



Review

Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things

Jinying Li ¹, Ananda Maiti ^{2,*} and Jiangang Fei ¹

¹ Australian Maritime College, University of Tasmania, Newnham, TAS 7248, Australia; jinying.li@utas.edu.au (J.L.); jiangang.fei@utas.edu.au (J.F.)

² School of Information and Communication Technology, University of Tasmania, Newnham, TAS 7248, Australia

* Correspondence: anandamaiti@live.com

Abstract: Regulatory Technology (RegTech) is an emerging set of computing and network-based information systems and practices intended to enhance and improve regulatory compliance processes. Such technologies rely on collecting exclusive information from the environment and humans through automated Internet of Things (IoT) sensors and self-reported data. The key enablers of RegTech are the increased capabilities and reduced cost of IoT and Artificial Intelligence (AI) technologies. This article focuses on a survey of RegTech, highlighting the recent developments in various sectors. This work identifies the characteristics of existing implementations of RegTech applications in the financial industry. It examines the critical features that non-financial industries such as agriculture must address when using such technologies. We investigate the suitability of existing technologies applied in financial sectors to other industries and the potential gaps to be filled between them in terms of designing information systems for regulatory frameworks. This includes identifying specific operational parameters that are key differences between the financial and non-financial sectors that can be supported with IoT and AI technologies. These can be used by both producers of goods and services and *regulators* who need an affordable and efficient supervision method for managing relevant organizations.

Keywords: regulatory technologies; RegTech; internet of things; IIoT; machine learning; artificial intelligence



Citation: Li, J.; Maiti, A.; Fei, J. Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things. *Future Internet* **2023**, *15*, 256. <https://doi.org/10.3390/fi15080256>

Academic Editor: Massimo Cafaro

Received: 25 June 2023

Revised: 16 July 2023

Accepted: 22 July 2023

Published: 30 July 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Regulation Technology, or RegTech, refers to the use of technology to assist organizations in meeting regulatory compliance requirements [1]. RegTech has rapidly gained popularity in the financial industry due to the benefits it offers [2]. The existing financial RegTech solutions have been well-developed with the ability to conduct automated data distribution and regulatory reporting through big data analytics, real-time reporting, risk exposure assessment, potential threat prediction, real-time monitoring, tracking of compliance states and future regulations, and auditing with the adoption of multiple technologies. With the benefits it can bring, RegTech has addressed many issues in financial industries, such as the regulatory interpretation problem, the development of compliant management and business policies, effective and productive regulatory compliance reporting, better performance of data governance and analysis for enterprises, integrated risk management, and automated control throughout the business [3].

RegTech, as large software solutions or complex cyber-physical solutions, comprises two kinds of entities: the *producers* of goods and services and the *regulators/supervisors* responsible for monitoring the producers. Generally, there are a large number of producers who have competing interests and a small number of regulators who must be impartial to all producers but find ways to improve the performance of the industries altogether. This way, supervisors have one-to-many relationships with the producers.

Supervisory technology (SupTech) has also been proposed from the perspective of the supervisory entity [4]. The significantly increased regulations after the last global financial crisis have driven financial institutions like banks to optimize workflow efficiency and challenge the supervisory processes that mainly rely on manual operations [5]. Financial institutions can enormously improve their internal processing speed to comply with policies and regulations by adopting regulatory technologies, which force the corresponding financial regulators or supervisors to take advantage of the supervisory technologies to keep the same pace as required.

RegTech and SupTech have different focuses, whereas the former is concentrated on assisting companies and the latter spotlights enhancing supervision from the supervisor's viewpoint. RegTech is a tool for enterprises to prove what they performed, while SupTech is used to evaluate and verify their behaviors. The key mediator that links them is the data collected and reported by one while being received and verified by the other. SupTech and RegTech belong to the family of compliance technologies as they share the same target of making the products or services qualified to meet compliance requirements and regulations. A failure in either the *reporting of data* or its *verification* will risk the whole compliance process, which must be integrated. In this paper, we refer to a broad scope of RegTech, as shown in Figure 1, when discussing RegTech from the perspective of compliance, which is the destination of all efforts. In short, the rapid development of compliance in all sectors relies on the joint efforts of all stakeholders.

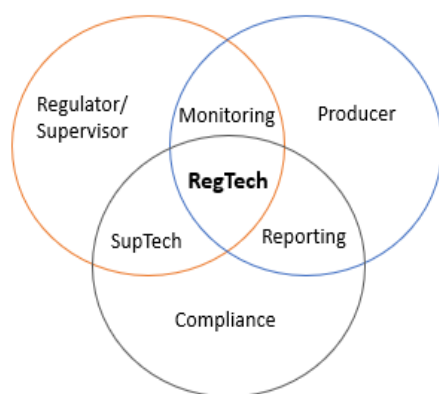


Figure 1. Focus of Broad RegTech.

In addition, by examining the characteristics and challenges of the various industries, this paper recommends an *integrated framework* of RegTech infrastructure that potentially suits *non-financial* enterprises more, strengthening the workflow and importance of data treatment as well as decision-making by taking advantage of various advanced and developed technologies. In discussing the proposed compliance system framework, both supervisory and producer roles are considered. By comparing the features of different sectors in using technologies, the Industrial Internet of Things (IIoT) is identified as one of the key differences between the financial area and the other fields in terms of data collection. In contrast to others, the financial RegTech system has negligible field data to collect.

The remainder of the paper is organized as follows: Section 2 presents the current applications, solutions, and terminologies used in RegTech and related technologies. Section 3 discusses how current RegTech applications work, their features, and standard operating policies. Sections 4 and 5 present a review of how RegTech currently works in financial applications and new approaches taken for other industries. We compare the difference between *financial technologies* and other fields in Section 6 and discuss a potential approach to using the IIoT to seamlessly extend the use of RegTech effectively in industries with considerable human or environmental actions and a substantial number of tangible products in Section 7.

2. Current Supervisory or Regulatory Technologies

2.1. Definition of Several Concepts: Fintech, RegTech, SupTech

Financial Technology (FinTech), Regulatory Technology (RegTech), and Supervisory Technology (SupTech) are all related to the application of technology in the financial industry, but they have distinct focuses and purposes.

2.1.1. FinTech

FinTech was first coined in 1993 [6] and defined by the Financial Stability Board (FSB) as “technology-enabled innovation in financial services” [7]. It refers to using technology to deliver innovative financial products, services, and solutions. It encompasses a wide range of applications, including mobile banking, online payment systems, peer-to-peer lending, robot advisors, digital currencies, digital wallets, etc. For example, a pioneer digital wallet provider, Safaricom, which is also a mobile network provider at the same time, provides M-PESA for clients who can manage money and accounts by themselves within the app [8]. Furthermore, multiple Fintech examples are listed by [9] in both the banking process and the insurance process in terms of provider types (bank, non-bank, insurer, and non-insurer) and interaction types such as B2C, C2C, and B2B, etc. For instance, Fintech products in the B2C business mode are identified, such as video conferencing (HVB, GER) and personal finance management (Mint, US) for Advice services; social media payments (Commonwealth Bank of Australia, AUS) and cryptocurrency (Bitcoin) in Payments services; robot-advisory (UBS, CH) and multi-assets trading (360t, GER) in Investment services; online credit application (Targobank, GER) and Corporate credits (Finpoint, GER) in Financing services; online bank account opening (Fidor Bank, GER) and electronic data safe (SecureSafe, CH) in Cross-process service. FinTech aims to enhance and automate various financial processes, increase accessibility, improve efficiency, and provide new business models. Although the development of fintech has become relatively mature, issues and challenges still exist. The research in [10] identified a series of Fintech challenges in framework and model, regulation and policy, financial literacy, supervision, personal data protection, collaboration, data security, etc. For instance:

- Fintech needs a practical and systematic framework.
- A stable and efficient public infrastructure and trust in the payment system are required for public policies.
- Absolute regulation may not be suitable or effective enough for Fintech.
- Significant data protection issues are caused by the use of big data and new technologies.
- knowledge of the success factors of equity crowdfunding open to non-accredited investors.
- Issues in secure data storage and processing.

2.1.2. RegTech

RegTech was first presented in 2015 by the Financial Conduct Authority (FCA) [11]. As quite a new industry, it is defined as “the use of technologies to solve regulatory and compliance requirements more effectively and efficiently” by the Institute of International Finance (IIF) [12]. RegTech focuses specifically on leveraging technology to address regulatory compliance challenges faced by organizations, particularly in highly regulated industries like finance. It involves using advanced technologies such as AI, machine learning (ML), natural language processing (NLP), and data analytics to streamline compliance processes, automate regulatory reporting, monitor risks, ensure data privacy and security, and manage regulatory changes effectively. RegTech solutions aim to help organizations meet their compliance obligations more efficiently, accurately, and cost-effectively. The basic differences between Fintech and RegTech are shown in Table 1.

Table 1. Comparison of Differences Between FinTech and RegTech.

	FinTech	RegTech
<i>Time Period</i>	1993–Now	2015–Now
<i>Focus</i>	Deliver innovative financial products, services, and solutions	Address regulatory compliance challenges faced by organizations
<i>Aim</i>	Enhance and automate various financial processes, increase accessibility, improve efficiency, and provide new business models.	Help organizations meet their compliance obligations more efficiently, accurately, and cost-effectively.
<i>Sector Scope</i>	Finance only, negligible tangible products involved	Varied and often involve tangible products that generate unique data
<i>Key Technologies</i>	Well-developed e.g., application program interface, artificial intelligence, machine learning, internet of things, big data analytics, distributed ledger technology, smart contracts, cloud computing, cryptography, biometrics	Everything in Fintech, but it is still evolving

The life cycle of products in certain industries, such as electronic products, is becoming shorter and shorter [13]. Companies must constantly design new products to replace old ones to maintain their market share. New products need to be designed to meet changing market demands and comply with regulations. Implementing RegTech ensures that designers are aware of whether the new products are compliant at the design stage so that they can be successfully launched after mass production.

At the same time, competition in new industries is increasing. A larger number of companies are startups developing new products. This creates a risk for consumers as the final products may not be of acceptable quality and/or the companies may not be able to meet the regulatory requirements while maintaining design and functional originality in the long run. Having an in-built RegTech application from the start of product design for such companies can ensure that companies are aware of quality requirements and confidently design and sell their products with high quality assurance. Larger companies, on the other hand, will benefit proportionately less from RegTech for new product design but can still ensure that the production and logistics themselves have acceptable regulatory compliance.

2.1.3. SupTech (RegTech for Supervisors)

The fast development of RegTech presents significant opportunities for supervisory agencies. SupTech refers to the application of technology by regulatory authorities to enhance their supervisory and regulatory functions. It involves the use of data analytics, AI, ML, and other technologies to collect, analyze, and monitor large volumes of data from regulated entities with “a shift away from current approaches based on past data, lengthy on-site inspections, and often delayed supervisory action, towards a pro-active, forward-looking supervision that relies on better data collection and sophisticated data analytics” [12]. SupTech can improve the efficiency and effectiveness of regulatory processes such as risk assessment, market surveillance, fraud detection, and compliance monitoring. It also enables regulators to have a more proactive and data-driven approach to supervision.

While FinTech focuses on innovation in financial products and services, RegTech addresses compliance challenges faced by organizations, and SupTech involves using technology by regulatory bodies to improve their supervisory functions. However, these terms are not mutually exclusive, and there can be overlap and synergy among them as technology continues to shape the financial industry.

2.2. Three Stages of RegTech Development

The development of RegTech has gone through three stages [14]. RegTech 1.0 refers to the early stages of RegTech development when companies started leveraging technology to address regulatory challenges. RegTech solutions primarily focused on automating manual processes, improving data management, and ensuring compliance with existing regulations during this period. It developed risk management practices by introducing new technologies to monitor regulations, risks, or specific processes before the 2008 global crisis [15].

RegTech 2.0 applications, driven by industry and regulators to improve regulatory compliance and efficiency after the global crisis, facilitated companies improvements in consumer protection and supervisory activities [16]. Regulators seek to enhance their capacity to analyze the rising volumes of data generated by institutions required by the post-GFC (global financial crisis) reporting obligations in 2008. It involves more advanced and sophisticated solutions that leverage emerging technologies like artificial intelligence, machine learning, natural language processing, and data analytics. These technologies strengthen risk assessment, real-time monitoring, predictive analytics, and regulatory reporting. It enables financial institutions to control costs and predict risks more effectively, saving regulatory funds and creating new opportunities for the financial industry. It also allows regulators to identify problems using continuous monitoring tools and spend less time conducting compliance breach investigations. Without RegTech, regulators will face significant challenges such as “fundamental information asymmetry, higher regulatory arbitrage, and more serious systemic risks” [17].

In the third phase, more advanced technologies are adopted in applications to foresee risks with predictive algorithms [18] and tools shifting the focus from KYC (Know Your Customer) [19] to KYD (Know Your Data) [20]. This stage involves further advancements in automation, integration, and scalability of RegTech solutions. It incorporates technologies like blockchain, cloud computing, and decentralized applications to address compliance challenges more efficiently and securely.

2.3. Current Development of RegTech and Existing Applications

The high compliance cost accelerates the increasing implementation of various compliance systems with digital technologies such as machine learning, artificial intelligence, big data, and blockchain. According to the statistics of Deloitte in 2023 [21], 485 RegTech companies have exposed detailed information about their businesses covering various sub-sectors such as regulatory reporting, risk management, identity management and control, compliance, and transaction monitoring (see Figure 2). Most RegTech solutions focus on compliance, one of the critical metrics for financial industries.

RegTech Industry Themes

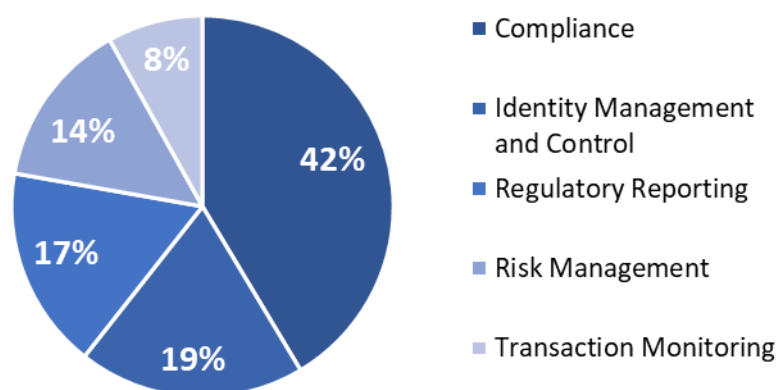


Figure 2. Thematic fields covered by RegTech companies (based on Deloitte, 2023).

2.4. Existing RegTech Applications

Some statistical presentations (Figures 3 and 4, and Table 2) are made based on the information disclosed in the “RegTech100 Report 2023” [22]. It can be concluded (see Figure 3) that most RegTech companies are small, with less than a hundred employees, which indicates that this industry is still in its primary development stage, attracting startups with incredible potential and opportunities. Figure 4 shows that most RegTech enterprises were set up after 2008. The worldwide economic crisis of 2008 forced countries to tighten regulations in various sectors, especially the financial sector, to avoid a similar large-scale economic collapse. Table 2 indicates that RegTech focuses on compliance management, risk management, onboarding identification, regulatory reporting, and transaction monitoring. This finding also matches the data shown in Figure 2. It is worth noting that almost all of the 100 applications are in the financial sector. This indirectly shows that RegTech applications in non-financial sectors still lag behind those in the financial industry. Moreover, there are some interesting new areas developed by some companies, including [22]:

- Digital Transformation and Automation (by “Profinch”)
- Market surveillance (by “Solidus Labs”)
- Web3 scam prevention (by “Solidus Labs”)
- Web3 Intelligence and Forensics (by “Merkle Science”)
- Blockchain Analytics and Investigations (by “Coinfirm”)
- Data Privacy (by “Enveil”)
- Taxation Reporting (by “MAP FinTech”)
- Trade Surveillance (by “MAP FinTech”)
- Staff Compliance (by “U-Reg”)
- Data Exchange (by “U-Reg”)
- Contract Lifecycle Management (by “SignDesk”)
- eSignature (by “SignDesk”)

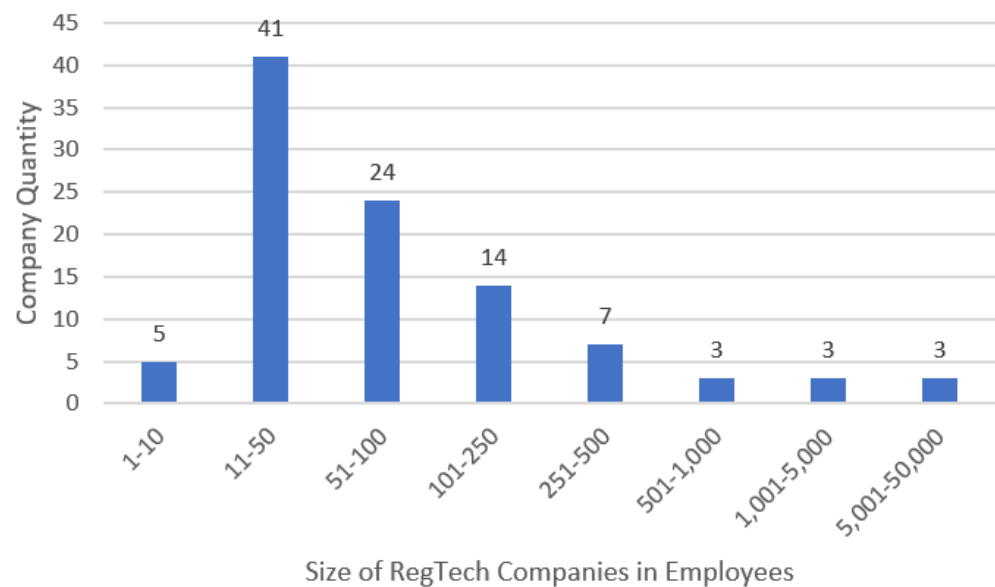


Figure 3. Size of RegTech Companies (Based on “RegTech100-Report-2023” [22]).

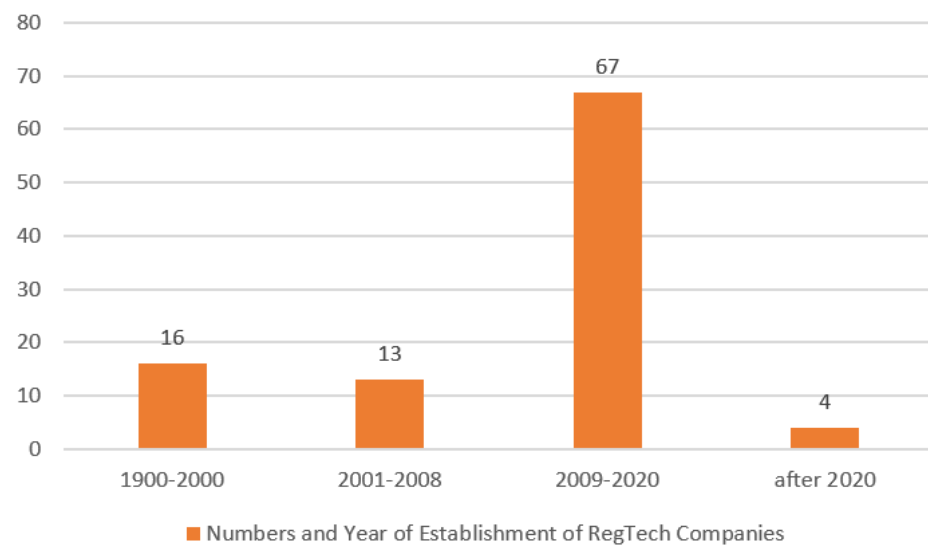


Figure 4. Numbers and Year of Establishment of RegTech Companies (Based on “RegTech100-Report-2023” [22]).

Table 2. Thematic fields covered by the report (Based on “RegTech100-Report-2023” [22]).

Subsector	Times Covered in the Report	Percentage
<i>Risk Management</i>	65	19%
<i>Compliance Management</i>	64	19%
<i>Onboarding Verification</i>	57	17%
<i>Regulatory Reporting</i>	49	14%
<i>Transaction Monitoring</i>	39	12%
<i>Identification/Background checks</i>	22	6%
<i>Cybersecurity/Information Security</i>	16	5%
<i>Communications Monitoring</i>	13	4%
<i>3rd Party Vendor Management</i>	5	1%
<i>Capital Planning/Stress Testing</i>	4	1%
<i>Investigations</i>	3	1%
<i>Regulatory Change Management</i>	2	1%

3. Fundamental Technologies for RegTech

FinTech is a complex, overarching set of technologies for monitoring, supervision, compliance, and ultimate consumer assurance and satisfaction. Key technologies in RegTech include artificial intelligence, machine learning, IoT, big data analytics, cloud computing, Distributed Ledger Technology (DLT), Application Program Interface (API), smart contracts, cryptography, biometrics, etc. The technologies adopted in RegTech are the same as those implemented in FinTech.

3.1. Features

For a cyber-physical solution to be part of RegTech, it has to have some specific features. Some of the critical aspects of RegTech include:

- *Automation:* RegTech solutions often involve the automation of compliance processes, which can help reduce the risk of human error and increase efficiency [14,23–28].

- *Data management*: RegTech solutions typically involve collecting, processing, and analyzing large amounts of data. This requires sophisticated data management tools and techniques like data analytics and machine learning [24,29–32].
- *Risk management*: RegTech solutions can help companies identify and manage compliance risks more effectively. This includes tools for risk assessment, monitoring, and reporting [14,16,23,31,33].
- *Transparency*: RegTech solutions can help improve transparency and accountability by providing real-time access to compliance data and reports [17,24].
- *Collaboration*: RegTech solutions often require collaboration between different stakeholders, such as regulators, industry associations, and technology providers. This can help promote innovation and best practices in regulatory compliance [34].

3.2. Tools

RegTech solutions, which have the above features, are typically composed of independently developed software and hardware tools. RegTech focuses on leveraging technology to improve compliance processes, reduce costs, and enhance the overall effectiveness of regulatory compliance by utilizing a range of technologies to automate, streamline, and enhance compliance processes. It may be noted that the technologies used in RegTech are extremely *mature* and have been in use for decades. This helps the developers integrate such software and hardware to meet the requirements. Some of the key technologies used in RegTech include:

- *AI and Machine Learning*: AI is an advanced technology that can perform tasks in areas that require human intelligence with the implementation and development of computer systems, including a broad range of techniques, algorithms, and methodologies that enable computers to mimic or simulate human intelligence. It involves creating intelligent machines that can perceive, reason, learn, and problem-solve in ways similar to or surpassing human capabilities [35]. For example, the AI-based scoring system is more objective in making credit decisions more precise and reasonable without bias and with brilliant fraud detection, no matter how sophisticated or complex the regulations are [36]. In addition, AI plays an incredible role in complying with the General Data Protection Regulation (GDPR) [37,38], the European Data Protection Law that aims to protect personal information. For instance, *Aigine* offers a tool based on AI to detect personal data from various sources, including structured or unstructured files such as emails or notes, to handle the challenge of unstructured personal data through four stages: filtering, highlighting, assessing, and documenting [16]. Machine learning is a subset of AI that focuses on algorithms and models that enable computers to learn from and make predictions or decisions based on data. It involves training computer systems to automatically improve performance on a specific task through experience and without explicit programming.
- *Blockchain*: Blockchain technology can improve transparency and traceability in compliance processes. For example, it can be used to create tamper-proof records of transactions and improve the audit trail [39–41]. Blockchain technology has several potential applications in RegTech, primarily due to its ability to provide an immutable and transparent record of transactions.
- *Natural Language Processing*: NLP can analyze unstructured data, such as text documents, to identify and flag potential compliance issues [42].
- *Big Data Analytics*: RegTech relies on analyzing large amounts of data to identify patterns, trends, and anomalies that may indicate compliance risks [2,43].
- *Cloud Computing*: Cloud computing can be used to store and process large amounts of data in a cost-effective and scalable way [44–46].
- *Robotic Process Automation (RPA)*: RPA can be used to automate routine compliance tasks, such as data entry and reconciliation, to improve efficiency and reduce errors [47–49].

- *Internet of Things*: IoT devices can be used to collect data from physical assets and locations, such as factories or supply-chain nodes [50–52], to monitor compliance and identify potential risks.

Adopting these technologies can automate compliance processes, such as monitoring and reporting, by analyzing large volumes of data in real-time [46,47]. They are constantly evolving as new solutions are developed to meet the specific needs of different industries and regulatory requirements.

3.3. Policies and Standard Operating Procedures

Over time, RegTech, particularly FinTech, has developed several well-known and tested policies and standard operating procedures. These are mainly aimed at acquiring the correct data from the correct source in a timely manner. They are based on the tools mentioned above. Here are some ways in which blockchain can be used in RegTech:

- *Know Your Customer*: Blockchain can be used to create a decentralized and secure identity verification system that allows customers to prove their identity without the need for intermediaries. This can streamline the KYC process for financial institutions while maintaining data privacy and security [53,54].
- *Regulatory Reporting*: Blockchain can be used to create a secure and transparent audit trail of regulatory reports, making it easier for regulators to monitor compliance and identify potential issues. This can potentially reduce the burden of regulatory reporting for financial institutions and improve the overall quality of the data [54].
- *Supply chain compliance*: Blockchain can be used to create a secure and transparent record of transactions in supply chains, enabling companies to track the movement of goods and ensure compliance with regulations. This can aid in reducing the risk of fraud and improving the overall efficiency of supply-chain management [55].
- *Smart contracts*: Blockchain can be used to automate compliance processes through the use of smart contracts, which are self-executing contracts that automatically enforce the terms of an agreement. This lowers the impact of errors and improves the overall efficiency of compliance processes [56].

3.4. Applications

The combination of blockchain and IoT can provide a powerful solution for compliance management, enabling companies to monitor and enforce compliance requirements securely, transparently, and efficiently. Some ways in which blockchain and IoT can be used in traceability and quality assurance are:

- *Supply chain management*: IoT devices can be used to collect data from physical assets and locations, such as factories or supply-chain nodes. These data can be stored on a blockchain, creating a secure and transparent record of transactions [57]. This can help to ensure compliance with regulations, such as food safety regulations, by providing an auditable trail of the movement of goods and the conditions under which they were transported.
- *Anti-Money Laundering (AML)*: Blockchain can be used to create a secure and tamper-proof record of transactions, making it easier to detect and prevent money laundering and other financial crimes. This reduces the risk of fraud and increases transparency in the financial system [53].
- *Asset tracking and management*: IoT devices can be used to track and monitor the condition of assets, such as machinery or vehicles [58–60]. Similar to the supply chain. These data can be stored on a distributed database, creating a reliable and quickly accessible record of the asset's history. This can help to ensure compliance with regulations, such as maintenance schedules or environmental standards, by providing an auditable trail of the asset's use and maintenance.
- *Identity verification*: Blockchain can be used to create a decentralized and secure identity verification system. IoT devices can be used to collect biometric data, such as fingerprints [61] or facial recognition, to verify the identity of individuals. This can

help streamline financial institutions' KYC processes and reduce the risk of identity theft or fraud.

- *Product tracking and monitoring:* IoT devices can be used to monitor the quality of products in real-time, such as temperature, humidity [62,63], or vibration. These data can also be stored on a blockchain, creating a record of the product's history. This can help identify quality issues and ensure that products meet the required quality standards.
- *Quality control and testing:* IoT devices can collect data for quality control [64] and testing processes, such as test results or inspection data, to monitor compliance with these requirements. Based on this, it can trigger automatic actions if required. This can help identify quality issues and improve the overall quality of products.

3.5. RegTech and TRL

RegTech can be used to determine the *Technology Readiness Level* (TRL) [65] in certain contexts. TRL measures how mature a technology is and its readiness for deployment [65]. It is often used in research and development projects to assess the progress of technology development and identify areas for further investment and improvement. RegTech can be used to automate the collection, analysis, and reporting of data related to TRL [65]. For example, RegTech solutions can be used to collect data on the performance and reliability of a technology, such as its ability to meet regulatory requirements, the quality of its data output, or its ability to integrate with other systems. These data can be analyzed to determine the technology's TRL and identify areas for improvement.

RegTech can also be used to automate compliance processes related to TRL. RegTech solutions can be used to ensure that the development of a technology complies with regulatory requirements and standards for safety, performance, and quality. RegTech can provide a more efficient and accurate way to determine TRL, enabling organizations to make better-informed decisions about developing and deploying new technologies.

4. RegTech in Financial Sector

The mortgage industry turned to a virtual approach during the pandemic period to serve clients by introducing digital mortgage companies and application processes, which brought back mortgage fraud and synthetic identity fraud [66]. According to the report by McKinsey [67], synthetic identity fraud contributed to 10–15% of lender losses in the UK. And the 2020 Q3 ACES Quality Control Industry Trends Report [68] indicated that the error rate of the industry reached the highest percentage (2.34%) since 2016. Hence, lenders must mitigate risks by introducing risk reduction and credit monitoring tools. RegTech can provide an easier solution for them to achieve this. Further, the latest *Anti Money Laundering* (AML) rules require businesses to use electronic verification instead of manual identity checks to keep pace with the increasing sophistication of fake identities and financial documentation. Electronic RegTech solutions help lenders check these faster and improve the application process timeline, which is a key sore point for applicants. This not only makes the companies comply with the ever-changing regulatory landscape cost-effectively but also boosts customer retention and competitiveness.

4.1. Benefits of the Current Compliance Application in Financial Sectors

RegTech offers numerous benefits to the financial industry, assisting financial institutions in streamlining their regulatory compliance processes and improving overall regulatory effectiveness. Some key benefits of RegTech in the financial industry include:

- *Compliance Efficiency:* With the help of RegTech applications, the compliance processes can be automated, greatly reducing manual effort and time to save costs and improve productivity in compliance operations [69]. In addition, useful tools enable financial entities to keep good auditable records of compliance activities by maintaining a robust audit trail [25] and capturing all relevant actions during the compliance process, which provides clear evidence for future investigations. Moreover, financial regulations keep

changing [16], which not only costs entities time to keep pace with them but may also cause potential non-compliance risks without good regulatory change management. RegTech solutions can automatically monitor and interpret regulatory changes and provide timely updates and alerts so that organizations can stay informed and adapt their compliance processes and policies accordingly. For example, the NLP can help users interpret the regulatory rules and identify any changes or updates; Robotic Process Automation can produce the regulatory reports automatically; distributed ledger technology can verify and check the authentication of the report; and the programming interface will enable the report to be submitted directly to regulators or supervisors [70]. The combination of various digital technologies can have a greater effect on the compliance process.

- *Transparency and Regulatory Collaboration:* RegTech can handle real-time monitoring [70] and internal and external reporting. On the one hand, by analyzing real-time data such as transactions, market activities, and regulatory changes, financial institutions can identify potential compliance issues or suspicious transactions and take appropriate action immediately against any potential risks. In addition, entities can identify and assess risks via real-time monitoring, detect patterns, and generate insights that support risk mitigation strategies by analyzing large volumes of data. On the other hand, RegTech also facilitates automated, accurate, and timely reporting to regulators or supervisors, contributing to transparency and accountability [32] and building trust between entities and supervisors. As a result, better collaboration and communication between two parties can be facilitated by providing a standardized platform with automated reporting, which can streamline the exchange of information, reduce duplication of efforts, and foster a more efficient and transparent relationship.
- *Customer Due Diligence:* Client background checks are crucial in the financial industry to avoid causing financial crimes such as money laundering. As criminals become more technologically advanced, it presents unprecedented challenges for financial service providers. Hence, customer due diligence processes such as Know Your Customer (KYC) and Anti-Money Laundering (AML) checks are inevitable [71]. By automating data collection, verification, and risk assessment, the applied RegTech can make more accurate analyses and judgments in due diligence procedures as well as streamline customer onboarding with reduced manual errors [71], establishing a good reputation in customer service.
- *Data Integrity and Security:* RegTech solutions often incorporate robust data management and security features, including encryption, access controls, audit trails, and other security measures to protect sensitive information and prevent data breaches [72], which helps financial companies ensure the integrity, confidentiality, and accuracy of data used in regulatory compliance.

RegTech offers significant advantages to the financial industry, allowing financial institutions to effectively navigate complex regulatory landscapes, enhance compliance efficiency, and mitigate risks. These benefits ultimately contribute to a more resilient and sustainable financial ecosystem.

4.2. Shortcomings of the Current Compliance Application in Financial Sectors

Limitations or challenges still exist despite the successful development of RegTech. It is suggested by Teichmann and Boticiu [14] that the following three challenges deserve attention:

- the inconsistent and complicated national and international regulatory landscape,
- cybersecurity issues caused by the exposure of internet vulnerabilities [73], and
- the difficult integration with new technologies for the legacy systems that require a lot of modifications [74].

Moreover, a wide variety of applications may create selection challenges for enterprises. It is expected that future RegTech applications can upgrade compliance processes to be more streamlined with more automation, standardization, and simplified interpre-

tation. But standardization is only possible with the long-term involvement of relevant governance bodies.

For short-term or mid-term solutions, there are limited options. The industry can proceed by:

- establishing a collaborative relationship among financial institutions, technology providers, and regulatory bodies to identify the specific challenges faced by compliance applications.
- creating regulatory sandboxes or innovation hubs that allow for better understanding of the limitations and challenges while providing an opportunity to refine and improve them based on real-world feedback.
- issuing clear guidance on compliance requirements and expectations, taking technological advancements into account.
- initiating pilot programs or demonstrations to showcase the effectiveness of compliance applications.
- regularly monitoring the evolution of compliance applications and providing timely updates to regulations and compliance requirements.

It is expected that most of these steps will be automated and data-reliant in future RegTech software solutions.

5. RegTech Applications in Non-Financial Sectors

RegTech was initially adopted in the financial industry, but it is gaining more and more attention in other sectors. RegTech aims to identify fraud in all industries. Increasing fraud occurrences pose significant challenges to regulators' authority and cause serious consequences or threats to consumers' safety. Fraud may result in the loss of capital in the financial sector and the loss of lives in non-financial industries. Hence, fraud detection and risk prediction are even more important in non-financial sectors.

5.1. Agriculture Sector

The agriculture industry faces many regulatory challenges, including environmental regulations, food safety regulations, and supply-chain transparency requirements. RegTech solutions can help companies comply with these regulations and improve their overall operations. Effective RegTech solutions will likely improve compliance with agricultural regulations by automating and streamlining processes for accurate data collection, analysis, and real-time reporting. For example, RegTech can monitor compliance with food safety regulations, track the use of pesticides and other chemicals, ensure that farmers meet environmental standards, improve traceability and transparency in the supply chain, and enhance risk management. The adoption of blockchain technology can track the movement of agricultural products from farm to market, providing a tamper-proof record of the products' journeys and ensuring compliance with regulations related to food safety [75].

A good example is *Aglive*, a cloud-based platform that provides traceability and compliance solutions for the agriculture sector. It allows farmers and producers to record and manage data related to animal health, welfare, and movements, as well as compliance with regulations around food safety and animal welfare. Similarly, *TR4 Hub* is a traceability platform developed specifically for the banana industry in Australia, allowing producers to track the movement of bananas from farms to retailers and enabling rapid response to any outbreaks of banana plant disease. Another traceability platform is *FreshChain*, which uses blockchain technology to track the movement of fresh produce through the supply chain. It allows producers to record and manage data related to product quality, safety, and compliance. Other traceability platform solutions perform similar functions and advantages, such as *BeefChain*, *Farmless*, *Livestock Data Link*, *AgriChain*, *HarvestMark*, *AgriLedger*, *OriginTrail*, *Farmforce*, *SmartAgriHubs*, *AgriVi*, *Farmbook*, *AgUnity*, *MUIIS*, *Bext360* (US), *AgroTrace* (Philippines), *AgriChain* (EU), *FieldSense* (EU), *Smartbow* (EU, livestock), etc.

All the above solutions address, to varying degrees, parts of or the whole stages of supply-chain tracking for agricultural products by adopting technologies such as blockchain, cloud computing, IoT, big data analysis, or tangible identification solutions such as QR codes or RFID. The digitalization of agricultural supply-chain tracking has gained varying degrees of popularity and application. Some of these solutions focus on the internal data management of farms or the tracking record from the perspective of end consumers for provenance, and others focus on the traceability of the whole supply chain from farm to fork to comply with regulations. But this is not enough for a mature application that can satisfy all stakeholders in agriculture supply-chain tracking. A few applications have added the timely supervision of regulators to the whole picture. There might be data available for supervisors to view, but few solutions have an architecture design with direct intervention mechanisms or real-time action windows open to them. In the context of international market expansion of agricultural products, given the complexity, diversity, and variability of international laws and regulations, future applications need to value the in-system supervision of the regulators.

RegTech in agriculture is still in its early stages of development, and several challenges need to be addressed for its widespread adoption.

1. *Limited data availability:* RegTech solutions rely on data to provide insights and automate compliance processes. However, data can be limited or fragmented in agriculture, making it difficult to develop effective RegTech solutions. For example, data on weather patterns, soil conditions, and crop yields may be available from different sources, making it challenging to integrate and analyze the data [76,77]. Weather pattern data may be obtained from local weather stations, while soil condition data is collected from soil testing laboratories, and remote sensing techniques capture information about soil composition. Additionally, crop yield data are sourced from agricultural surveys, farm management systems, and market reports. These diverse sources lead to data fragmentation, where information is scattered across multiple platforms, formats, and sources.
2. *High implementation costs:* Implementing RegTech solutions can be expensive and may be prohibitive for smaller farms. To gather the required data, the farm would need to invest in various sensors, which can be quite costly considering the scale of deployment across different fields or crops. In addition, acquiring and maintaining the necessary hardware, software, and connectivity infrastructure can add to the expenses. Moreover, collecting and analyzing the data may involve utilizing cloud-based storage, advanced analytics platforms, and data integration tools. These technologies often come with subscription fees or licensing costs, which can be prohibitive for smaller farms with limited budgets. Furthermore, farmers or farm managers may need training to operate the sensors, interpret the data, and make informed decisions based on the insights obtained, which requires additional expenses for professional training or hiring consultants. Lastly, sensors may require software updates and potential system repairs that incur additional costs. This can limit the adoption of RegTech solutions, particularly in developing countries or regions where agriculture is a significant source of income [78].
3. *Lack of standardization:* Agriculture is a complex industry, with different crops, farming practices, and regulations varying by region and country. Different crops have unique growth requirements, susceptibility to pests and diseases, and market demands. For example, if there are two regions and region A specializes in wheat production and follows conventional farming practices, the local regulatory authority requires farmers to adhere to specific guidelines for pesticide usage, irrigation methods, and soil conservation. In contrast, if region B focuses on vineyard cultivation and practices organic farming methods, the regulatory framework in this region places strong emphasis on organic certification, water conservation, and biodiversity protection. Farms in Region B need to keep detailed records of crop inputs, such as organic fertilizers, compost, and pest control products, to secure organic certification. This

can make it challenging to develop RegTech solutions that are widely applicable and can be scaled across different contexts [77,79].

4. *Limited understanding and awareness:* Many farmers and agricultural stakeholders may not be aware of the potential benefits of RegTech solutions [76,78] or may lack the technical expertise to implement and use them effectively [78,80]. A small family-owned farm in a rural area with tight budgets may be reluctant to allocate resources towards technology adoption if farmers are not aware of the potential return on investment or long-term benefits. The farmers have been using traditional farming practices for generations and are not familiar with modern technologies or digital solutions. They may also lack the necessary skills and knowledge to set up and operate the required hardware, software, and connectivity infrastructure and struggle with data collection, analysis, and interpretation. This can limit the adoption and impact of RegTech solutions in agriculture [81].
5. *Regulatory barriers:* In some cases, regulations may not allow the use of certain technologies or may require manual processes that cannot be automated with RegTech solutions. For example, drones equipped with advanced imaging sensors and artificial intelligence algorithms can efficiently identify pest infestations, monitor crop health, and optimize irrigation practices. However, due to concerns related to airspace regulations, privacy, or safety, the regulatory framework in a particular region may prohibit or limit the use of drones in agriculture. In addition, some agricultural regulations may require manual processes or paper-based record-keeping for compliance purposes. For instance, a regulation might require farmers to manually record the use of certain pesticides or the application of specific fertilizers, which poses challenges when integrating RegTech solutions that automate data collection, analysis, and reporting. This can limit the potential impact of RegTech in agriculture.

5.2. Manufacturing

Manufacturing companies face a range of regulatory requirements, such as environmental regulations, health and safety standards, labor laws, and product quality standards. The compliance cost is a heavy burden for manufacturers. The World Bank reports that about 8% of the gross national product is spent on regulatory compliance annually [82]. The National Association of Manufacturers (NAM) also reports that the U.S. company spent \$9991 on average per employee per year to comply with federal regulations in the USA. But it cost each manufacturer almost \$19,654, which is two times the average, and the smaller producers' costs could be close to \$35,000, which is almost three times more than the average [83]. Fulfilling compliance requirements is expensive for manufacturers, who will pay more if they fail to meet regulatory guidelines, as non-compliance can cost up to \$14.82 million for manufacturers, according to the study conducted by the Ponemon Institute [84]. With the help of RegTech, which can facilitate the automation and precise interpretation of ever-changing compliance guidelines, manufacturers can increase efficiency in the compliance process and reduce labor costs significantly. They can automate data collection, analysis, and reporting processes, enabling real-time monitoring of compliance status and facilitating timely corrective actions.

Moreover, workplace injuries are another high cost for manufacturers related to occupational health and safety compliance. RegTech can minimize this loss by specializing in risk management that monitors employee behavior and workplace conditions. Potential dangers can be identified by analyzing incident data to improve processing procedures by reducing weak points. For example, manufacturers can apply pressure-sensitive tags to "circumvent recurring blockage of their stamping equipment by examining the data sets presented for embossing" [82].

In addition, manufacturers must adhere to stringent regulations and standards to ensure product safety and quality. RegTech solutions can automate product testing, quality control, and traceability processes. By integrating data from various sources, such as IoT devices or quality management systems, RegTech tools provide real-time visibility

into production processes and enable proactive measures to maintain compliance with relevant standards.

Moreover, manufacturers can minimize the potential impact on their operations and keep a good reputation through supply-chain compliance management and product quality control by proactively addressing compliance risks. Manufacturers often have complex supply chains involving multiple suppliers and subcontractors. Effective supply-chain management directly impacts the manufacturer's efficiency in production. RegTech solutions can assist them in automating due diligence processes and monitoring suppliers' compliance status. By enhancing transparency and traceability, RegTech enables manufacturers to ensure that their suppliers meet regulatory requirements, such as ethical sourcing or product safety standards.

By taking advantage of technology and automation, RegTech solutions enable manufacturers to navigate complex regulatory landscapes, enhance compliance efficiency, and mitigate compliance risks, ultimately contributing to improved operations, reduced costs, and increased regulatory effectiveness.

5.3. Healthcare

The healthcare industry is the most attractive target for cyberattacks because healthcare records contain sensitive personal data and important financial information that are valuable resources for criminals. In addition, during the pandemic, more healthcare professionals worked remotely, which further increased the vulnerability of cybersecurity. Moreover, healthcare workers' education and awareness of cybersecurity risks need to be improved. These issues can be solved by implementing standardized security protocols such as "Single Sign-On Software", "risk-based authentication policies, and annual cybersecurity training for healthcare professionals" [85].

In addition, the healthcare fraud issue is regarded as a top priority by The National Money Laundering Risk Assessment (NMLRA) [86]. According to this report, 345 people were charged in healthcare fraud schemes involving over \$6 billion in 2020, the largest fraud in history. Applications of RegTech such as AML, KYC, and anti-fraud detection can be adopted in the risk prediction of Medicare fraud. In addition, RegTech services provided by *Abide* RegTech and *6Clicks* can track current and upcoming regulations for the medical industry [85]. In addition, the highly digital transformation of the healthcare industry has also brought new issues, such as data privacy. To address this issue, Theta Lake uses AI to identify risks such as video and voice content by implementing a data privacy impact assessment, which can standardize health data protection [85].

5.4. Logistics

RegTech solutions can enhance tracking and traceability capabilities in logistics operations. Through technologies such as RFID (Radio Frequency Identification) and IoT, RegTech tools enable real-time visibility of shipments, inventory, and transportation conditions. Logistics companies must comply with regulations governing transport operations and driver safety. RegTech solutions can automate driver compliance checks, including driver qualifications, licensing, hours of service, and vehicle maintenance records.

5.5. International Trade and Business

RegTech is crucial in facilitating compliance and streamlining international trade and business processes. It can benefit international trade and business in the following aspects:

- *Trade Compliance Automation:* The complex international political environment brings significant regulatory challenges to cross-border trades [87] that need to comply with regulations imposed by governments and international bodies. Providing real-time monitoring and screening of parties involved in trade transactions against sanctioned lists or restricted entities can ensure compliance with export control requirements, mitigate reputational risks, and help businesses avoid penalties. The trade compliance processes can be automated by digitizing documentation, automating data collec-

tion, and providing real-time updates on regulatory changes to achieve a simplified compliance process and smoother cross-border transactions with reduced error.

- *Cross-Border Payments*: The settlement of payments for international trade carries a high risk. In international trade, the consignee often refuses to pay the final payment for various reasons. This problem can be avoided to a certain extent by using smart contracts [88].
- *Efficient Documentation Management*: International trade involves extensive documentation, including contracts, invoices, bills of lading, and certificates of origin. Proper digitalization reduces reliance on physical paperwork [89], improves accessibility, and facilitates efficient sharing of documents with trading partners and regulatory authorities. It also ensures proper record-keeping, easy retrieval, and compliance with document retention requirements. For instance, RegTech can assist in classifying products more accurately in terms of their harmonized system (HS) codes and automatically calculating customs duties to minimize errors, improve efficiency, and ensure compliance with tariff regulations.

Implementing RegTech in international trade and business helps businesses navigate complex regulatory landscapes, streamline compliance processes, mitigate risks, and enhance efficiency, facilitating smoother international trade transactions and overall business success in the global marketplace.

5.6. Challenges in Non-Financial Sectors

Based on the above investigation of RegTech applications, some common challenges associated with a range of non-financial industry sectors are identified:

- *Lack of Customization*: Existing RegTech applications, derived from the financial industry, may not be readily applicable to the wide range of non-financial regulations to cater for the specific compliance needs of different sectors, which will create gaps in compliance coverage and hinder effective regulatory compliance in specific industries.
- *Complex and Evolving Regulatory Landscape*: Keeping pace with the evolving regulatory landscape is challenging as regulations of various industries can be complex and rapidly changing, which leads to difficulties in staying up to date with regulatory changes, gaps in compliance coverage, and potential non-compliance risks.
- *Limited Adoption and Awareness*: RegTech adoption in non-financial sectors is relatively low, and the limited awareness of available RegTech solutions may result in a lack of understanding about these technologies' potential benefits and limitations.
- *Integration Challenges*: Many non-financial organizations have legacy systems that were not designed to accommodate modern RegTech solutions. Integrating new RegTech applications with existing infrastructure can be challenging. It requires additional investments in technology and staff training and may also cause disruptions during implementation. In addition, disparate systems with different data sources collected from non-financial entities are not easily integrated, which presents great challenges to the existing applications in effectively aggregating, normalizing, and analyzing data.
- *Standardization*: The implementation of RegTech in the financial sector is comparatively advanced and well-established, with hundreds of applications providing relatively complete functional modules and practical technical applications. However, it is still in the initial application stage in other sectors, such as agriculture, the food industry, supply-chain management, etc. No matter how developed they are, on-shelf applications lack uniformity and standardization.

To address these challenges, RegTech solution providers must recognize non-financial sectors' diverse compliance requirements and develop customized solutions. Collaboration between RegTech providers, regulators or supervisors, regulatory producers, and industry stakeholders can help foster innovation and awareness of effective compliance solutions. Additionally, solution providers should consider the development based on specific industry requirements and seek integration strategies that ensure seamless data flow and interoperability with existing systems.

6. Comparing FinTech and Different RegTech

In this section, we discuss how different non-financial sectors differ but can still benefit from or evolve to improve compliance and monitoring. Although RegTech is derived from the financial sector and has made good progress in that field, the development in other sectors is still in its infancy. The application of RegTech in the non-financial sectors has much to learn from the valuable experience of the financial sector. It is also important to note that there are many differences in the non-financial sectors in terms of product or service features, business focus, compliance focus, value chain, and scope of compliance. The following aspects have been identified that deserve further attention in future framework designs, as shown in Table 3:

Table 3. Comparison of Differences Between Financial Industry and Non-Financial Industries.

Aspects\Sectors	Finance	Agriculture	Manufacturing	Food Services	International Trade
<i>Aim of Compliance</i>	Financial crime	Product Safety	Product Safety	Food Safety	Product Safety
<i>Physical Safety of Humans</i>	N/A	YES	YES	YES	YES
<i>Business Focus</i>	Transaction	Farming/ Planting	Processing; SCM	Processing; SCM	Processing; SCM; Logistics; Transaction
<i>Value Chain</i>	Simple	Simple	Complex	Complex	Complex
<i>Business Procedures Complexity</i>	Low	Medium	High	Medium	High
<i>Industrial Equipment</i>	N/A	Medium	High	Medium	High
<i>Logistics</i>	No	YES	YES	YES	YES
<i>Physical Environment</i>	Not necessary	Necessary	Necessary	Necessary	Necessary
<i>Field Data</i>	No	YES	YES	YES	YES
<i>Network Dependency</i>	High	Low	Low	Low	Medium

6.1. Different Business Focuses

All actions in the financial sector revolve around trading. It includes the object of the transaction, the instruments used for the transaction, the medium, and how the transaction is completed. In the current highly digital age, most transactions are performed through electronic devices and networks. This feature dictates that all transactions are traceable and that any transactional behavior leaves a footprint online. The application of regulatory technology tools has made tracking and monitoring transactions easy, and data access is relatively simple. The supervision procedures also focus on transaction-related activities.

In the non-financial sector, transactions are only a small part of the value chain. The core lies in the products or services and the humans who operate the business. The manufacturing entities aim to sell as many products as possible. But the products can only be sold consistently if they meet the buyer's quality standards and the relevant regulatory requirements, such as Work Health and Safety (WHS), industry certification, government regulations, and even the regulations of the target markets for the exported products. Failure to meet compliance requirements at any point or in any way could result in the product not being sold. It is particularly high-risk for sellers in international trade. Regulators will issue industrial certificates to those who comply with the regulations. The company must obtain these certificates to sell its products properly.

6.2. Different Compliance Focus

Compliance in the financial industry mainly lies in the legitimacy of the sources, paths, and destinations of transactions as well as the identities of clients. However, compliance in other fields, such as manufacturing, is quite different. Producers may do anything to

obtain regulatory certificates, such as falsifying data. The role of regulation is to avoid these irregularities and the potentially serious consequences they may entail. Furthermore, compliance involves more factors in the latter, including raw materials, production processes, production equipment, the environment, and the relevant production operators that must all comply with the laws and regulations.

In the manufacturing sector, each qualified product needs to be processed through a series of processing operations, from the raw material's processing to the assembly of the finished product. These procedures may involve one or multiple manufacturers depending on the product type, and each manufacturer has different management abilities and processing standards as per the industrial requirements or buyer's standards. The compliance of the finished product depends on the overall compliance of the whole supply chain. It includes not only the processing procedures from upstream to downstream but also the laborers hired by different entities, who may vary in enterprise culture, expertise in compliance, and the relevant technological equipment. All these will positively or negatively affect the ultimate compliance degree of the finished product.

6.3. Different Audit Sequences

In finance, it may be possible to do something first and audit later. It means that the regulator will come to audit the legality of the transaction after it has been completed, while in the non-financial sectors, the relevant certification must be obtained before the product or service can be sold on the shelves.

6.4. Value Chain

Compliance is more complicated in non-financial sectors due to the longer value chain, the complicated processing procedures, and the variety of environments and business focuses (see Table 2). For example, the manufacturing industry focuses on the processing of materials and supply-chain management (SCM). As the products are involved in multiple manufacturing processes, compliance must be achieved within the whole supply chain, from the raw material to the final finished product. Outsourcing materials may bring risks without proper supplier management. Hence, manufacturers need to play a supervisor's role before products reach consumers, and each process is as important as the final one.

Furthermore, several features exist in the non-financial sector but are absent in finance:

- *Industrial Equipment*: Industrial equipment is unnecessary in the financial industry, but it is indispensable in most physical industries.
- *Physical Safety of Humans*: Compliance in the financial sector is less concerned with people's physical health and safety, which is considered as important as product quality in non-financial fields due to its huge impact.
- *Field Data*: There is no field data in finance. However, it is a critical source of information for non-financial entities. Collecting field data is more challenging because of extreme weather and human interference.
- *Logistics*: Logistics is only available in non-financial industries to contribute to the value-adding process. Thus, logistics-relevant activities are also within the scope of compliance, such as the truck driver's behavior, the internal environment of containers in transportation, etc.

6.5. Virtual vs. Physical World

The financial industry relies on the internet network, and most business activities are conducted online in cyberspace. On the contrary, the businesses of non-financial sectors are conducted in the physical environment. In contrast, the activities also need the internet for communication, documentation, and payment, but most value-adding processes take place offline, in the field, in workshops, or at other workplaces. The corresponding compliance scope of products or services covers humans, machines, materials, procedures, environments, and even supply-chain management.

6.6. Human Roles

The activity is more of a peer-to-peer mode in the financial field. However, the roles of humans play differently in the non-financial industries, and it is difficult to avoid human interference in real-world activities that affect the various perspectives in the compliance process, which causes compliance issues. For example, humans operate industrial equipment, do quality control, inspections, and packaging, do on-site audits, and may have close contact with products during processing. All these processes that require human operation or control can create compliance issues, as the complexities of human nature can have positive or negative effects and outcomes that are hard to control with digital devices.

The supervision of non-financial sectors involves more aspects such as equipment, environment, humans, materials, and even the policies of entities. By comparison, the supervision in finance focuses on the data, which is in large volume and might be available online in most cases. But supervision in other industries includes both online and offline activities, which make it more difficult to collect and integrate data.

7. RegTech and Industrial Internet of Things

So far, we have discussed the current status of RegTech developments, their underlying computing technologies, and how RegTech functions in different industries. In this section, we present a possible future direction for RegTech. We present the basic components of RegTech in terms of how data propagate through various phases of a RegTech solution and then discuss the potential issues and usability of IIoT in RegTech.

7.1. The Core of RegTech

The data-relevant treatment is the focal objective of the entire regulation compliance process, which involves data from both regulators and regulated entities. Due to the existing legacy systems, the integration of varying user systems is the key to large-scale RegTech adoption. Such integration must be low-cost and involve minimal disruptions to operations and existing practices. RegTech is expected to gain unprecedented popularity if its implementation can achieve this goal with the lowest cost in terms of time and monetary investment and, at the same time, help companies operate and run more efficiently under the premise of protecting enterprise data. It is suggested that the general activities of RegTech are data collection, data processing, data analysis, and data visualization [5].

- *Data collection* is a continuous, repeating process that involves quality management internally and regulatory compliance externally. Considering the privacy of data and the protection of organizations' interests, a screener is necessary to be designed in the data collection process to make sure that only the compliance-related required data are retrieved. In the traditional regulation audit process, regulation-related data are prepared in advance by the organizations on paper or digital devices. Collecting authentic data is a significant challenge for supervisors, as these documents can be easily forged or tampered with.
- *Data processing* is the step where the authentication of data should be verified and the fake, invalid, and irrelevant data should be cleared.
- *Data analysis* is the process where the generated data are matched with the standard of regulatory rules, and a positive or negative decision is made along with it.
- *Data visualization* is the proper presentation of data, showing the result of data analysis in a readable and easy-to-comprehend format. Data storage, or data archiving, is the definitive treatment of data. In this step, all the data should have clear identification, and they deserve various destinations as per their categories. In terms of complexity, the most time-consuming procedure is data processing.

There may be some additional steps, such as *data storage* or *archiving*. The development of regulatory technologies benefits some key drivers that are relevant to data processing. It is mentioned that the following data issues in the financial sector, to some extent, drive regulation technology forward [5]:

- *Unstructured Data*: Data is collected from various sources within organizations without a unified format, so it is time-consuming for regulators to aggregate information and identify risks.
- *The complexity of Received Data*: The increasing regulations, which are increasingly complex, challenge the expertise of professionals to make timely and correct judgments or recommendations.
- *New Risks Caused by the Dynamic Development of Entities*: Migrating financial companies to virtual companies may bring new potential risks to the industry in terms of regulation and management.

We can conclude that the financial industry and other industries are facing these problems, too. Although other industries started later than the financial sector, the issues and needs in these regulatory activities are similar. Other industries even face more problems. A major difference between the financial sector and the other physical industries is that there needs to be more filed data in the former, but field data in the latter is one of the main data sources.

7.2. The Need for IIoT in RegTech

To improve information transparency from the perspective of regulators, the implementation of IIoT is necessary, especially for industries involving large amounts of field data. Not only can IoT applications free human hands from data collection, but the data collected automatically by the devices also avoids possible data falsification and human errors. For example, operators may make up fake data to cover up mistakes they make in the processing procedures. Moreover, the significant information asymmetry between firms and regulators causes extra costs for regulators to supervise. It is identified by Gao, Ling, and Liu [90] that social media can promote the information disclosure of non-compliance behaviors based on the case analysis of environmental incidents. However, it is important to note that media information is also sourced indirectly from secondary sources, and media disclosures are processed and guided by subjective language or concepts rather than objective and neutral ones. Data collected by the IoT is more objective and unbiased in the absence of malicious human intervention. The adoption of IoT can improve information transparency, save labor in data collection, reduce human errors, and solve the information asymmetry issue between regulators and producers.

7.3. Data Security and Access Control

Information privacy is a significant point that needs to be addressed. Psychologically, it is human nature to be reluctant to make public disclosures [91]. From a business perspective, companies may be concerned about their trade secrets being leaked. Implementing IoT for data collection can provide a good database for maximum data sharing, and at the same time, the privacy of enterprises should be properly protected. In addition, the threat to cyber security is another serious problem in the existing network [92–95]. Data sharing should be conducted within safe networks for both regulators and regulated entities. Blockchain, defined by Don and Alex Tapscott [96] as “an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value”, is one of the potential solutions to this issue due to its significant advantages or features such as transparency, immutability, and trustworthiness with high reliability [97–99]. With the advantages of the technology, blockchain is identified as an effective tool in the bill operation of commercial banks through building a decentralized digital billing system to decrease bill-forgery risk and credit risks, as well as in the cross-border payment operation to save service charges and transfer time compared with the traditional payment method such as the SWIFT system [100]. Similarly, blockchain technology can be used in RegTech applications to ensure data security and smooth information communication between stakeholders.

In addition to adopting blockchain technology to protect data privacy and security, another effective way is to set proper access control as agreed upon by all stakeholders

who have access to relevant data pools. For example, Attribute-Based Encryption (ABE) is the best way to apply access control [101–103]. It is also taken as a useful technique to solve the issue of “data privacy and fine-grained access control” in popular cloud storage systems [104]. By taking advantage of this technology, access to the relevant data can be restricted to desired groups of users only through data encryption and authorized decryption [105]. This will prevent data breaches in daily compliance activities and protect the producer’s commercial confidentiality. The combination of ABE and blockchain (as shown in Figure 5) can make data sharing flexible and secure.

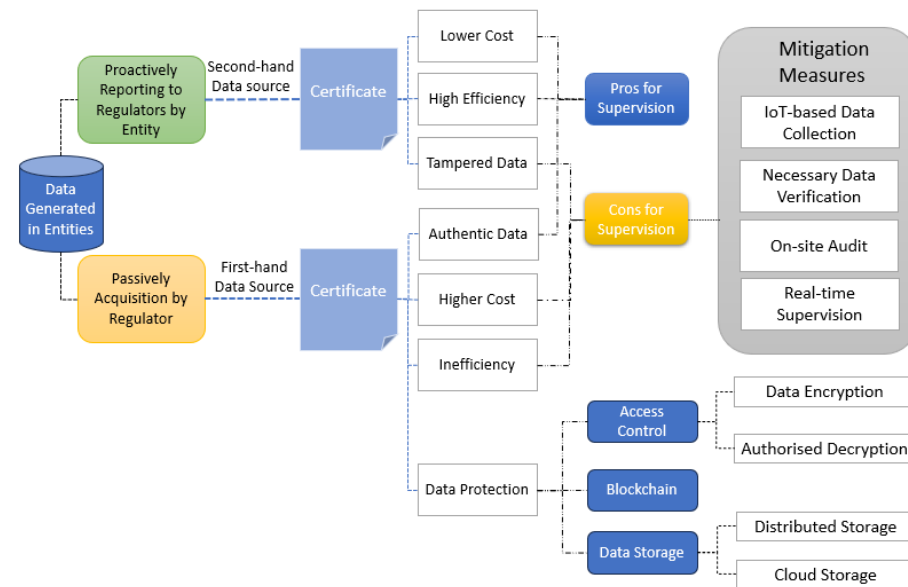


Figure 5. Regulatory Supervision Framework in Non-Financial Sectors.

7.4. Data Storage and Archiving

The daily collected data needs to be stored securely after being processed. Some data may need to go to the blockchain after processing, while others may be stored on a local server. Data treatment is different in terms of importance. Furthermore, centralized storage methods such as cloud storage and decentralized storage is another potential solution for dealing with the massive amounts of data generated daily. Data is more secure to store on blockchain networks. But the limitations of blockchain technology, such as scalability and availability in data processing, retrieval, and storage [106], restrain its application to large files or document storage. The Interplanetary File System (IPFS), which “identifies, verifies, and transfers files relying on the cryptographic hashes of their contents” [107], is a content-addressable distributed file storage platform [108] with a decentralized storage protocol. It is a potential solution to address excessive file redundancy when using blockchain technology.

The IPFS system can allocate a unique hash for each file stored by users who have access to their corresponding files via the hash address. Data owners can encrypt their data before storing it on the IPFS platform. For example, Sun and Yao discussed the implementation of IPFS in medical data storage to control the access to the patient’s medical records of various users [109]. They indicate that medical data can be encrypted based on attributes and determine the attributes of users by matching the private key related to their attributes with the access policy set in advance. The users can have secured data access by matching the private key related to the users’ attributes with the access policy set in advance and related to the ciphertext. They also advocate that blockchain can record medical data’s storage and search processes, providing both tracking of data sources and data retrieval records. In addition, IPFS is a good way to archive data. Centralizing data storage on a cloud server is cost-effective and convenient for data retrieval for companies. However,

the failure of one cloud model may lead to the unavailability of the whole cloud server. In contrast, the IPFS has no single point of failure without a central server, and the data are stored in duplicate copies in different places worldwide [104]. In short, the regulated entities may choose the most suitable data storage mode—cloud storage or distributed storage—as shown in Figure 5.

7.5. Potential IIoT-Based Regulatory Supervision Framework

The presence of supervisory activity is a sign of the regulator's distrust of the regulated entities. Traditionally, the supervisors may need to audit producers on site to confirm their actions comply with the regulatory requirements. But it is more difficult to ascertain compliance immediately after such spot checks. Although many of the producers follow the rules, some of them can violate them to reduce costs or pursue higher profits. One possible solution is real-time supervision. There are two ways to conduct it. One is that the producers can proactively report to regulators or supervisors. The other way is that regulators can passively acquire the reports. From the regulators' perspective, the former way has prominent pros such as lower cost and high efficiency, but the data might be tampered with as they are second-hand sources. The disadvantages of the latter approach are higher costs and inefficiency. However, the data are authentic (see Figure 5). Regulators want authentic data, while supervision needs to be cost-effective and efficient. To achieve this, the ideal solution would be to map real-world production processes onto the web applications with technologies such as *digital twins* [110]. This would allow for real-time monitoring and management, which could become as easy as supervision in the financial sector. However, it is difficult to achieve this in all industries worldwide at the moment. Nevertheless, there are a few options that can be tried to become closer to this goal:

- *IoT-based Data Collection*: this not only saves labor costs for producers for data collection by replacing traditional manual work but also increases the transparency of the process.
- *Necessary Data Verification*: this measure prevents data fraud risks such as IoT devices being damaged or tampered with by humans. It can be achieved by introducing AI and ML technologies to assist decision-making after certain algorithms are trained [111].
- *On-site Audit*: Activities in the non-financial sectors involve fieldwork. A proper on-site audit is necessary, as supervisors can only partially rely on online supervision. For example, pesticide spraying is important for the cultivation of crops because it is effective against pests and diseases. However, excessive pesticide use is a serious threat to human health, and therefore precise control of pesticide doses is very important. It is therefore important to check records of pesticide purchases and actual use.
- *Real-Time Supervision*: Real-time monitoring in some critical procedures with automatic reporting to regulators can help manufacturers comply with regulations with less labor cost in data collection as well as establish a good reputation. Machine learning can help companies eliminate potential risks by using daily data to predict their occurrence in advance. On-premises real-time monitoring is difficult, as companies would be reluctant to set up such infrastructure without any benefit. However, manufacturers can also benefit if the IIoT is deployed for both their own production and compliance monitoring.

While these tools can solve some problems, they can also create new ones. For example, the daily collected data are of high volume, and how to safely process, share, and store it is a significant issue. The algorithms training for data verification takes time and money before they can make precise judgments. The frequent on-site audit is expensive for supervisors and a burden for producers. The regulator needs to balance the frequency and cost of data verification and its negative impact on industrial innovation. Real-time supervision may result in data privacy issues.

8. Conclusions

While the adoption of RegTech in the financial sector is relatively mature, its implementation in the non-financial industry is still in its early stages. There are already a variety of applications in various sectors that are experimenting with these technological tools. However, the non-financial sectors are more pragmatic and have more diverse and complex business environments. RegTech applications need to consider these industrial features at the initial framework stage to meet the industry's specific needs. The following aspects are identified as the most challenging points to be considered for future technological development or research: Real-time reporting for agricultural products is not easy due to diverse data sources and data collection environments; complete supply-chain traceability from raw materials to end products in manufacturing is challenging because of the complex value chain processes and the different interests of various stakeholders; the high level of privacy protection in the healthcare industry is rather critical for patients who are exposed to high risks without proper personal data protection; and supply-chain compliance in international trade and business is significantly challenged by the ever-changing international regulations, policies, and political situations.

In addition, humans continue to play a prominent role in the non-financial sectors because business operations in many industries are difficult to operate without human intervention, thus opening many possibilities for human factors to interfere with compliance outcomes. Moreover, RegTech development should consider the cost of implementation and the extent of applicability to various businesses without adding an extra burden or disrupting existing processes and practices. When considering the adoption of compliance solutions, companies should assess their private business requirements as well as the compatibility of their existing equipment and make sure training and support are available to their employees before choosing the most suitable and affordable application. Finally, the development of RegTech requires collective efforts from the government, regulators, and industries through Research and Development for the benefit of all in the value chains. These aspects are worthy of further study by researchers, industrial professionals, regulators, and organizations.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Grassi, L.; Lanfranchi, D. RegTech in public and private sectors: The nexus between data, technology and regulation. *J. Ind. Bus. Econ.* **2022**, *49*, 441–479. [CrossRef]
2. Firmansyah, B.; Arman, A.A. A Systematic Literature Review of RegTech: Technologies, Characteristics, and Architectures. In Proceedings of the 2022 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 8–9 November 2022; pp. 310–315.
3. Butler, T. Towards a standards-based technology architecture for RegTech. *J. Financ. Transform.* **2017**, *45*, 49–59.
4. Gasparri, G. Risks and Opportunities of RegTech and SupTech Developments. *Front. Artif. Intell.* **2019**, *2*, 14. (In English) [CrossRef] [PubMed]
5. Dziawgo, T. Supervisory Technology As a New Tool for Banking Sector Supervision. *J. Bank. Financ. Econ.* **2021**, *15*, 5–13. [CrossRef]
6. Schueffel, P. Taming the beast: A scientific definition of fintech. *J. Innov. Manag.* **2016**, *4*, 32–54. [CrossRef]
7. Wilkins, C. *Financial Stability Implications from Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention*; Financial Stability Board: Basel, Switzerland, 2017.
8. SafariCom. SafariCom. Available online: <https://www.safaricom.co.ke/personal/m-pesa/getting-started> (accessed on 15 July 2023).
9. Puschmann, T. Fintech. *Bus. Inf. Syst. Eng.* **2017**, *59*, 69–76. [CrossRef]
10. Suryono, R.R.; Budi, I.; Purwandari, B. Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review. *Information* **2020**, *11*, 590. [CrossRef]
11. Call for Input: Supporting the Development and Adoption of RegTech. Available online: <https://www.fca.org.uk/news/news-stories/call-input-supporting-development-and-adoption-regtech> (accessed on 8 June 2023).

12. FinTech, R. SupTech: What They Mean for Financial Supervision. 2017, 20, 20. Available online: https://www.torontocentre.org/videos/FinTech_RegTech_and_SupTech_What_They_Mean_for_Financial_Supervision.pdf (accessed on 29 July 2023).
13. Billington, C.; Lee, H.L.; Tang, C.S. Successful strategies for product rollovers. *MIT Sloan Manag. Rev.* **1998**, *39*, 3.
14. Teichmann, F.; Boticiu, S.; Sergi, B.S. RegTech–Potential benefits and challenges for businesses. *Technol. Soc.* **2023**, *72*, 102150. [CrossRef]
15. Narang, S. Accelerating Financial Innovation Through RegTech: A New Wave of FinTech. In *Fostering Innovation and Competitiveness with FinTech, RegTech, and SupTech*; IGI Global: Hershey, PA, USA, 2021; pp. 61–79.
16. Johansson, E.; Sutinen, K.; Lassila, J.; Lang, V.; Martikainen, M.; Lehner, O.M. Regtech-a necessary tool to keep up with compliance and regulatory changes. *ACRN J. Financ. Risk Perspect. Spec. Issue Digit. Account.* **2019**, *8*, 71–85.
17. Yang, D.; Li, M. Evolutionary approaches and the construction of technology-driven regulations. *Emerg. Mark. Financ. Trade* **2018**, *54*, 3256–3271. [CrossRef]
18. Umalkar, M. RegTech: An untapped opportunity. *J. Digit. Bank.* **2021**, *6*, 72–82.
19. Turki, M.; Hamdan, A.; Cummings, R.T.; Sarea, A.; Karolak, M.; Anasweh, M. The regulatory technology “RegTech” and money laundering prevention in Islamic and conventional banking industry. *Heliyon* **2020**, *6*, e04949. [CrossRef]
20. Buckley, R.; Arner, D.; Barberis, J. The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data. *J. Financ. Transform.* **2016**, *44*, 79–86. [CrossRef]
21. RegTech Companies. Available online: <https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html> (accessed on 17 April 2023).
22. “REGTECH100-2023”, in “REGTECH100”, 2023. Available online: <https://fintech.global/regtech100/wp-content/uploads/2022/12/RegTech100-Report-2023.pdf> (accessed on 16 July 2023).
23. Butler, T.; O’Brien, L. Understanding RegTech for digital regulatory compliance. *Disrupting Financ. FinTech Strategy 21st Century* **2019**, 85–102.
24. Yan, P.; Crane, M.; Brennan, R. GDPR Compliance tools: Best practice from RegTech. In *Proceedings of the Enterprise Information Systems: 22nd International Conference, ICEIS 2020, Virtual Event, 5–7 May 2020; Revised Selected Papers*. Springer: Berlin/Heidelberg, Germany, 2021; pp. 905–929.
25. Papantoniou, A.A. Regtech: Steering the regulatory spaceship in the right direction? *J. Bank. Financ. Technol.* **2022**, *6*, 1–16. [CrossRef]
26. Ivanoski, J.; Bailey, D.; Walters, M.; Vazirani, J. The transformative power of regtech. *Front. Financ. Decis.-Mak. Financ. Serv.* **2017**, *57*, 14–17.
27. Colaert, V. RegTech as a response to regulatory expansion in the financial sector. Available at SSRN 2677116 **2018**.
28. Walshe, J.; Cropper, T. Should you be banking on RegTech? *J. Secur. Oper. Custody* **2018**, *10*, 167–175.
29. Kurum, E. RegTech solutions and AML compliance: What future for financial crime? *J. Financ. Crime* **2023**, *30*, 776–794. [CrossRef]
30. Arner, D.W.; Zetsche, D.A.; Buckley, R.P.; Weber, R.H. The future of data-driven finance and RegTech: Lessons from EU big bang II. *Stan. J. Bus. Fin.* **2020**, *25*, 245.
31. Armstrong, P. *Developments in RegTech and SupTech*; Paris Dauphine University: Paris, France, 2018. Available online: https://www.esma.europa.eu/sites/default/files/library/esma71-99-1070_speech_on_regtech.pdf (accessed on 22 July 2018).
32. McCarthy, J. The regulation of RegTech and SupTech in finance: Ensuring consistency in principle and in practice. *J. Financ. Regul. Compliance* **2023**, *31*, 186–199. [CrossRef]
33. Packin, N.G. RegTech, compliance and technology judgment rule. *Chi.-Kent L. Rev.* **2018**, *93*, 193.
34. Ryan, P.; Crane, M.; Brennan, R. Design challenges for GDPR RegTech. *arXiv* **2020**, arXiv:2005.12138.
35. Bolton, M.; Mintrom, M. RegTech and creating public value: Opportunities and challenges. *Policy Des. Pract.* **2023**, 1–17. [CrossRef]
36. Khanzode, K.C.A.; Sarode, R.D. Advantages and disadvantages of artificial intelligence and machine learning: A literature review. *Int. J. Libr. Inf. Sci. (IJLIS)* **2020**, *9*, 3.
37. Mahalakshmi, V.; Kulkarni, N.; Kumar, K.P.; Kumar, K.S.; Sree, D.N.; Durga, S. The Role of implementing Artificial Intelligence and Machine Learning Technologies in the financial services Industry for creating Competitive Intelligence. *Mater. Today Proc.* **2022**, *56*, 2252–2255. [CrossRef]
38. Regulation, G.D.P. General data protection regulation (GDPR). *Intersoft Consult. Accessed Oct.* **2018**, *24*. Available online: <https://gdpr-info.eu/art-24-gdpr/> (accessed on 17 April 2023).
39. Voigt, P.; Von dem Bussche, A. The eu general data protection regulation (gdpr). In *A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10, p. 10-5555.
40. Neovius, M.; Karlsson, J.; Westerlund, M.; Pulkkis, G. Providing tamper-resistant audit trails for cloud forensics with distributed ledger based solutions. *Cloud Comput.* **2018**, *2018*, 29.
41. Ahmad, A.; Saad, M.; Njilla, L.; Kamhoua, C.; Bassiouni, M.; Mohaisen, A. Blocktrail: A scalable multichain solution for blockchain-based audit trails. In *Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 20–24 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
42. Ahmad, A.; Saad, M.; Bassiouni, M.; Mohaisen, A. Towards blockchain-driven, secure and transparent audit logs. In *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, New York, NY, USA, 5–7 November 2018; pp. 443–448.

43. Carrell, D.S.; Cronkite, D.; Palmer, R.E.; Saunders, K.; Gross, D.E.; Masters, E.T.; Hylan, T.R.; Von Korff, M. Using natural language processing to identify problem usage of prescription opioids. *Int. J. Med. Inform.* **2015**, *84*, 1057–1064. [\[CrossRef\]](#)
44. Zetsche, D.A.; Buckley, R.P.; Arner, D.W.; Barberis, J.N. From FinTech to TechFin: The regulatory challenges of data-driven finance. *NYUJL Bus.* **2017**, *14*, 393.
45. Aziz, H.; Guled, A. Cloud computing and healthcare services. *J. Biosens. Bioelectron.* **2016**, *7*, 220. [\[CrossRef\]](#)
46. Youssef, A.E. Exploring cloud computing services and applications. *J. Emerg. Trends Comput. Inf. Sci.* **2012**, *3*, 838–847.
47. Atlam, H.F.; Alenezi, A.; Alharthi, A.; Walters, R.J.; Wills, G.B. Integration of cloud computing with internet of things: Challenges and open issues. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 670–675.
48. Syed, R.; Suriadi, S.; Adams, M.; Bandara, W.; Leemans, S.J.; Ouyang, C.; ter Hofstede, A.H.; van de Weerd, I.; Wynn, M.T.; Reijers, H.A. Robotic process automation: Contemporary themes and challenges. *Comput. Ind.* **2020**, *115*, 103162. [\[CrossRef\]](#)
49. Kumar, K.N.; Balaramachandran, P.R. Robotic process automation—a study of the impact on customer experience in retail banking industry. *J. Internet Bank. Commer.* **2018**, *23*, 1–27.
50. Devarajan, Y. A study of robotic process automation use cases today for tomorrow's business. *Int. J. Comput. Tech.* **2018**, *5*, 12–18.
51. Nagy, J.; Oláh, J.; Erdei, E.; Máté, D.; Popp, J. The role and impact of Industry 4.0 and the internet of things on the business strategy of the value chain—The case of Hungary. *Sustainability* **2018**, *10*, 3491. [\[CrossRef\]](#)
52. Zhang, Q.; Huang, T.; Zhu, Y.; Qiu, M. A case study of sensor data collection and analysis in smart city: Provenance in smart food supply chain. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 382132. [\[CrossRef\]](#)
53. Pal, K. Internet of things and blockchain technology in apparel manufacturing supply chain data management. *Procedia Comput. Sci.* **2020**, *170*, 450–457. [\[CrossRef\]](#)
54. Malhotra, D.; Saini, P.; Singh, A.K. How blockchain can automate KYC: Systematic review. *Wirel. Pers. Commun.* **2022**, *122*, 1987–2021. [\[CrossRef\]](#)
55. Parra-Moyano, J.; Thoroddsen, T.; Ross, O. Optimised and dynamic KYC system based on blockchain technology. *Int. J. Blockchains Cryptocurrencies* **2019**, *1*, 85–106. [\[CrossRef\]](#)
56. Wang, B.; Lin, Z.; Wang, M.; Wang, F.; Xiangli, P.; Li, Z. Applying blockchain technology to ensure compliance with sustainability standards in the PPE multi-tier supply chain. *Int. J. Prod. Res.* **2022**, *61*, 4934–4950. [\[CrossRef\]](#)
57. Shojaei, A.; Flood, I.; Moud, H.I.; Hatami, M.; Zhang, X. An implementation of smart contracts by integrating BIM and blockchain. In Proceedings of the Future Technologies Conference (FTC) 2019, San Francisco, CA, USA, 14–15 November 2019; Volume 2, pp. 519–527.
58. Park, A.; Li, H. The effect of blockchain technology on supply chain sustainability performances. *Sustainability* **2021**, *13*, 1726. [\[CrossRef\]](#)
59. Bernal, E.; Spiriyagin, M.; Cole, C. Onboard condition monitoring sensors, systems and techniques for freight railway vehicles: A review. *IEEE Sens. J.* **2018**, *19*, 4–24. [\[CrossRef\]](#)
60. Munirathinam, S. Industry 4.0: Industrial internet of things (IIOT). In *Advances in computers*; Elsevier: Amsterdam, The Netherlands, 2020; Volume 117, pp. 129–164.
61. Zhou, C.; Damiano, N.; Whisner, B.; Reyes, M. Industrial Internet of Things (IIoT) applications in underground coal mines. *Min. Eng.* **2017**, *69*, 50. [\[CrossRef\]](#)
62. Reising, D.; Cancellieri, J.; Loveless, T.D.; Kandah, F.; Skjellum, A. Radio identity verification-based IoT security using RF-DNA fingerprints and SVM. *IEEE Internet Things J.* **2020**, *8*, 8356–8371. [\[CrossRef\]](#)
63. Sinha, N.; Pujitha, K.E.; Alex, J.S.R. Xively based sensing and monitoring system for IoT. In Proceedings of the 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 8–10 January 2015; pp. 1–6.
64. Venkatesan, R.; Tamilvanan, A. A sustainable agricultural system using IoT. In Proceedings of the 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017; pp. 0763–0767.
65. Shahbazi, Z.; Byun, Y.-C. Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors* **2021**, *21*, 1467. [\[CrossRef\]](#)
66. Tomaschek, K.; Olechowski, A.; Eppinger, S.; Joglekar, N. A survey of technology readiness level users. In *Proceedings of the INCOSE International Symposium*, 18 July 2016; Wiley Online Library: Hoboken, NJ, USA, 2016; Volume 26, pp. 2101–2117.
67. What the RegTech Industry Means for the Booming Mortgages Industry Right Now. Available online: <https://www.planetcompliance.com/what-the-regtech-industry-means-for-the-booming-mortgages-industry-right-now/> (accessed on 10 June 2023).
68. Waldron, B.R.a.D. Fighting Back against Synthetic Identity Fraud. Available online: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/fighting-back-against-synthetic-identity-fraud> (accessed on 6 June 2023).
69. MORTGAGE QC INDUSTRY TRENDS—Q3 2020. Available online: <https://www.acesquality.com/resources/reports/q3-2020-aces-mortgage-qc-industry-trends> (accessed on 10 June 2023).
70. Arner, D.W.; Barberis, J.; Buckley, R.P. FinTech, RegTech, and the reconceptualization of financial regulation. *Nw. J. Int'l L. Bus.* **2016**, *37*, 371.
71. Von Solms, J. Integrating Regulatory Technology (RegTech) into the digital transformation of a bank Treasury. *J. Bank. Regul.* **2021**, *22*, 152–168. [\[CrossRef\]](#)

72. Singh, C.; Lin, W. Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising. *J. Money Laund. Control* **2021**, *24*, 464–482. [CrossRef]
73. Elimelech, O.C.; Ferrante, S.; Josman, N.; Meyer, S.; Lunardini, F.; Gómez-Raja, J.; Galán, C.; Cáceres, P.; Sciamia, P.; Gros, M. Technology use characteristics among older adults during the COVID-19 pandemic: A cross-cultural survey. *Technol. Soc.* **2022**, *71*, 102080. [CrossRef]
74. Cowburn, N.; Barnet, P. RegTech Opportunities in a Post-4MLD/5MLD World. *RegTech Book* **2019**. [CrossRef]
75. Kampan, K.; Tsusaka, T.W.; Anal, A.K. Adoption of Blockchain Technology for Enhanced Traceability of Livestock-Based Products. *Sustainability* **2022**, *14*, 13148. [CrossRef]
76. Akhter, R.; Sofi, S.A. Precision agriculture using IoT data analytics and machine learning. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5602–5618. [CrossRef]
77. Anidu, A.; Dara, R. A review of data governance challenges in smart farming and potential solutions. In Proceedings of the 2021 IEEE International Symposium on Technology and Society (ISTAS), Waterloo, ON, Canada, 28–31 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8.
78. Virk, A.L.; Noor, M.A.; Fiaz, S.; Hussain, S.; Hussain, H.A.; Rehman, M.; Ahsan, M.; Ma, W. Smart farming: An overview. *Smart Village Technol. Concepts Dev.* **2020**, *17*, 191–201.
79. Amiri-Zarandi, M.; Hazrati Fard, M.; Yousefinaghani, S.; Kaviani, M.; Dara, R. A platform approach to smart farm information processing. *Agriculture* **2022**, *12*, 838. [CrossRef]
80. Pivoto, D.; Waquil, P.D.; Talamini, E.; Finocchio, C.P.S.; Dalla Corte, V.F.; de Vargas Mores, G. Scientific development of smart farming technologies and their application in Brazil. *Inf. Process. Agric.* **2018**, *5*, 21–32. [CrossRef]
81. Ada, E.; Sagnak, M.; Uzel, R.A.; Balcioglu, I. Analysis of barriers to circularity for agricultural cooperatives in the digitalization era. *Int. J. Product. Perform. Manag.* **2022**, *71*, 932–951. [CrossRef]
82. How Regtech Will Help Drive the Manufacturing Industry Forward. Available online: <https://www.planetcompliance.com/how-regtech-will-help-drive-the-manufacturing-industry-forward/> (accessed on 12 June 2023).
83. Timmons, J. The Cost of Federal Regulation. Available online: <https://www.nam.org/the-cost-of-federal-regulation/> (accessed on 20 May 2023).
84. Hickey, A. Compliance May Cost Companies Millions, but Non-Compliance Costs Even More. Available online: <https://www.ciodive.com/news/compliance-may-cost-companies-millions-but-non-compliance-costs-even-more/513280/> (accessed on 12 June 2023).
85. RegTech Transforming the Healthcare Industry. Available online: <https://www.planetcompliance.com/regtech-transforming-the-healthcare-industry/> (accessed on 12 June 2023).
86. Treasury, D.o.t., (Ed.) *National Money Laundering Risk Assessment*; 2022; p. 71. Available online: <https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf> (accessed on 12 June 2023).
87. Fadahunsi, A.; Rosa, P. Entrepreneurship and illegality: Insights from the Nigerian cross-border trade. *J. Bus. Ventur.* **2002**, *17*, 397–429. [CrossRef]
88. Li, X.H. Blockchain-based cross-border E-business payment model. In Proceedings of the 2021 2nd International Conference on E-Commerce and Internet Technology (ECIT), Hangzhou, China, 5–7 March 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 67–73.
89. Amankwah-Amoah, J.; Khan, Z.; Wood, G.; Knight, G. COVID-19 and digitalization: The great acceleration. *J. Bus. Res.* **2021**, *136*, 602–611. [CrossRef] [PubMed]
90. Gao, S.; Ling, S.; Liu, W. The role of social media in promoting information disclosure on environmental incidents: An evolutionary game theory perspective. *Sustainability* **2018**, *10*, 4372. [CrossRef]
91. Li, K.; Cheng, L.; Teng, C.-I. Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Inf. Process. Manag.* **2020**, *57*, 102128. [CrossRef]
92. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber security threats to IoT applications and service domains. *Wirel. Pers. Commun.* **2017**, *95*, 169–185. [CrossRef]
93. Al Nafea, R.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 779–786.
94. Humayun, M.; Niazi, M.; Jhanjhi, N.; Alshayeb, M.; Mahmood, S. Cyber security threats and vulnerabilities: A systematic mapping study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
95. Ullah, F.; Naeem, H.; Jabbar, S.; Khalid, S.; Latif, M.A.; Al-Turjman, F.; Mostarda, L. Cyber security threats detection in internet of things using deep learning approach. *IEEE Access* **2019**, *7*, 124379–124389. [CrossRef]
96. Bahga, A.; Madiseti, V.K. Blockchain platform for industrial internet of things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
97. Golosova, J.; Romanovs, A. The advantages and disadvantages of the blockchain technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.
98. Niranjnamurthy, M.; Nithya, B.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Clust. Comput.* **2019**, *22*, 14743–14757. [CrossRef]
99. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhlimeh, A. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* **2021**, *9*, 12730–12749.

100. Wu, B.; Duan, T. The advantages of blockchain technology in commercial bank operation and management. In Proceedings of the 2019 4th International Conference on Machine Learning Technologies, Nanchang China, 21–23 June 2019; pp. 83–87.
101. Ramu, G.; Eswara Reddy, B. Secure architecture to manage EHR's in cloud using SSE and ABE. *Health Technol.* **2015**, *5*, 195–205. [[CrossRef](#)]
102. Mhatre, S.; Nimkar, A.V. Secure cloud-based federation for EHR using multi-authority ABE. In Proceedings of the Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2017, Central University of Rajasthan, Ajmer, India, 23–25 November 2017; Springer: Berlin/Heidelberg, Germany; Volume 2, pp. 3–15.
103. Reedy, B.E.; Ramu, G. A Secure Framework for Ensuring EHR's Integrity Using Fine-Grained Auditing and CP-ABE. In Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 85–89.
104. Wang, S.; Zhang, Y.; Zhang, Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access* **2018**, *6*, 38437–38450. [[CrossRef](#)]
105. Yang, X.; Maiti, A.; Jiang, J.; Kist, A. Forecasting and Monitoring Smart Buildings with the Internet of Things, Digital Twins and Blockchain. In *Online Engineering and Society 4.0, Cham*; Auer, M.E., Bhimavaram, K.R., Yue, X.-G., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 213–224.
106. Gao, W.; Hatcher, W.G.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–11.
107. Steichen, M.; Fiz, B.; Norvill, R.; Shbair, W.; State, R. Blockchain-based, decentralized access control for IPFS. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1499–1506.
108. Huang, H.-S.; Chang, T.-S.; Wu, J.-Y. A secure file sharing system based on IPFS and blockchain. In Proceedings of the 2nd International Electronics Communication Conference, Singapore, 8–10 July 2020; pp. 96–100.
109. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [[CrossRef](#)]
110. Jones, D.; Snider, C.; Nassehi, A.; Yon, J.; Hicks, B. Characterising the Digital Twin: A systematic literature review. *CIRP J. Manuf. Sci. Technol.* **2020**, *29*, 36–52. [[CrossRef](#)]
111. Maiti, A.; Raza, A.; Kang, B.H.; Hardy, L. Estimating service quality in industrial internet-of-things monitoring applications with blockchain. *IEEE Access* **2019**, *7*, 155489–155503. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.