendhran, R., and Balamurugan, M. (2020). Integrating IoT and machine learning—the driving force of industry 4.0. In *Internet of Things for Industry 4.0*, pages 219–235. Springer.

[Uhlemann et al., 2017] Uhlemann, T., Lehmann, C., and Steinhilper, R. (2017). The digital twin: Realizing the cyber-physical production system for Industry 4.0. In *CIRP*, volume 61, pages 335–340, Kamakura, Japan.

[ul Ain Arshad et al., 2023] ul Ain Arshad, Q., Khan, W. Z., Azam, F., Khan, M. K., and Yu, H. (2023). Blockchain-based decentralized trust management in iot: systems, requirements and challenges. *Complex Intelligent Systems*, 9:6155–6176.

[Wang et al., 2018] Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., Guo, Y., and Wang, F. (2018). Blockchain-powered parallel healthcare systems based on the acp approach. *IEEE Transactions on Computational Social Systems*, 5(4):942–950.

[Wohlin et al., 2012] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in Software Engineering: An Introduction*. Springer-Verlag, Norwell, USA, 2nd edition.