Environment Systems and Decisions
https://doi.org/10.1007/s10669-023-09902-5

Deployment of distributed ledger and decentralized technology for transition to smart industries

Bokolo Anthony Jr[1]

Accepted: 20 February 2023

Abstract

Industries are now deploying smart initiatives and innovative business models towards digital transformation. One of such initiatives is the adoption of distributed ledger technology (DLT) which promises to support smart industrial revolution. DLT facilitates non trusted entities to communicate and achieve a consensus in a fully distributed method through an immutable and cryptographically secure ledger. DLT ensures traceability and secure exchange of information while ensuring confidentiality and portability of data. However, only fewer studies have explored the extent to which DLT can support digitalization to achieve smart industrial process. Besides, the governance role of DLT in industrial sectors is still considered a nascent domain of research and DLT governance design and archetypes for smart industries are still in the early stage. Also, there are fewer studies in the literature that presents consensus mechanisms for integrating DLT for digitalization of smart industries. Grounded on the secondary data this study examines the practical benefits and challenges faced in achieving a smart industrial operation. Findings from this study identifies governance and security issues that influences DLT deployment in industrial sectors. More importantly, several factors that impacts the deployment of DLT for smart industries are presented. Implications from this study will be useful for industrial regulators, practitioners and researchers interested in gaining innovative insights about how smart industries can leverage DLT to create value for competitive advantage.

Keywords Emerging technologies · Distributed ledger technology · DLT governance design · DLT governance design archetypes · DLT governance factors · Smart industries

1 Introduction

Digitalization is an industry-wide goal aimed at enabling the diffusion of ICT and digital innovation to improve productivity, manage complexity, minimize project delays and high cost, while enhancing quality and safety (Li and Kassem 2019). Findings from the literature states that one of the main challenges facing smart industrial revolution includes poor collaboration, lack of trust, data availability, lack of practitioner's readiness and disinterest in adopting digital innovations (Li and Kassem 2019). For many public and private industries digitalization has led to a complete revision of their organizational practices as digital innovation mostly requires modernization of enterprise's business model and operation (Maull et al. 2017). Digitalization has the prospect to bring change in industrial`s business models (Panda et al. 2020). Digitalization enables almost any physical asset to be dematerialized replacing physical objects or records with a paperless computerized/digital version (Maull et al. 2017; Anthony Jr and Abbas Petersen 2021). Smart industries are proposed to link the physical components and the digital by connecting IT systems both within and across the industry (Roeck et al. 2020). The goal of smart industries is to achieve an inter-connected smart industry with processes which autonomously operates and can adapt to new business requirements in a cost-effective way irrespective of shorter product lifecycles, increasing customer demand, and service demand fluctuation (Lu et al. 2020; Roeck et al. 2020).

But the implementation of smart industries is still facing many strategic and governance challenges. Smart industrial revolution has begun due to digitalization which is the modernization of business models and processes facilitated by digital innovation such as robotization, additive 3D, big data analytics, cloud computing, social media analytics, artificial intelligence (AI), machine learning, digital twin,

✉ Bokolo Anthony Jr
anthony.bokolo@ife.no

[1] Department of Applied Data Science, Institute for Energy Technology, Os Alle 5, 1777 Halden, Norway

internet of things (IoT), distributed ledger technology (DLT), etc. (Anthony Jr and Abbas Petersen 2021). Findings from the literature (Roeck et al. 2020) argued that DLTs can be adopted to support the actualization of smart industries. DLT is one of the emerging digital technologies that is paving way for industrial revolution (Maull et al. 2017). A distributed ledger is basically a consensus of synchronized, shared, and replicated digital data geographically dispersed across several locations without requiring a centralized data storage or central administrator (Panda et al. 2020; Priem 2020; Shahid et al. 2020). Particularly, DLTs can be utilized to facilitate managing a generic view among inter-connected nodes without a central regulator (Kuo et al. 2018).

A recent report by the European Commission (EC) highlighted that DLT could be implemented to digitalized various types of industries such as supply chain, energy, manufacturing, health, transportation, etc. (Kuo et al. 2018). There are different DLTs implementations in smart industrial sectors with pros and cons. For example, Ethereum offers a distributed virtual machine that processes different kind of computation but is associated with scalability issue. Another DLT is IOTA which provide improved scalability but is constrained with not providing distributed computation support (Zichichi et al. 2020). The use of DLT in smart industries provides the potential for truly digitalized economy through smart contracts (Maull et al. 2017; Casado-Vara and Corchado 2019). DLT is suggested as an innovative technology that can unlock novel disruptive business models and consequently have potential implications for smart industries such as Facebook, Microsoft, IBM, etc. are participating heavily in DLTs such as blockchain (Ferraro et al. 2018; Atlam and Wills 2019; Priem 2020). Presently, studies related to DLT have been conducted across several domain but there is fewer academic literature that examined the deployment of DLT for smart industrial revolution. Besides, practitioners' issues related with integration of DLTs into existing industrial infrastructures calls for an inquiry of the issues posed by DLTs adoption in smart industrial revolution (Danzi et al. 2020).

Accordingly, grounded on secondary data from the literature this study systematically examines the practical benefits and challenges face in achieving a smart industrial operation for digitalization. Findings provide the potential of DLT deployment to support smart industrial transition. Also, this article goes beyond to provides insights on the security issues, DLT governance designs and archetypes and provides a more in-depth characteristics of DLT applications in smart industrial environment. Findings from this study identifies several factors that may impacts the implementation of DLT in smart industries. The findings from this study provides a taxonomy for DLT governance which enables practitioners and researchers to structure and understand DLT deployment in smart industrial sectors to create, capture, and deliver value. Lastly, this study provides recommendations on open technological, environmental, and social issues toward the successful integration of DLT. The remainder of this article is structures as Sect. 2 is the literature review, and Sect. 3 is the methodology. Section 4 is the findings, and Sect. 5 is the discussion and implications. Finally, Sect. 6 is the conclusion.

2 Literature review

The deployment of DLT have gained great consideration over the recent years. As such various studies have been published that examined the fundamental challenges in adopting DLTs in different industries. For example, Hofman (2020) researched on the adoption of DLT in supply and logistics chain visibility to reduce costs, improve decision making, and synchronize industrial processes. Further findings from the study identified general supply chain requirements for visibility transformed into conceptual specifications to improve supply chain visibility. Nagel and Kranz (2020) researched on smart applications based on blockchain in towards designing a multi-layer taxonomy. The authors illustrated how blockchain is utilized in diverse smart business models and explores technological characteristics and configurations of blockchain-based applications. Findings from their study identified blockchain archetypes in several sectors. Zichichi et al. (2020) presented a DLT based architecture to support smart transportation system in creating, storing, and sharing data generated by users via mobile sensors. The authors further employed IOTA and Ethereum smart contract as DLTs to manage mobility related data to achieve social mobility.

Additionally, Roeck et al. (2020) explored the potential application of DLT in smart factories strategies in the context of Industry 4.0. The study focuses to examine practical issues that manufacturing industries face when creating smart factories and assimilating them into their current value chain. Treiblmaier and Sillaber (2020) employed a case study based on qualitative interviews data and project document of blockchain based digital transformation within public sector. The main goal of their research was to streamline the complex managerial processes involved in public administration which has led to steadily increased workload with inadequate resources. Likewise, Zichichi et al. (2020) investigated if DLTs can be employed to support complex services such as intelligent transportation systems. IOTA is employed to support verifiability, traceability, and immutability of mobility related data. Findings from the authors suggested that the responsiveness and scalability of DLTs still need to address in the literature. Furthermore, Corchado (2019) developed a distributed e-health accounting ledger based on blockchain architecture. The architecture uses a wireless sensor networks controller to orchestrate patient's healthcare via smart contracts which helps to eliminate the need for intermediaries and reduces staffs' error.

Lamberti et al. (2019) developed an open multimodal mobility system based on DLT. The platform provided a distributed mobility application which is useful for providing different mobility services using a cost-efficient, transparent, and distributed data management infrastructure. Li and Kassem (2019) explored the readiness for macro adoption of DLT in construction industry. The socio-technical systems framework was adapted to construction industry based on four variables which comprises of policy, technical, social, and process. Findings from the study aimed to develop a roadmap to improve DLT adoption readiness in construction industry. Strugar et al. (2019) developed an architecture for DLT billing and machine-to-machine (M2M) transactions for electric vehicles (EV). The authors focussed to address the location privacy and imposed service fees faced in the mechanisms of EV charging and payment requirement.

Findings from the literature reveal that DLTs such as blockchain, IOTA, Ethereum, etc. are being integrated in different industrial sectors (manufacturing, e-health, energy, transportation, etc.) to support industries in managing and providing data driven services in response to digitalization. However, none of the reviewed studies have examined how DLTs can support digitalization to achieve smart industrial transition. Besides, DLT governance designs and archetypes and security issues have not been well researched in the literature. Hence, this current study adds to the body of knowledge by carrying out a descriptive literature review on the practical benefits and challenges faced in achieving a smart industrial operation for digital transformation. This article also identifies several factors that may impacts the deployment of DLT for actualization of smart industries.

3 Methodology

A descriptive literature review methodology was employed to present evidence similar to prior studies (Anthony Jr 2021a, b, c, d). A descriptive literature review aims to expediently assess prior studies that are appropriate to the specific research topic in order to present a fair assessment of an investigated topic using a rigorous and trustworthy approach. Therefore, the research flow for this study comprises of five phases as shown in Fig. 1.

Figure 1 depicts the research flow for this study, where each phase is discussed below in the subsequent sub-sections.

3.1 Inclusion and exclusion criteria

The inclusion and exclusion criteria are the sampling method employed to select articles to provide answers to the research questions presented in the introduction section. The inclusion and exclusion criteria are presented in Table 1. Thus, an article is included if it meets up to the criteria in the inclusion column and is excluded if it satisfies any of the exclusion criteria.

3.2 Search strategies and data sources

The sources employed in this study were retrieved through a comprehensive search of prior DLT/blockchain adoption research through online databases which comprise of Google

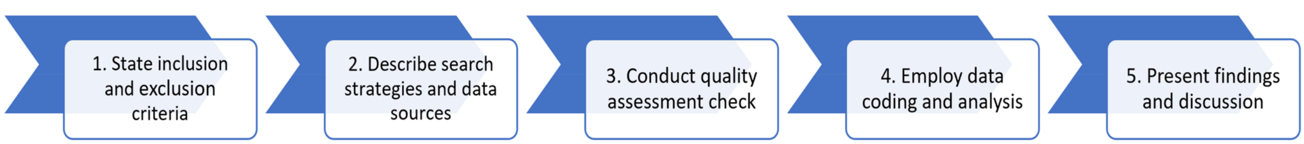


Fig. 1 Research flow

Table 1 Inclusion and exclusion criteria

Inclusion	Exclusion
Should involve background of DLT/blockchain deployment and factors that impacts DLT/blockchain deployment	Studies that do not present background of DLT/blockchain deployment and factors that impacts DLT/blockchain deployment
Should be based on an approach, model, theory, framework for exploring DLT/blockchain deployment	Models, approach, frameworks or theories used in contexts other than DLT/blockchain deployment
Should be mainly written in English and published between 2000 and 2022 as this is the duration of the cryptocurrency and bitcoin	Studies not within 2000 to 2022 and are not written in English
Studied on DLT/blockchain characteristics, governance, security challenges, general issues, benefits, and recommendations	Studies not on DLT/blockchain characteristics, governance, security challenges, general issues, benefits, and recommendations

Scholar, Wiley, Taylor & Francis, IGI Global, ScienceDirect, Sage, Emerald, IEEE, ACM, Inderscience, and Springer. The search was undertaken within January 2021, and then in April 2022. A final search was carried out in November 2022 after revision of this paper. The search terms include the keywords ((“distributed ledger technology deployment” OR “DLT deployment” OR “blockchain deployment”) AND (“governance” OR “security” OR “archetypes” OR “design” OR “smart industries” OR “industries”) AND (“factors” OR “drivers”)). These keywords were employed to retrieve appropriate articles to provide empirical evidence regarding the objectives of this study.

Figure 2 shows the preferred reporting items for systematic reviews and meta-analysis (PRISMA) flowchart which was used for screening of articles as previously utilized by Anthony Jnr (2021a, b, c). The final search resulted to 137 articles using the keywords above (the retrieved 137 sources are not provided as they all are not aligned to the scope of this current study, only the paper in line with the inclusion and exclusion criteria are finally provided). Five articles were established as duplicates and were removed. Thus, the articles remained 132. The articles were checked against the inclusion and exclusion criteria and 78 sources were removed since they were not related to DLT/blockchain deployment, DLT governance, security, and factors that impacts DLT/blockchain deployment resulting to 54 articles. The remaining articles was checked for quality assessment. A check was carried out to verify if the articles were indexed in Scopus or/and ISI Web of Science databases. The findings as discussed in the quality assessment section suggest that the selected studies meet the inclusion and quality assessment criteria. Then, 15 articles were included via cross

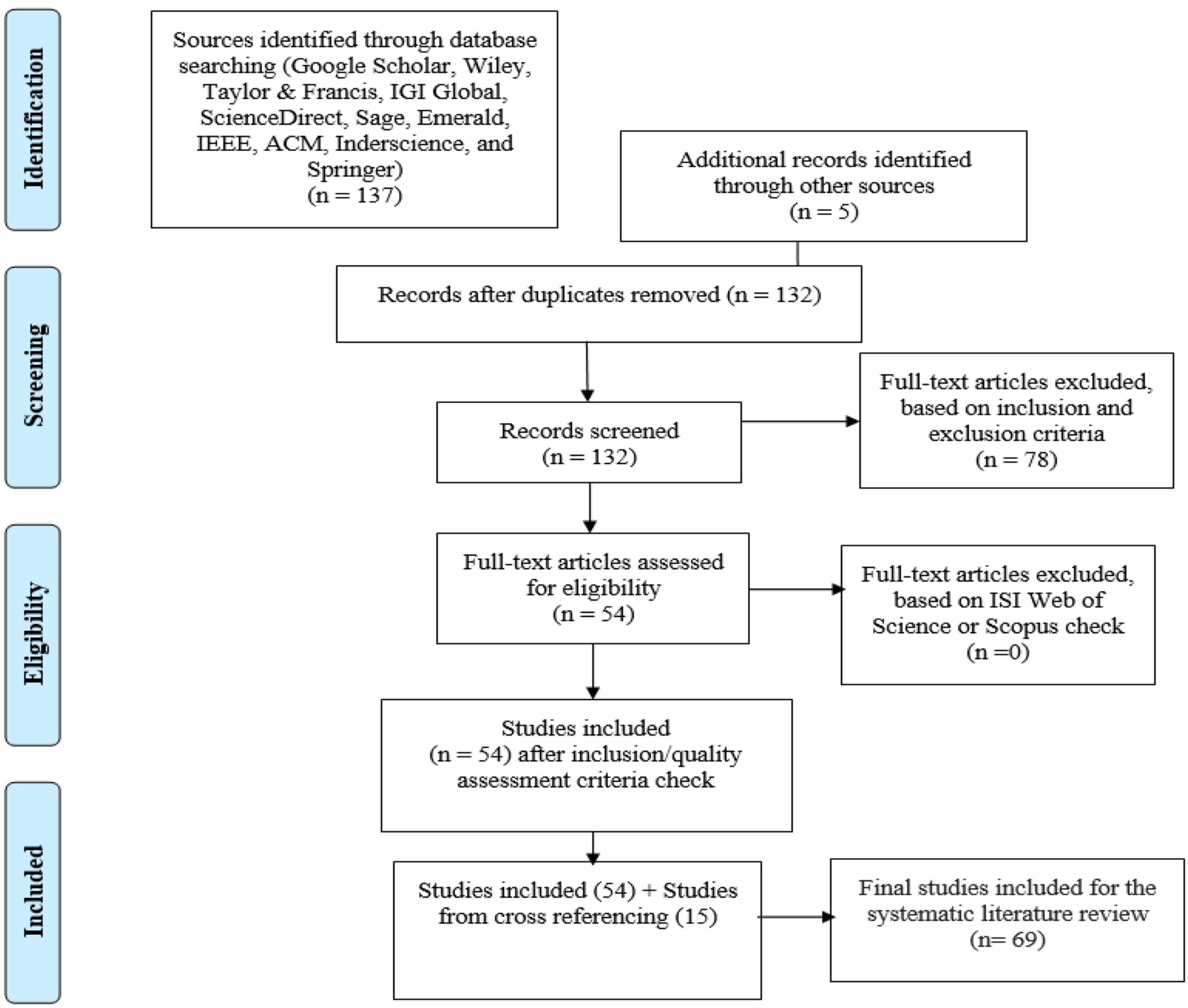


Fig. 2 PRISMA flowchart for the selected articles

referencing as seen in Fig. 2. Finally, one souce was added (Li and Kassem, 2019). All included sources are presented in the reference section of this paper totaling to 70 articles.

3.3 Quality assessment

One of the important benchmarks that is required to be checked with the inclusion and exclusion criteria is the quality assessment check as recommended by Anthony Jr (2021a, b, c). Therefore, quality assessment check was employed for all selected papers to confirm if the papers are indexed in Scopus or/and ISI Web of Science database as previously stated. This criterion helped to evaluate the quality of the selected studies. Respectively, more than half of the articles included are indexed in Scopus or/and ISI Web of Science database.

3.4 Data coding and analysis

Based on a descriptive literature review approach, the final 70 studies are utilized to provide evidence in response to the objectives of this study. This helps to provide information on DLT deployment for smart industrial transition. Thus, secondary data is extracted, synthesized, coded, and examined in detail and evidence from these sources as related to the objectives of this paper. The included 70 studies are presented in the reference section which comprises of 44 journal articles 13 conference proceedings, 8 book chapters, 4 preprints, and 1 technical report by Castro and Liskov (1999). Overall, most papers are published from 2000 to 2022.

4 Findings

Grounded on the selected 70 sources included for this study related to DLT deployment towards smart industries, this section reports the findings of this descriptive literature review.

4.1 Overview of distributed ledger and decentralized technology

Distributed ledgers can be defined as a decentralized trust technology which enables secure and transparent transactions between nodes within a distributed eco-system (Ølnes et al. 2017). DLT are distributed computer software that runs on peer-to-peer networks and offers a tamper-resistant, transparent, and verifiable transaction managed through a consensus mechanism (Lu et al. 2020). The technological structures of distributed ledgers enable business models deployed on smart contracts which potentially promotes disintermediation and better protection against data manipulation (Rückeshäuser 2017; Perera et al. 2020). DLT offers a shared digital infrastructure for platforms such as for financial transactions as it aids the running of an append-only database (termed as a ledger), which is distributed within several storage devices (termed as nodes) in an untrustworthy setting (Gräbe et al. 2020). In traditional industries, traditional ledgers are mostly paper based or digital files that aid with recording transactions, such as outstanding balances, accounts paid, etc. (Tekeoglu and Ahmed 2019). In comparison DLT creates online, distributed and mostly publicly available ledgers updated regularly by every node within the distributed network (Gräbe et al. 2020).

This is made possible based on consensus of nodes with the use of similar consensus algorithm or a proof-of-work (PoW), and without the intervention of a trusted third party (Zamani and Giaglis 2018). In DLT such as blockchain the nodes, i.e. the miners or the peers, decides which "block" should be included next on the "chain", ultimately forming the blockchain securely using public key cryptography (Zamani and Giaglis 2018; Gräbe et al. 2020). Similarly, transactions are referred to as hashes of the public keys belonging to the peers involved in blockchain which are cryptographically signed by the sender (Ribitzky et al. 2018; Zamani and Giaglis 2018). When a node accepts a new transaction, the transaction is validated and forwarded to all adjacent nodes, which then subsequently validates and forwards the new transaction. Since all nodes in DLT are maintained as a local replication of the ledger, all nodes are synchronized and settled on a common state of the distributed ledger to attain consistency (Ribitzky et al. 2018). Accordingly, a consensus mechanism is employed to orchestrate the negotiation between nodes, which finally agree on a mutual replication of the ledger. Once added, data can hardly be removed or altered anymore (Gräbe et al. 2020).

Furthermore, each transaction is referenced on the DLT eco-system and time-stamped, thus no transaction is transferred twice, and the earliest time-stamp transaction is considered the valid one in case of complaint (Lacity 2018). This helps to ensure the infrastructure is secured as compared to other forms of digital transfers. Respectively, DLT works in a similar manner to traditional business ledgers, using cryptocurrencies for settlements (Wu et al. 2017; Zamani and Giaglis 2018). Although DLT can address some challenges faced in industries today, it does not come without any shortcomings. For instance, as compared to be centralized database, DLT operate at a lower transaction processing time leading to increased latency within the system (Viriyasitavat et al. 2019; Arslan et al. 2020). However, due to the decentralized architecture of DLT it avoids single points of failure and offers a scalable and reliable services. Also, using smart contracts DLTs greatly improve system connectivity and opens up new more functionality to industries (Rahmadika and Rhee 2018).

Figure 3 shows the components of DLT deployed in smart industrial sectors such as manufacturing, supply chain, distribution, production, etc. for digitalization which comprises of shared ledger, cryptography, nodes, and consensus mechanism. The shared ledger comprises of a shared database that stores all transactions of the participating nodes within the network. The shared ledger is accessed, synchronized, and updated with other copies of the ledger within the network across different locations within a short time with improved latency (Atlam and Wills 2019). The cryptography is responsible for recording, managing, and securing transactions across different communication nodes. Every individual node within the network can securely execute a transaction cryptographically without the need for a dominant authority. Cryptography aids DLT for approving and authenticating nodes, verifying records, and aiding consensus when the ledger updates using cryptographic digital signatures for all participating node to validate a transaction (Atlam and Wills 2019). Next are the nodes which characterize the participating users within the distributed ledger network. The nodes have diverse governance and accountable roles within the distributed ledger network including auditor, asset issuer, system administrator, validator, and proposer as seen in Fig. 4.

The system administrator usually implements the control access of the system and carryout management services.

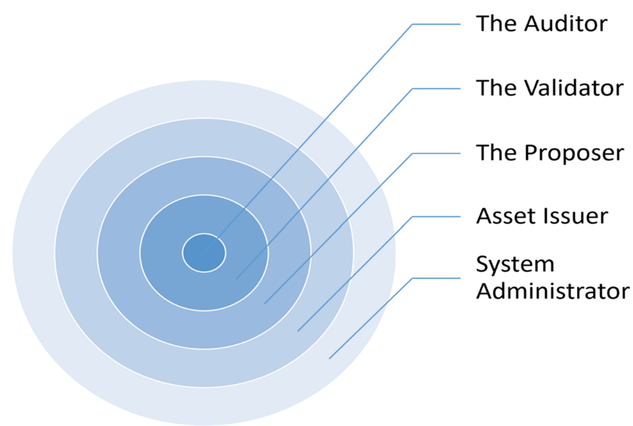
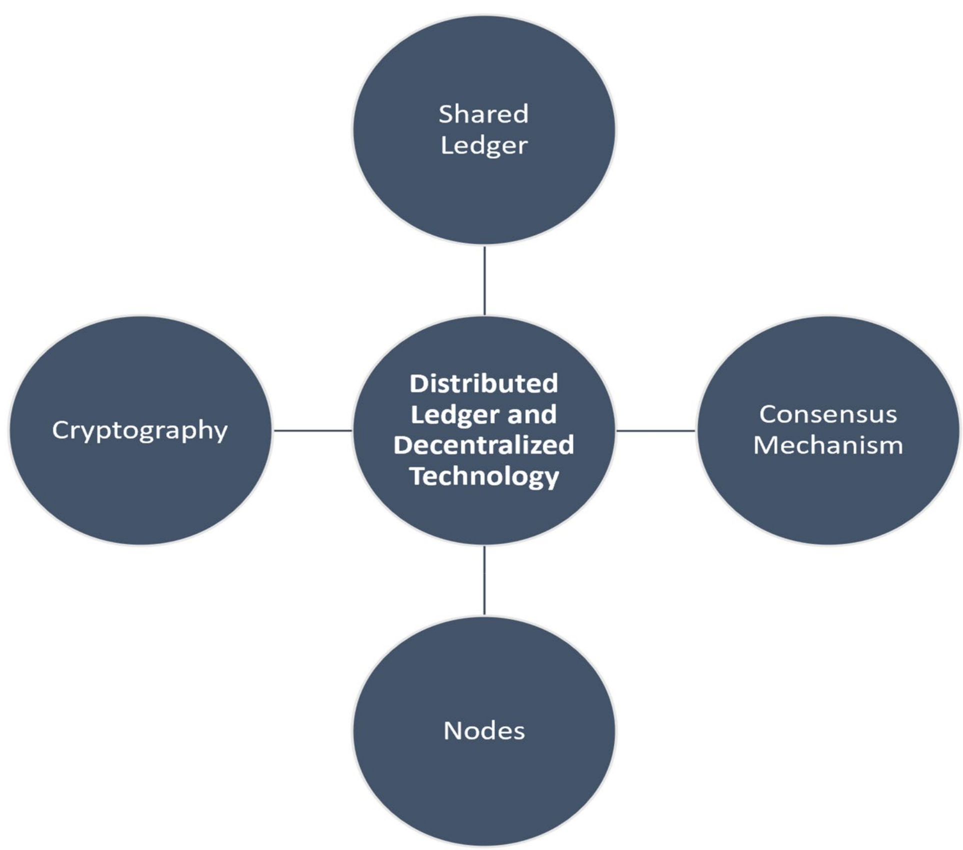


Fig. 4 Governance role of DLT deployed in smart industrial sectors

While asset issuer mostly has the permission to add new assets. The proposer as the title implies propose updates for the distributed ledger network whereas the validator approves the legitimacy of a proposed update within the distributed ledger network. The auditor occupies the least role and has rights to read only or view the distributed ledger network without the permission to apply updates or changes (Atlam and Wills 2019). Furthermore, the consensus mechanism comprises of the process employed by all participating nodes within the network to authenticate the contents of the

Fig. 3 Components of DLT deployed in smart industrial sectors



distributed ledger. Consensus usually comprises of two main phases the validation and ledger update agreement. Presently there exist several consensus mechanisms as discussed in Sect. 4.5.1 However, the most widely adopted mechanisms are proof-of-work (PoW) and proof of stake (PoS) (Nakamoto 2008; Sunyaev 2020). The main difference between different consensus mechanisms is linked to how they reward and delegate the authentication of transactions (Atlam and Wills 2019).

4.2 Characteristics of distributed ledger and decentralized technology

The traditional ledgers have been replaced by digital ledgers which comprising of time-stamped digital data have widely adopted in industries due to digitalization. Thus, digital distributed ledgers are being developed with the use of security protocols, incentive mechanisms, and cryptographic puzzles, to achieve transparency, trust and unlocks innovative platforms that is not orchestrated by a centralized architecture (Zhu et al. 2019). This section identifies the characteristics of distributed ledger and decentralized technology as seen in Table 2.

Table 2 depicts some characteristics of distributed ledger and decentralized technology which makes DLTs suitable to be deployed towards smart industrial transition. DLTs such as Ethereum, Hyperledger, etc. uses smart contracts to deploy the business logic of DLT. Thus, smart contracts are discussed in the subsequent section.

4.3 Significance of smart contracts in DLTs

Smart contract was proposed in 1994 by Nick Szabo who defined smart contract as a set of promises (set of principles and agreements), itemized in digital form, comprising of protocols within which agreed parties perform transactions on these promises (Teslya and Ryabchikov 2017; Rahman et al. 2019). Accordingly, a smart contract is a programmed rules/codes or transaction protocol that executes the terms of a pre-defined terms and contents within the contract, allowing stakeholders to translate prescribed clauses into embeddable code consequently decreasing external risks and participation (Casino et al. 2019; Kaczmarczyk and Sitarska-Buba 2020). The smart contract is also referred to as the business logic of DLTs as it is responsible for reading and writing data to the across the distributed ledger by executing the business logic (Rahman et al. 2019; Dewan and Singh 2020).

A smart contract automatically enforced an agreement between participants which may not trust each other. Therefore, within DLT smart contracts are computer scripts running in a decentralized method and stored in the network without depending on any trusted authority (Casino et al. 2019; Hrga et al. 2020). Smart contracts are mostly programmed using a language called Solidity which is a full-scale programming language like JavaScript (Rahman et al. 2019). As mentioned by Hrga et al. (2020) there are three main types of smart contract platforms and they include financial applications (insurance, custom currencies, and other financial derivatives), semi-financial applications (monetary transactions such as a non-financial side, including bounty programs), and non-financial applications (such as decentralized governance, crowdfunding, online voting, auctions, reputation systems, as well as micropayments etc. (Xu et al. 2019)). Likewise, Dewan and Singh (2020) stated that smart contract aids in getting the consent of all parties as it contains comprehensive description of terms and agreements. Hence, smart contracts can be utilized to deliver digital services such as registry contracts, legal contracts, asset trade contracts, insurance contracts, etc. (Dewan and Singh 2020; Anthony Jr et al. 2021d). Smart contracts help to minimize disputes through an open and shared process (Giraldo 2018).

Additionally, smart contracts are responsible for confirming that all new transactions within the network are compliant with the pre-defined agreed consensus. Thus, covering the agreed consensus within the business agreements and network business rules to build trust within the network (Kaczmarczyk and Sitarska-Buba 2020). Smart contract works by invoking the pre-defined code functions for decision making, data storage, and sending of cryptocurrencies across the network (Rahmadika and Rhee 2018; Howell et al. 2019). As stated by Ølnes et al. (2017) smart contract can be employed in e-voting system powered by blockchain ensuring that a voter can only cast a vote once and check if the vote is properly stored by accessing the data. This can minimize possible voter fraud thus making data manipulation of voting results more challenging because of the distributed ledger of nodes and the distributed network protocol that confirms the data integrity. Therefore, DLT based platforms can range from simpler to complex transactions and data exchange and smart contracts can be utilized to regulate and orchestrate transactions in industries (Ølnes et al. 2017).

4.4 DLT deployment for smart industrial transition

Industries aims to achieve economic advantages mostly through the standardization of organizational and development processes due to increased costs (Anthony Jr et al. 2018). The smart industrial context comprises of digitally interlinked smart factories where production processes are run autonomously based on a decentralized data structure. In smart industrial environment various devices are seamlessly connected preferably using different communication technologies to provide services (Atlam and Wills 2019). In smart industries, information and communication technology

Table 2 Characteristics of distributed ledger and decentralized technology

Characteristics	Description
Flexibility	There are several open source and commercial DLT that industries can adopt to supports their organizational goals without spending much on research and development (Atlam and Wills 2019). DLT also provides design support for maintenance, upgrade, and further development (Sunyaev 2020)
Institutionalization	DLT supports emergent deployment of artifacts and concepts in social structures to support organization process (Sunyaev 2020)
Anonymity	This relates to the extent to which participating users of DLT are not identifiable based on a set of pre-defined subjects (Sunyaev 2020)
Performance	This is associated with the achievement of a given task by DLT assessed against a standards speed, completeness, costs, and accuracy (Sunyaev 2020)
Security	DLTs offers a secure and immutable environment for different industrial systems. It helps to achieve data availability, integrity, and confidentiality (Atlam and Wills 2019; Sunyaev 2020
Usability	Involves the degree to which different users can utilize a DLT platform to attain specified targets with respect to effectiveness in industrial context (Sunyaev 2020)
Block creation interval	DLTs employs different time between repeatedly when a new transaction or data is created (Sunyaev 2020)
Scalability	DLTs possess the ability to manage an increasing volume of workload, or it has the capability to be expanded to accommodate development of more services (Sunyaev 2020; Hussien et al. 2021)
Throughput	This involves DLT`s capability to manage several validated transactions appended to the distributed ledger in a particular time interval (Sunyaev 2020)
Availability	Entails the possibility that a DLT platform operates appropriately at an arbitrary within a given time (Sunyaev 2020)
Integrity	DLT based platforms requires high degree of veracity to store transactions which are protected against unauthorized manipulation or alteration (Sunyaev 2020). DLTs provides a tampered-proof and immutable ledger that cannot be updated without the consent and verification from majority of participating nodes (Atlam and Wills 2019)
Immutability	Involves the capability of DLTs to perform different actions and interactions that can be traced and audited via a distributed ledger (Zhu et al. 2019)
Decentralization	DLT is an autonomic platform managed by stakeholders through a pre-designed consensus mechanism with no main entity (Zhu et al. 2019)
Distributed	DLT employs a distributed and sharing system that provides assurance and auditing of data to improve transparency throughout the industrial process (Zhu et al. 2019)
Transparency	Each participant node within the network can have a complete copy of the distributed ledger meaning that all data in the ledger are open to data providence or tracing (Zhu et al. 2019)
Automation and programmability	Smart contracts in DLT platforms such as Ethereum provide a programmatic user interface within the distributed ledgers which can be automatically executed (Zhu et al. 2019)
Pseudo-anonymity	DLT provides a pseudonym referred to as the address which is employed to conceal the real identity of each participating member node (Zhu et al. 2019)
Tamper-proof	In DLT a new transaction is validated and verified by the consensus mechanism which is appended via cryptographic hash method. Thus, the hash functions and consensus mechanism are deployed to ensure that historical data within the distributed ledger are almost difficult to be altered (Zhu et al. 2019)
Resilient	DLT deploys distributed and decentralized communication between individual nodes within the network to mitigate single point of failure issue (Atlam and Wills 2019)
Susceptibility to manipulation	DLT provides an immutable and decentralized environment which has the capability to detect and stop potential malicious action (Atlam and Wills 2019)
Authentication and access control	DLT provides decentralized authentication logic and rules using smart contracts to enable efficient authentication for smart industrial services (Atlam and Wills 2019)

(ICT) are deployed to manage issues faced by connecting people, infrastructures, and organization to achieve a more sustainable and efficient resource usage (Nagel and Kranz 2020). Smart industries deploy a more agile and efficient system that offers greater flexibility and less production downtime as compared to traditional industries. However, the smart industry concept has not yet fully deployed across industrial environment due to several issues ranging from data interoperability, system integration, data governance, data security, etc. (Roeck et al. 2020; Bokolo 2022).

Therefore, to properly manage DLT governance provided by the digital services deployed in smart industries such as authenticity, access control, and verifiability of DLTs can be employed as it offers a trusted and decentralized ledger of data (Zichichi et al. 2020). Similarly, due to smart industries potential for automation and distributed nature smart industries are an important field for DLT application. DLT is making waves in research and development and has recently been developed as a viable approach for digitalization in the smart industrial domain (Yu et al. 2018; Anthony Jnr and Abbas Petersen 2021). DLTs such as blockchain can enhance supply chain process by offering system resilience, contract automation, visibility, data aggregation (Teh et al. 2020), and data validation to achieve a more stable secured, transparent, robust, efficient business process, and can also facilitate improved interoperable and integration of different industrial departments (Babich and Hilary 2018; Trump et al. 2018a, b). DLT has great potential to open new possibilities to improve the economic and social state of industries by competently establishing trust among machines and people, decreasing cost, and increasing usage of resources (Zia et al. 2020).

DLT offers a promising solution for smart industrial transition by providing transparent and tamper-proof information required during service production and distribution which could be trusted by stakeholders such as the retailers, distributors, manufacturer, deliverer, transporters, and customers (Zhu et al. 2019). In addition, DLT helps to manage data governance as it eliminates bottlenecks within the flow of information as well as stakeholder control by preventing unauthorized data access, deploys policy enforcement, and enabling secure authentication of the identity (Charalampidis and Fragkiadakis 2020). In manufacturing and production industries DLT can supports Machine-to-Machine (M2M) communication without the connection of central servers for achieve a smart factory where systems can offer device decoupled services (Atlam and Wills 2019; Charalampidis and Fragkiadakis 2020). But, while DLT has several advantages, its deployment in the best possible ways in industrial sectors is still being explored in the literature (Yu et al. 2018).

4.5 DLT governance design and archetypes for smart industrial transition

DLT general describes technologies for the distribution, storage, and dissemination of data between users over publicly or privately governance distributed networks (Liu et al. 2020). There are different DLT governance designs of which includes public permissionless, private permissionless, public permissioned, and private permissioned (Zia et al. 2020) and DLT governance archetypes such as public distributed ledgers, private distributed ledgers, federated private distributed ledgers and permission type (permissionless and permissioned) as illustrated in Fig. 5.

Figure 5 depicts permission type (permissionless and permissioned) which determines DLT write permissions. In the permissionless distributed ledgers, all participating nodes have equal write permissions, whereas for permissioned ledgers, network nodes are required to be granted permission to authenticate and commit new transaction or data to the ledger. Permissionless DLT are open source, public, and designed based on the Proof-of-Work consensus algorithm (Trump et al. 2018a, b). Any industrial practitioner can contribute in a permissionless DLT without getting approval by just downloading the needed ledger software and start running it in their machine. The industrial practitioner can send data to the ledger and these transactions will be included within the distributed ledger if its valid (Anthony Jr 2022a). Though DLT transactions are anonymous, the new transactions are transparent to everyone on the network (Liu et al. 2020).

In comparisons DLT governance designs such as public permissionless is typically employed for fully decentralized DLT (Zia et al. 2020), as any individual can access the distributed ledger network at any time and all nodes can contribute to verify, validate, and record transactions. Public permissionless DLTs are mostly secure, immutable, and transparent but are less competent in terms of computation cost and performance (Zia et al. 2020). Next, there are public permissioned DLT that allows individuals to have free access to network nodes without registration. Though, specified individuals can authorize transactions. Public permissioned DLT are more efficient in terms of computation cost and performance as compared to public permissionless DLT. But it is less efficient in security, immutability, and transparency (Zia et al. 2020). Another DLT governance design is the private permissionless DLT which requires a membership procedure for individual industries to access the distributed ledger network. Individual industries are not permitted to use the distributed ledger network before a signed membership contract. Once an industry member signs the contract, they can carry out transactions. In terms of approval, private permissionless DLT permits all its users to contribute to validating transactions. Private permissionless DLT has less computation cost and high performance (Zia et al. 2020). Also, the private permissioned and permissionless DLTs are different from a constraints-based database system where all participants are known, and membership contract exist. This is because in DLT all transactions or data saved cannot be changed once the data has been appended into the distributed ledger, unlike in constraints-based database system where data can still be manipulated by the system administrator. This is unlikely in DLT as its based on consensus mechanism which is not employed in traditional database systems.

Furthermore, the last DLT governance design is the private permissioned DLT which is the most constrained DLT as participating industries are required to sign membership contract before using the distributed ledger network and only limited individuals have rights to verify and accept transactions. Similar to private permissionless DLT, private

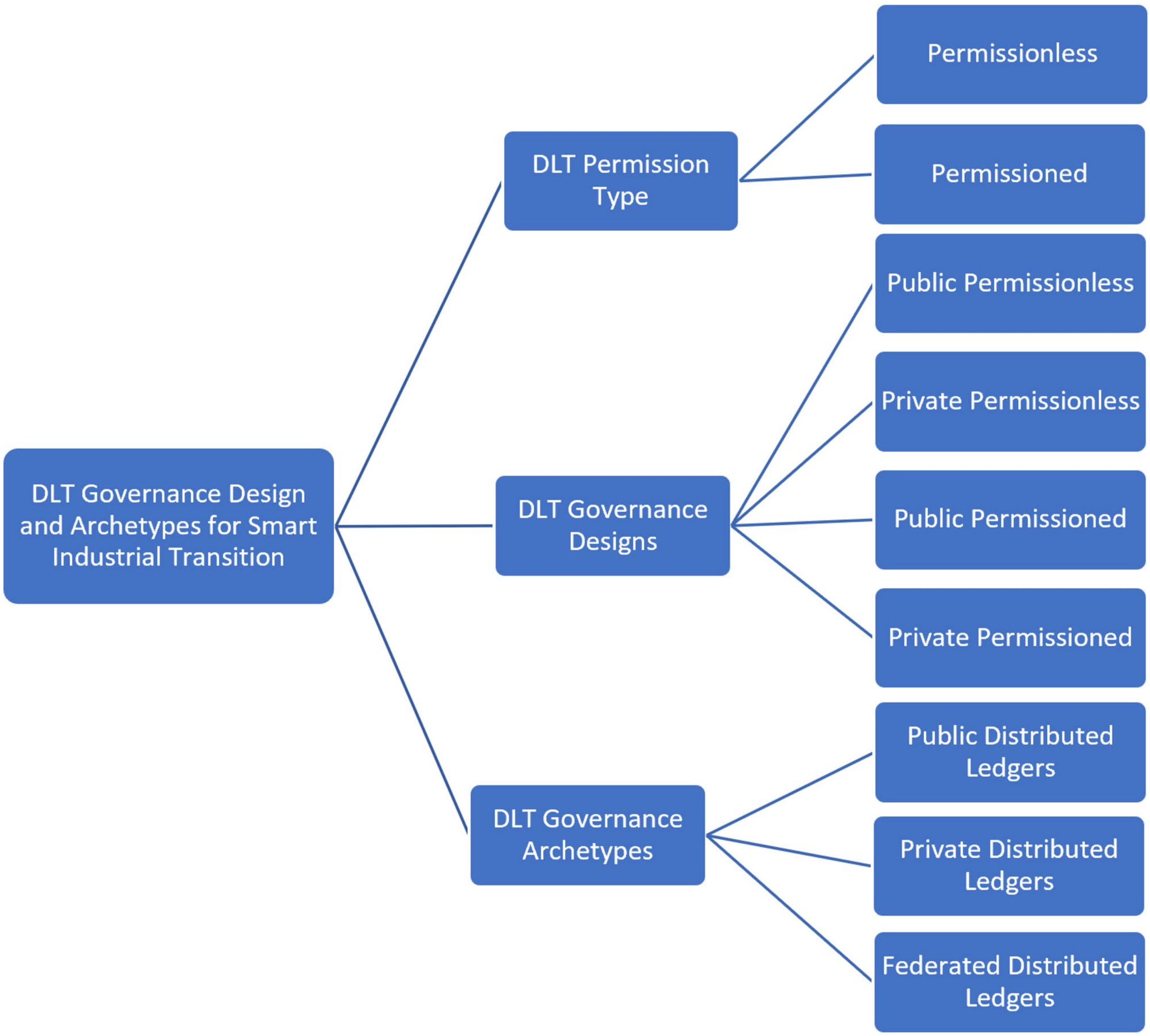


Fig. 5 DLT governance design and archetypes for smart industrial transition

permissioned DLTs are very efficient in term of computation cost and performance. But it lacks security, immutability, and transparency features (Zia et al. 2020). In a publicly distributed ledger, a new node or data can directly append or join the network whereas for a privately owned ledger the new node must get permission to add new data or join the network. Public distributed ledgers design is typically managed by many participating nodes, for instance in Ethereum and Bitcoin. In a public design DLT each node retains a replication of the ledger to attain a high level of availability. To support several (subjective) nodes to find consensus, public distributed ledgers design is scalable not to reduce performance with increased number of nodes (Sunyaev 2020). In contrast, private distributed ledgers design comprises of a definite set of nodes, where each node is identifiable and known to the other nodes within the network. Private DLT are often employed to store data that should not be made available to the public. Accordingly, private DLT design necessitates confirmation of new nodes that join the distributed ledger, for example by using a public key infrastructure (Sunyaev 2020). DLT can be permissioned as well, where permissioned DLTs can be further categorized into public, federated, and private DLTs. Federated DLTs are typically maintained by a special set of participants.

Also, arbitrary participants are not permitted to validate any transaction. Only pre-defined participants are responsible for the process validity of transactions. In federated DLTs public members can be granted the right to read transactions, however only a few selected members can write new transactions. Examples of well-known federated DLTs are R3 enterprise blockchain technology for digital industry transformation used in the financial industry for banking and The energy web foundation (EWF), which is a blockchain based consortium devoted to the energy sector. Additionally, a private DLT is archetypally centralized to one industry and only this enterprise can authorize transactions. The public are not allowed to read the ledger data or transactions, or at times only some designated individuals can access ledger transactions. An example of private DLT is Multichain which helps industries to easily develop and deploy blockchain based applications (Liu et al. 2020). The difference between a private DLT and a federated DLT is the number of industries that operate the DLT. A private DLT is operated by a single industry, whereas, a federated DLT is operated by several industries, although federated DLTs are still be considered as private DLTs (Liu et al. 2020). Based on the literature (Liu et al. 2020; Nagel and Kranz 2020), Table 3 presents a summary of DLT governance topologies. This can be useful for industries to determine which DLT is more suitable for digitalization towards smart industrial transition.

4.5.1 DLT consensus mechanisms for smart industrial transition

Owing to the differences between private and public distributed ledgers design, there exist different consensus mechanisms or algorithms (Sunyaev 2020) responsible for the maintenance of the distributed ledger and the authorization of nodes to join to DLT network. The consensus algorithms make DLT different from conventional distributed database technologies. Moreover, the consensus algorithms are mostly involved in managing the governance and decision making of distributed ledger in relation to how decisions can be made for all member groups who use the DLT platform (Liu et al. 2020). Findings from the literature (Sunyaev 2020) suggested that consensus mechanisms employed for private ledgers are mainly designed for small number of network nodes to achieve consensus. Thus, some consensus mechanisms not suitable for publicly deployed distributed ledgers. In comparison, public consensus mechanisms can be employed to privately distributed ledgers, but the cost of efficiency which relates to high inefficiency or low number of validated transactions per second is affected (Nakamoto 2008). For instance, DLTs such as Ethereum and Bitcoin requires each network node to manage a full replication of transaction stored on the distributed ledger (Sunyaev 2020). A fast consensus can be employed which enhances a throughput of multiple transactions per second.

In permissionless based DLT designs, the nodes' identity is not known since all network nodes have same permissions.

Table 3 Comparison of DLT governance topologies

Topologies	Public	Private	Federated
Permission type of distributed ledger	Mostly permissionless	Mainly permissioned	Mainly permissioned
Reading of distributed ledger	All network nodes can be read, and transactions can be saved by anyone. However, only approved individual nodes can validate data or transactions	It is highly restricted as only approved network nodes can read, submit, and validate transactions	In this DLT only approved network nodes are permitted to read, submit, and authenticate transactions. This is due to restrictions set within the DLT
Writing of distributed ledger	All network nodes are permitted to read, and transactions can be saved by anyone. Although, the approval of transactions is only permitted by a certain group of individual nodes	This DLT is mainly restricted as only approved network nodes can read, submit, and validate any transactions	In this DLT only approved network nodes can read, submit, and validate any transactions based on pre-defined restrictions
Validation of distributed ledger	All individual nodes within the networks can read, save, and validate any transactions	In this DLT only a few authorized members are allowed to carry out validation of transactions	Mostly limited to only few authorized members

Also, permissionless DLT designs comprises of large number of nodes as seen in DLTS such as Ethereum Bitcoin which consensus finding is typically probabilistic and does not offer total finality since it is impossible to achieve finality in the distributed ledger networks which allow network nodes to randomly join or leave (Nakamoto 2008). Accordingly, the uniformity between all network nodes of a public or permissionless distributed ledger can at a point in time only be presumed with a particular probability. Furthermore, a data appended to the distributed ledger is only expected to be immutably retained to a given probability. In DLTs, this probability of a given data or record's immutability increases when new transaction is added to the distributed ledger (Nakamoto 2008). The duration pending when an added transaction is considered immutable is referred to as confirmation latency. In the following, the most widely employed consensus mechanisms by different DLTs deployed in smart industrial sectors are discussed.

a. Proof-of-work (PoW)

PoW was initially designed to prevent denial of service (DoS) attacks and spam e-mails by requiring users to carry out a specified task before requesting a service. PoW concept was later extended and eventually applied as a consensus mechanism in public, permissionless DLT designs such as in Bitcoin (Nakamoto 2008). In distributed ledger the use of PoW as a consensus mechanism entails each node to solve a computationally challenging task before new transactions can be added into the distributed ledger. A reward is allocated to the node which first solves the given challenge and adds computational power. The reward can be in form of coin as in block chain such as Bitcoin with protocol specifying the number of coins. In DLT designs that utilizes blocks, the creation of blocks as a reward is referred to as mining. Where, the nodes that are involved in the mining process are referred to as miners. By regulating the target's effort required the work to be accomplished as PoW is kept in moderation (Nakamoto 2008).

PoW is mostly employed for public and permissionless DLT design with probabilistic finality where the DLT is in an unpredictable state due to forks which appears within the DLT when at least two nodes create blocks almost concurrently permitting the nodes network to accept several blocks as the correct successor of the former block. PoW maintains such forks automatically based on a pre-defined fork resolution rule (Nakamoto 2008). In DLTs such as Bitcoin new mined blocks that are not included in the distributed ledger, are referred to as stale blocks. One of the limitations of PoW is that it consumes energy due to its computationally difficult required to solve complex puzzles and discovery a nonce with a conforming hash value which is lower than the target. Therefore, PoW is often criticized for its inefficiency (Liu et al. 2020; Sunyaev 2020).

PoW provides protection against denial of service (DoS) attacks since it an attacker requires high amount of computational power to successfully breach PoW based DLTs such as blockchain, Bitcoin. Thus, PoW can mitigate DoS attacks on DLTs because it is extremely possible that an attacker has the capability to get enough energy resources and hardware to override the rest of the network nodes. Although, PoW is susceptible to 51% attack, where an attacker has most of the mining power. Thus, an attacker can control the DLT procedures and stop other mining nodes from adding new blocks. Accordingly, the attacker only gets the rewards and can even inverse transactions with 51% of the computing power (Liu et al. 2020).

b. Proof-of-stake (PoS)

PoS is a consensus mechanism that consumes less energy as compared to PoW as it requires less computational power for mining operations. The PoS specifies that the probability of a node mining the succeeding block is closely connected to the reminder of the miner's previously held tokens. In PoS-based DLTs, the new block's creator is selected by means of several combinations of random choices and the stake's age or wealth. Choosing a miner based on its account balance would lead to centralization, since the single richest individual node would have more benefit (Sunyaev 2020). Several selection alternatives were proposed to be employed in PoS such as Delegated PoS (DPoS), coin-age-based selection, and randomized block selection. The randomized block selection adopts the least hash value in combination with the current size of the stake that a specific node holds, predicts the subsequent block miner. But as a miner's stakes are mostly public, a node can predict which node will be selected and assigned the permission to add a block. But this has often been criticized as a limitation.

Next is the coin-age-based selection which integrates randomized block selection with the coin age method. Thus, the larger or older the owned coins are the greater the probability of creating the succeeding block. But, as soon as a miner's stake of coins has been utilized to sign a block, it begins with a coin age of zero and delays for about 30 days before validating another block (Sunyaev 2020). In comparison the DPoS utilizes a limited number of nodes to recommend and authenticate transactions to be appended to the distributed ledger for fast transaction processing. DPoS uses the DLT design of EOS.IO which is based on a set of 21 randomly selected nodes that can participates in verification or creation of new transactions within the distributed ledger (Sunyaev 2020). DPoS-based DLTs do not require powerful computing hardware as a computer with a constant Internet connection is all that is required to be executed as a node. DPoS runs faster as it does not require mining operations as compared to PoW based DLTs. Additionally, DPoS-based DLTs are resilience to 51% attack due to its design but it is challenging to realize full decentralization as DPoS-based DLTS only permits limited numbers of nodes in creating new transactions (Liu et al. 2020).

c. Practical byzantine fault tolerance (PBFT)

PBFT is utilized in private, permissioned DLT designs, where the distributed ledger network owner first examined each of the nodes registered within the distributed ledger. PBFT supports the deployment of high-performance Byzantine fault-tolerant replicated state machines (RSMs), which was proposed by Miguel Castro and Barbara Liskov (Castro and Liskov 1999) to manage the replication same data set across multiple independent devices. RSM also aids the nodes to function as a state machine, which can receive an input in one state and produce an output based on the distinct operations. Thus, RSMs can manage thousands of requests per second, but findings from the literature highlights that RSMs have poor scalability (Castro and Liskov 1999). In the PBFT method all nodes are organized in order where one node is defined as the primary node *p*, with others backup nodes.

All the network nodes across the distributed ledger communicates among each other to ultimately attain consensus on the distributed ledger's succeeding view (Sunyaev 2020). PBFT aids the DLT to tolerate Byzantine faults, i.e. protect against security breach from malicious nodes (Herrera and Kopainsky 2020). PBFT employs a low latency low and overhead time (Liu et al. 2020). The PBFT algorithm can confirm blocks and transactions without requiring approvals as in PoW. Also, PBFT consensus algorithm utilizes significantly lesser energy as compared to PoW. Although it performs well for DLTs of small sizes due to its communication approach among nodes. It is also vulnerable to Sybil attacks and the DLT size cannot be significantly increased just to control Sybil attacks. In smart industrial sectors PoW can be deployed with PBFT to address the Sybil attacks problem (Liu et al. 2020).

d. Delegated proof-of-stake (DPoS)

As previously stated DPoS is another recognized consensus algorithm developed by Daniel Larimer. This consensus algorithm comprises of three groups of governance actors: delegates, witnesses, and stakeholders. The stakeholders are responsible for selection of witnesses. Each stakeholder can only vote one witness. Witnesses with the greatest number of votes are chosen. Stakeholders can vote to increase the witnesses till at least 50 percent of the stakeholders considers that the distributed ledger has attained satisfactory decentralization. The witnesses are accountable for the creation and inclusion of transaction to the distributed ledger. Voted witnesses can take turns to add new blocks in a pre-define timeframes. However, their work quality is monitored by stakeholders via a reputation assessment system. Less acting witnesses will lose their titles or scores. Delegates are also selected by the stakeholders. The delegates are mostly responsible for maintaining the distributed ledger and recommending changes (Liu et al. 2020).

For instance, delegates can recommend remunerated incentive, block size variations, and transaction fee variations. The stakeholders will approve if the suggested changes should be implemented. Rewards can be allocated to delegates as well. DPoS requires less energy as compared to PoW because witnesses produce blocks based on explicit time schedules, rather than contending with each node to add blocks. The computing hardware required is not as demanding as in PoW. Furthermore, DPoS achieves better decentralization since its consensus algorithm permits stakeholders to select suitable witnesses to authenticate transactions. Although, DPoS consensus mechanism can never be completely decentralized, but decentralization can be improved by voting in more witnesses to validate transaction in so doing improves the scalability (Liu et al. 2020).

e. IOTA's directed acyclic graph (DAG)

IOTA is an open source DLT with great potential for applications of M2M suitable for smart industrial environment. IOTA employs a platform called Tangle hashes which uses Winternitz signatures which is a hash-based cryptography deployed alongside an elliptic curve cryptography (Liu et al. 2020). Tangle is operated via IOTA's directed acyclic graph (DAG) which enables new transaction to be validated by at least two preceding transactions before it can be included to the DAG. By deploying Tangle for smart industrial process, all nodes within the IOTA network can issue and authenticate transactions at the same time as data are linked to transactions. Though, Tangle does not store transactions into blocks as in other DLTs such as block chain. Therefore, Tangle is a blockless DLT and does not need mining to achieve consensus. This prevents powerful mining computers and high use of energy.

Also, the no mining policy of IOTA also means no fees are required to recompense miners. Prospective and current industrial practitioners are not required to pay transaction fees as well. Tangle is extremely scalable since it employs DAG as its ledger and instantaneous process transaction. High transactions in a DAG do not delay the IOTA network. Instead, performance is enhanced as the number of transactions or data increases based on the characteristic of concurrent authentication. DAG employed by Tangle has an improved speed as compared to other than DLTs consensus mechanism. The DAG of Tangle employs a coordinator to stop malicious activities since it does not have sufficient transaction nodes to conduct authentication. The coordinator is excluded after the Tangle network becomes self-sustainable (Liu et al. 2020).

4.6 Potential benefits of deploying DLT for smart industrial transition

DLT can decrease complexity of industrial process and automatically improve value chain for stakeholders. This section presents the benefits of deploying DLT in smart industrial environment to practitioners as discussed in Table 4.

Overall, Table 4 discusses the potential benefits of deploying DLT for smart industrial transition which comprises of immutability and verifiability of transactions, managing access control within the organization, decentralization of digital services, pseudo-anonymity and data sovereignty towards data ownership, access and control, efficiency of services, automation of business process, improving business integrity, availability and resilience of critical industrial infrastructure, administering security, improving disrupted capabilities, reinforcing trust, better transparency, preserves user`s privacy, enable tokenization based on digital assets, and lastly reducing associated cost incurred by the industry.

4.7 Factors that impact deployment of DLT for smart industrial transition

Towards the actualization of smart industrial transition DLT can be adopted to track connected industrial devices, facilitate transaction processing and authentication, data synchronization and sharing. Additionally, DLT uses smart contracts to improve connectivity and discover innovative possibilities to improve smart industrial services (Arslan et al. 2020). While DLTs can improve industrial process, it is faced with barriers that impacts its full implementation such as complexity of associated with coding and maintaining smart contracts, confidentiality, storage, interoperability, data reliability, and possible longevity needed (Li and Kassem 2019; Bokolo 2022). Also, the actualization of smart industrial environment based on DLT involves a complex process (Panda et al. 2020), which depends upon various interrelated factors as seen in Fig. 6.

Figure 6 illustrates the identified factors that influences the deployment of deployment of DLT for smart industrial transition. Each of the factors are discussed below.

4.7.1 Awareness and maturity

The deployment of distributed ledger towards smart industries is still in the initial stage of development. There are huge concerns about the resilience and robustness of the DLT particularly for collaborative business process involves several transactions. The negative public perception of users associated to cryptocurrencies which has slowdown the adoption of such technology (Priem 2020). Similarly, there is limited understanding among industrial practitioners about how DLTs such as blockchain, IOTA Tangle, etc. can and achieve business development. Though IT industries such as IBM and Microsoft have started to develop digital products and services based on DLT which provide confidence and trust in the potentials of DLT (Ferraro et al. 2018; Atlam and Wills 2019; Priem 2020).

4.7.2 Interoperable standard

The deployment of different distributed ledger platforms that need to be integrated with existing infrastructures may require large expenditures and extensive coordination. Achieving an eco-system of different software solution to work efficiently towards supporting diverse services with DLT may be challenging to achieve (Atlam and Wills 2019). Also, a smart industrial process may involve multiple DLT systems as DLTs are public or privately deployed a complex workflow involving production records, delivery of products, and payments may be a difficult workflow. Likewise, conversion and transfer of data from one distributed ledger to another to how these data from one distributed ledger can be utilized by another DLT is still an issue. Thus, there are issue related to standards to ensure that DLTs can be interoperable across applications (Zhu et al. 2019).

4.7.3 Energy efficiency

DLTs are considered as being high consumers of energy which is mostly due to the consensus mechanisms employed and peer-to-peer communication protocol deployed for synchronizing the distributed ledger (Panda, et al. 2020). For smart industrial environment it is required to have a reliable and long-lasting node which comprise of energy efficient hardware that can perform computations with less power.

4.7.4 Data storage capacity

Smart industries now deploy smart devices that generates real-time Terabytes of data that needs to be stored and processed to produce insights (Agbo et al. 2019; Atlam and Wills 2019). But the deployment of DLTs such as blockchain is not developed to retain huge amounts of data like those produced by devices in smart industrial environment. Hence

Table 4 Potential benefits of deploying DLT for smart industrial transition

Potential benefits	Description
Immutability and verifiability	DLTs confirms the integrity of transactions by creating verifiable and immutable ledgers. As data cannot be changed pending the approval from participating nodes within the distributed ledger network (Atlam and Wills 2019)
Manage access control	The inbuilt cryptographic capability of DLT can be employed to regulate access to private data saved in the distributed ledger from authorized access (Panda et al. 2020)
Decentralization	DLT employs a decentralized infrastructure in nature using a shared ledger that provides all participating nodes the capability to have an original copy of the ledger without the controlled of a central authority (Atlam and Wills 2019)
Pseudo-anonymity and data sovereignty	Transactions within a distributed ledger are pseudo-anonymous based on the cryptographic nature which encrypts transactions. This aids each node user to manage access to and govern ownership of their own information (Cullen et al. 2020)
Efficiency	DLT decreases the efforts required for business settlement which are mostly handled manually in traditional industrial environment. DLT helps to achieve efficient business process through immutability and distributed features (Atlam and Wills 2019)
Automation	DLT supports computerization of industrial operations to smart industrial environment so business operations can be intelligently verified automatically. This feature is deployed by smart contracts which creates digital contracts by executing contracts condition among partners as programming actions and conditions. These business actions are repeatedly implemented as soon as the set business conditions are verified (Atlam and Wills 2019). Smart contracts can automate industrial transactions and improve open areas machine-to machine interactions required in smart industrial environment (Babich and Hilary 2018)
Improves integrity	Maintaining transaction or data integrity means that communicated information must not be modified during transmission. In smart industrial environment data integrity is importance as it ensures the consistency of the data throughout product or service lifetime. This can be realized by permitting only authorized users to manage stored data. The immutability feature of DLTs such as IOTA can be employed to enforce integrity which ensures that once a record in retained in the ledger it cannot be changed. Also, block hash is employed in block chain to calculate the existing block hash and the Merkle root value which makes it computationally impossible for a data or content of a block to be altered (Panda, et al. 2020)
Availability and resilience	DLT offers a high level of accessibility as it can run on a nonstop base supposedly. The shared and distributed nature of DLT enables data and processes recovery in case of cyber-attack (Atlam and Wills 2019). Moreover, DLT removes the single point of system failure which affects the resilience of the system (Atlam and Wills 2019). Thus, the distributive architecture makes it possible for DLT platforms to continue offering service if a node fails (Panda, et al. 2020). However, findings from the literature (Atlam and Wills 2019) mentioned that the availability of distributed ledger has not been well tested specifically when large volumes of data are involved
Enforces security	DLT provides security since it uses public key that guards against malicious attackers (Cantelmi et al. 2021). This helps to guarantee security and integrity features of the employed consensus mechanism (Atlam and Wills 2019). In smart industrial environment each factory devices have their own unique ID and asymmetric key pair managed by a security protocol. The cryptographic state of DLT means that issues such as key distribution and management are intrinsically handled (Cullen et al. 2020)
Disrupted capabilities	The openness of distributed ledger unlocks possibilities for innovate business models such as peer-to-peer services. Specifically, the deployment of DLT in smart industrial environment has the prospect to actualize the sharing economy paradigm across several industries at a global scale (Maull et al. 2017)
Trust	DLT employs a distributed consensus mechanism that supports data exchange without the need for a trusted central authority to confirm data integrity. In smart industries this would enable physical devices within the factory to communicate with one another without requiring a centralized server (Cullen et al. 2020). DLT build a distributed framework for smart factory resulting in a secure, robust, and transparent, architecture (Panda, et al. 2020)
Transparency	DLT provides data transparency by sharing transaction among all members nodes involved in the transactions (Atlam and Wills 2019). The shared distributed ledger substitutes the need for trusted third-party mediators with an agreement of appropriateness that provides a transparent, immutable, and irreversible record of transactions (Maull et al. 2017). In smart industries this would enable different devices to orchestrate their use in order to accomplish a common goal as each device owns a copy of the distributed ledger and can validate the correctness of the data (Cullen et al. 2020)

Table 4 (continued)

Potential benefits	Description
Preserves privacy	Privacy of identity and information is important and has been of critical concern for smart industrial transition. The huge amount of data produced by smart devices deploy in smart industries environment may expose sensitive data like personal information of practitioners. Hence, it's important that practitioners should have complete control to disclose their information publicly or not. Data decentralization in DLT confirms sensitive data is not controlled by any central authority or third party. The anonymity of distributed ledger can be exploited by smart industrial systems to preserve user's privacy (Panda et al. 2020)
Enable tokenization based on digital assets	DLT can create verifiable digital entitlements as "tokens" align to inventory, financial assets, and production thus facilitating the trading, exchange, and sharing of factory assets among multiple practitioners. This supports the integration, coordination and synchronization of distribution chains and trading of digital assets thereby minimizing transaction and legal costs (Babich and Hilary 2018)
Reduces cost incurred	DLT shares its contents with nodes within the distributed ledger network thus providing each participating user with a copy of the original ledger without requiring a central authority. This decreases costs related with issuing and managing the ledger. DLT lower organizations costs of adding new data, user, and record validation (Babich and Hilary 2018). Thus, the adoption of distributed ledger in industries removes maintenance costs of each ledger and minimize costly enterprise continuity plans. Likewise, it diminishes costs incurred to confirm data integrity as distributed ledger are immutable in nature (Atlam and Wills 2019)

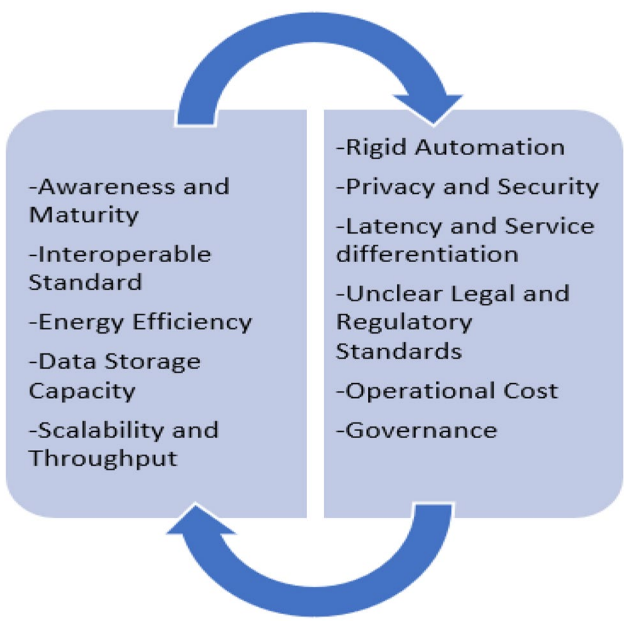


Fig. 6 Factors that impact deployment of DLT for smart industrial transition

storage capacity is seen as one of the issues faced by DLTs (Atlam and Wills 2019; Panda, et al. 2020).

4.7.5 Scalability and throughput

Presently, existing DLTs such as Ethereum and Bitcoin can process about 20 and 7 transactions per second, individually. This current processing speed cannot manage the processing required smart industrial environment which comprises of different machines connected to different system with millions of transactions. Besides, the reduced bandwidth associated with DLTs cannot facilitate real-time transaction processing (Atlam and Wills 2019), due to high transaction volume and required speed verifications. This has negative implications on DLT throughput (Zhu et al. 2019; Panda et al. 2020). The throughput of DLTs is associated to the transaction authentication time and communication dissemination time. Thus, the time taken by consensus algorithm is linked to the time each node must execute and carryout data validation to maintain the accuracy of the ledger. The throughput is still an open challenge issue being address in the literature (Panda et al. 2020).

4.7.6 Rigid automation

The pre-defined rules programmed in smart contracts are written ahead of a system's deployment and are not easily dynamically updated and this may become too rigid for some dynamic environments such as in smart industrial sectors. These unforeseen outcomes may result to immutable changes stemming from the "black box" state of DLTs (Babich and Hilary 2018).

4.7.7 Unclear legal and regulatory standards

DLT is a decentralized infrastructure that has developed across different countries to manage data communication across different devices deployed in smart industrial sectors. DLT must also abide to each country's rules and regulations regarding data privacy (Atlam and Wills 2019). But DLT is still faced with unclear government directives (Priem 2020).

Accordingly, data regulations that deal with information privacy and information handling are still an issue to be tackled in the adoption of distributed ledger technology as these ledgers can collect data from individual nodes from across countries without having any compliance or legal code (Atlam and Wills 2019). Over the years there has been report of DLTs such as bitcoins used to sponsor illegal conducts and fraudulent transactions (Agbo al. 2019). Thus, a regulatory standard for distributed ledger is needed to manage the validity of data stored within the distributed ledger. This will ensure that DLT as an emerging technology is in line with other similar technologies such as artificial intelligence, internet of things, etc. Moreover, this will reinforce that DLT is not used for illegal activities and protect all stakeholders' interests. This will improve the benefits to be derived from DLT for smart industrial transition as seen in Table 4. Similarly, a standardized rule is required for data protection and verifying the identity of valid nodes within the distributed ledger network. Although regulatory standards that govern DLT deployment across the world are not available (Atlam and Wills 2019). This calls for a standardization approach to facilitate the governance of the entire DLT eco-system (Bokolo 2022).

4.7.8 Operational cost

The deployment of DLTs still encompasses the transmission of huge amount of data and metadata for example the block header in blockchain which requires huge traffic payloads. Thus, practitioners create transactions which required a fee to be paid to the DLT nodes that authenticates these transactions (Danzi et al. 2020). Another issue is the cost associated with ledger replications which results to higher cost in operating servers which constantly stores and authenticates the distributed ledger (Danzi et al. 2020).

4.7.9 Latency and service differentiation

As the number of transactions within the ledger rapidly increases in size the transaction time of the distributed ledger begins to slow (Charalampidis and Fragkiadakis 2020). Similarly, the increase of contributing nodes within the distributed ledger network adds more latency which logarithmically increments as new users are added. Thus, DLT may be ineffective to scale up to process increased data transactions in smart industrial environment (Atlam and Wills 2019). There can also be latency when publishing new information to the distributed ledger precisely the authentication delay which may lead to slow real-time reporting (Danzi et al. 2020). In addition, DLT platforms do not offer service differentiation, which poses challenges for smart industrial applications that require to achieve high reliability. DLTs are generally application-based, and the transaction prioritization and the importance of transactions transmitted are based on fee paid. Hence, the authentication delay for a particular transaction relies on its importance with respect to other transactions waiting to be authenticated by the distributed ledger network (Danzi et al. 2020).

4.7.10 DLT governance

In the deployment of distributed ledger technology environment there are still issues related to governance and access rights. Thus, the initiation of an active governance policy for the overall DLT infrastructure is still needed to achieve an effective governance. In permissioned or permissionless DLT it is uncertain how to apply governance as the administrator in DLTs such as the permissioned DLT can be subjected to explicit governance structure or hierarchy depending on the type of the DLT (Atlam and Wills 2019).

4.7.11 Privacy and security

Data privacy is an issue faces mostly in publicly based DLTs where all participating nodes in the distributed ledger network can access the values of all transactions (Babich and Hilary 2018). This can result to disclose of user's private information. Information may be utilized for unintended use and false transactions may be more challenging to delete as the distributed ledger increases (Babich and Hilary 2018). So, the uses of distributed ledger for smart industrial transition may not be a smart initiative as may result to loss of trade secret or risk of confidentiality (Atlam and Wills 2019). Also, DLT provides a tamper-proof an immutable ledger that guarantees data integrity however the saved data can be corrupted before being saved into the distributed ledger by malicious intruder (Atlam and Wills 2019). Likewise, if one node is breached the entire distributed ledger network will be in danger (Agbo et al. 2019).

4.8 Recommendations towards deploying DLT for smart industrial transition

The deployment of distributed ledger technologies is continuously increasing in providing digital solutions in several industries. DLT platforms offers numerous benefits when deployed such as decreasing cost incurred, enhancing operational processes, improving transparency, etc. Yet, DLTs are faces with several challenges as discussed in the subsequent section. One of such issues relates to the privacy of participants which is extremely important so that it is difficult to identify patterns and associate data to real identities (Charalampidis and Fragkiadakis 2020). To address privacy without breaching international laws such as the general data protection regulation (GDPR), encryption techniques, advanced obfuscation, and avatars based tokenized identity can be integrated to enhance node participants privacy (Priem 2020; Zia et al. 2020). Avatars employs pseudonymous identities linked to the original source data stored in a separate ledger maintained by a trusted gatekeeper who assigns certain rights to the node avatars perform certain account management. There is also risk associated with incompatibility and lack standardization between different systems which prevents interoperability of DLTs resulting to fragmentation (Zia et al. 2020; Bokolo 2022).

Nonetheless, there are common DLT standards and protocols developed by companies such as the Post-Trade Distributed Ledger Group, HyperLedger Linux Foundation, etc. that provides an establishment of agreement related to standardized DLT solutions, but this may reduce the speed of DLTs (Priem 2020). Security and energy consumption are also issues associated with DLTs deployment. Cryptographic encryptions employed within the distributed ledger must be robust to resist cyber-attacks and make DLT platform tamperproof. However, publicly based DLTs consumes high electricity to safeguard system security. Hence, the objective is to achieve both the optimal security and less energy consumption for an effective real-life deployment of DLTs (Zia et al. 2020). Also, mining in DLTs is a complex operation that consumes huge amount of energy, employing sophisticated AI techniques with DLTs can help optimizing energy utilization of consensus mechanisms of DLTs deployed for smart industrial environment (Atlam and Wills 2019). This is because AI can help when deploying DLT in industries by providing predictive modelling and forecasting the inflexible DLT energy consumption based on electricity consumption load curves, pattern recognition, and real-time analytics to control electricity resource efficiency (Anthony et al. 2019; Jnr et al. 2020). The accuracy of such advanced AI systems can guarantee optimizing multimodal visualization for energy consumption by DLT platforms deployed as well as the industrial demand-side management, which allows for efficient energy use (Anthony Jr 2021a).

Apart from technological based issues, there is also lack of social awareness on the usefulness of DLT. Society awareness regarding the benefits of DLTs can carried out by using public campaigns and advertisements depicting the advantages of distributed ledgers towards smart industrial transition. Additionally, current governance regulation and laws still do not broadly defined DLT deployment in industries. These policies are essential to define transaction mechanism, privacy standards, data integrity, etc. (Zia et al. 2020; Bokolo 2022).

4.8.1 Recommendation to improve DLT governance and security

The deployment of DLTs in smart industrial environment is dependent upon how practitioners secure access to the distributed ledger either as public or private/permissionless or permissioned access as seen in Fig. 5. Besides, other technical factors are considered such as the availability of computing energy to store and process huge amount of data in addition to the significant electricity needed to power the DLT platform, and recurrent long delays needed to process industrial transactions (Trump et al. 2018a, b; Anthony Jr, 2021b). Moreover, socio-political requirements and standards must be considered as each country has different governance policies such as the EU general data protection (GDPR) (Trump et al. 2018a; b; Kannengießer et al. 2020). As it is quite difficult to adhere to the requirements stipulated by the EU GDPR as if personal user's data are stored in the distributed ledger since GDPR requires for a possibility to totally delete personal user data. Data from participating nodes are required to enhance the flexibility and adaptation of DLT applications thus there is need for software developers to judiciously govern which data should be stored on the distributed ledger or off the distributed ledger (Kannengießer et al. 2020).

Additionally, it remains completely clear how to offer flexibility for DLTs to become compliant with future standards or regulations and at the same time attain a high level of integrity. Therefore, private data should be mostly stored off the distributed ledger. However, offline stored data are managed by at least one trusted third party which limits the decentralization of platforms connected to the distributed ledger. As these external offline data are needed to be confidentially stored and made available for the distributed ledger. The interoperability of distributed ledger designs with oracles have becomes significant for DLT governance archetypes (Anthony Jnr 2022a, 2022b). Besides, the oracles must also be compliant and adhere to laws and regulations that governs DLT usage in smart industrial sectors (Kannengießer et al. 2020). As DLTs across different smart industrial sectors there is need or certain policies to prevent malicious, unintentional misuse of distributed ledger as its governance includes a broad variety of actors as seen in Fig. 4.

Furthermore, DLT infrastructures can be affected by potential security attacks and can be used to foster crimes. One of these vulnerabilities of DLTs is linked to its consensus mechanism (PoW), which is disposed to 51% security attack (Nakamoto 2008). This is possible if the computational power of an individual miner node exceeds 50% of the overall power of the whole DLT network, then the entire distributed ledger could hypothetically be managed by the attacker (Liu et al. 2020). Likewise, the 51% security attack can also take place in a PoW based DLT network if the number of stakes maintained by a single node is higher than 50% of the total DLT network. The orchestrators of a 51% security attack have the capability to reverse transactions, carryout double spending, reject transactions, reorganize transactions thus creating problems for normal transaction and stopping the mining procedures of other mining nodes (Liu et al. 2020; Sunyaev 2020). Another vulnerability faced by DLTs is the Sybil security attack which takes advantage of the possibility that public based DLT networks have no centrally trusted nodes, and all transactions are sent to other nodes within the network for processing. A Sybil security attack is introduced when an attacker allocates some identifiers to the same node giving the attacker the power to outvote genuine nodes to takes control of the entire DLT network (Sunyaev 2020).

A private key which simply contains user identity can be another source of security vulnerability in DLT infrastructure. A private key is mostly utilized to sign transactions and authenticate asset owners. Private keys can also be utilized for transaction validation and node block verification. But a valid user's private key can be lost and when this happens it is difficult to recover the users private key. The genuine user will not have access his/her profile on the distributed ledger network, and this may result to lose of the users' assets (Liu et al. 2020). Accordingly, the management of public or private key pair should be made secure and easy for users, security management tools can be used for industrial users for the organization of users' private and public and keys. Similarly, if a private key is taken by an illegal user, the valid user's profile can be tampered. If any damage is initiated by the criminal, it is usually challenging to recover, repair, and track such actions as there are no centralized third party to technical support (Kannengießer et al. 2020).

On the other hand, blockchain networks can be used by criminals to commit crimes (Liu et al. 2020). One such case is ransomware which encrypts the files of the victim. DLTs such as Blockchains can also be utilized by criminals for underground business to market weapons, drugs, etc. Due to DLT's anonymous nature, it is problematic to track down the parties involved (Liu et al. 2020). Additionally, there are legal issues associated with DLT use in smart industrial sectors for instance, the deployment of smart contract which may challenges the conventional legal ethics of contract regulation such as contract creation and termination (Trump et al. 2018a; b). Such DLT based platforms make it challenging for law courts to resolve any future disputes arise over a use of smart contract since its use is based on a decentralized trustless architecture. Correspondingly, there are jurisdiction issues as distributed ledgers are connected to several participating nodes from different jurisdictions across the world, it can create challenge from a jurisdictional viewpoint (Atlam and Wills 2019).

5 Discussion and implications

5.1 Discussion

Currently industrial operations are being developed because of the digitalization which involves the adoption emerging technologies such as DLT and smart contracts systems. Distributed ledger technologies provide a new promising tool that can help in the distributed management of smart industrial services (Bertone al. 2019; Anthony Jr 2022b). DLT is being adopted in different areas such as supply chain management, healthcare, finance, energy, transportation, etc. Several DLT platforms are being implemented but only a few are truly deployed in industries (Sunyaev 2020). This study provides insights on the intersection between distributed ledger technology and smart industrial transition. For this purpose, this current study provides evidence grounded on secondary data on the deployment of DLT to support smart industrial transitions. Overall, findings from this article presents DLT governance and security issues faced in smart industrial environment.

Particularly, similar to prior study (Nagel and Kranz 2020), this study provides insights on the characteristics of distributed ledger and decentralized technology and significance of smart contracts to shapes the creation, capture, and delivery of economic value for industries. The findings also present the DLT permission type, governance designs, and archetypes for integrating DLT for digitalization of smart industries. Besides, the practical benefits and challenges face in achieving a smart industrial operation are discussed. Finally, the findings present several factors that may impacts the deployment of DLT for smart industrial transition. The findings further show how DLTs impacts and enables business models and which governance design, and archetypes are used in industrial sectors. Thus, this study provides factors that impacts deployment of DLT for smart industrial transition and can serve as a foundation for further theorizing in developing a research model. Additionally, this study contributes to research on smart industry as the author scrutinize how a digital innovation such as DLT can be integrated to disrupt and positively transform industrial operation.

5.2 Theoretical and industrial implications

DLT has become extensively recognized beyond the financial sector to industrial domain. Findings from this study will be useful for regulators, practitioners, and researchers interested in gaining practical insights about how industries can leverage distributed ledgers to create and capture value towards smart industrial transition. This article provides practitioners with a deeper insight into viability of DLT governance designs and archetypes for execution of DLT and their possible impacts on practitioners' decision supports for DLT design. The derived DLT governance design and archetypes suggest potential benefits and drawbacks for deployment of DLT which provide insights to industries towards assessing which consensus mechanisms should be adopted in their distributed ledger to avoid the deployment of unsuitable DLT design and archetypes and consequent waste of technological resources. Moreover, the careful selection of DLT design and archetypes is crucial to guarantee that DLT's unique advantages can be attained, eventually, promoting distributed ledger technologies from a hype to an important infrastructure for future industrial development.

5.3 Practical and managerial implications

DLT is considered as crucial technology for digitalization and the attainment of smart industrial transition for future virtual enterprise collaboration in the digital age. This work contributes to the viable deployment on DLT by discussing benefits, drawbacks, and recommendations for adoption of DLT and presenting DLT governance designs and archetypes. This work provides a guide and roadmap for researchers and practitioners to better understand how to practically improve security drawbacks that affects the deployment of DLT in smart industrial environment. Overall, this article contributes to the scientific knowledge base by exploring the extent to which DLT can support digitalization to achieve smart industrial process by discussing the components of DLT deployed in smart industrial sectors. Findings from the literature are attempting to solve the operational and technological issues still faced by DLT systems such as the integration of technical standards, resolving polices and regulations, etc. This article presents the technological, organizational, environmental, and human factors that impact DLT deployment in smart industries.

6 Conclusion

Industrial sectors are faced with many challenges which ranges from data interoperability, lack of trust, system integration, low productivity, inadequate collaboration, poor compliance and regulation, information sharing, etc. (Bokolo 2022). DLT is being employed to foster the digitalization of the industrial sectors to optimize and improve industrial process. However, the deployment DLT in smart industrial environments is still not well researched. Therefore, the aim of this article is to address this gap by examining the practical benefits and challenges face in achieving a smart industrial operation for digitalization. Also, this study identifies several factors, governance and security issues that impacts DLT deployment in industrial sectors. This paper depicts the synergy between smart industries and DLT which is believed to still be in its infancy by providing a taxonomy for DLT governance design and archetypes. This article has provided an overview of the fundamental characteristic of DLT, identifying the key challenges, benefits, and recommendations of deploying DLT to create innovative applications and services.

Evidence from this study reveals that integrating DLT to smart industrial sectors can bring countless benefits. For instance, the decentralization architecture of distributed ledger can process millions of transactions between factory devices. This current study is faced with a few limitations first only secondary data from the literature was employed. As DLT deployment are currently in their infancy there is need to carryout case study research to in future to provides insights on the current state of DLT deployment in smart industrial environments. Data can be collected using semi-structured interviews to provide insights and further validate the DLT governance design and archetypes presented in this study towards developing a theory-based or practically oriented model that can be employed to assess DLT deployment in smart industrial sectors. Additionally, longitudinal data from survey questionnaire would be valuable to better understand the real-life impact of the identified factors and how they impact DLT deployment in smart industries.

Author contributions AJB conducted the review of the literature and wrote the manuscript.

Funding Open access funding provided by Institute for Energy Technology. This study did not receive any funding.

Declarations

Conflict of interest The author declare that they have no conflict of interest.

References

Agbo B, Qin Y, Hill R (2019) Research directions on big IoT data processing using distributed ledger technology: a position paper. IoTBDS. Science and Technology Publications, pp 385–391

Anthony B Jr (2021a) Exploring data driven initiatives for smart city development: empirical evidence from techno-stakeholders' perspective. Urban Res Pract. https://doi.org/10.1080/17535069.2020.1869816

Anthony B Jr (2021b) Integrating electric vehicles to achieve sustainable energy as a service business model in smart cities. Front Sustain Cities 3:685716

Anthony B Jr (2021c) Distributed ledger and decentralised technology adoption for smart digital transition in collaborative enterprise. Enterp Info Syst. https://doi.org/10.1080/17517575.2021.1989494

Anthony B Jr (2021d) Managing digital transformation of smart cities through enterprise architecture–a review and research agenda. Enterp Info Syst 15(3):299–331

Anthony B Jr (2022a) Toward a collaborative governance model for distributed ledger technology adoption in organizations. Environ Syst Decis 42(2):276–294

Anthony B Jr (2022b) Investigating the decentralized governance of distributed ledger infrastructure implementation in extended enterprises. J Knowl Econ. https://doi.org/10.1007/s13132-022-01079-7

Anthony B Jr, Abbas Petersen S (2021) Examining the digitalisation of virtual enterprises amidst the COVID-19 pandemic: a systematic and meta-analysis. Enterp Info Syst 15(5):617–650

Anthony B Jr, Majid MA, Romli A (2018) A collaborative agent based green IS practice assessment tool for environmental sustainability attainment in enterprise data centers. J Enterp Inf Manag 31(5):771–795

Anthony B, Petersen SA, Ahlers D, Krogstie J, Livik K (2019) Big data-oriented energy prosumption service in smart community districts: a multi-case study perspective. Energy Info 2(1):1–26

Anthony B Jr, Petersen SA, Ahlers D, Krogstie J (2020) Big data driven multi-tier architecture for electric mobility as a service in smart cities: a design science approach. Int J Energy Sect Manage 14(5):1023–1047

Anthony B Jr, Petersen SA, Helfert M, Ahlers D, Krogstie J (2021e) Modeling pervasive platforms and digital services for smart urban transformation using an enterprise architecture framework. Inf Technol People 34(4):1285–1312

Arslan SS, Jurdak R, Jelitto J, Krishnamachari B (2020) Advancements in distributed ledger technology for Internet of Things. Internet Things 9(1):100114

Atlam HF, Wills GB (2019) Intersections between IoT and distributed ledger. Advances in Computers. Elsevier, pp 73–113

Babich V, Hilary G (2018) Blockchain and other distributed ledger technologies in operations. SSRN. https://doi.org/10.2139/ssrn.3232977

Bertone F, Caragnano G, Simonov M, Goga K, Terzo O (2019) A classification of distributed ledger technology usages in the context of transactive energy control operations. Conference on complex, intelligent, and software intensive systems. Springer, Cham, pp 876–885

Bokolo AJ (2022) Exploring interoperability of distributed ledger and decentralized technology adoption in virtual enterprises. Info Syst e-Bus Manag. https://doi.org/10.1007/s10257-022-00561-8

Cantelmi R, Di Gravio G, Patriarca R (2021) Reviewing qualitative research approaches in the context of critical infrastructure resilience. Environ Syst Decis 41(3):341–376

Casado-Vara R, Corchado J (2019) Distributed e-health wide-world accounting ledger via blockchain. J Intell Fuzzy Syst 36(3):2381–2386

Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat Info 36:55–81

Castro M, Liskov B (1999) Authenticated byzantine fault tolerance without public-key cryptography. MIT Laboratory for Computer Science

Charalampidis P, Fragkiadakis A (2020) When distributed ledger technology meets internet of things--benefits and challenges. Preprint at https://arxiv.org/abs/2008.12569.

Cullen A, Ferraro P, King C, Shorten R (2020) On the resilience of dag-based distributed ledgers in iot applications. IEEE Internet Things J 7(8):7112–7122

Danzi P, Kalor AE, Sorensen RB, Hagelskjær AK, Nguyen LD, Stefanovic C, Popovski P (2020) Communication aspects of the integration of wireless iot devices with distributed ledger technology. IEEE Netw 34(1):47–53

Dewan S, Singh L (2020) Use of blockchain in designing smart city. Smart Sustain Built Environ 9(4):695–709

Ferraro P, King C, Shorten R (2018) Distributed ledger technology for smart cities, the sharing economy, and social compliance. IEEE Access 6:62728–62746

Giraldo J (2018) X-border platforms: the implications of distributed ledger technology. Twenty-sixth European conference on information systems (ECIS2018). AIS

Gräbe F, Kannengießer N, Lins S, Sunyaev A (2020) Do not be fooled: toward a holistic comparison of distributed ledger technology designs. Proceeding of the 53rd Hawaii International Conference on System Sciences. SSRN

Herrera H, Kopainsky B (2020) Using system dynamics to support a participatory assessment of resilience. Environ Syst Decis 40(3):342–355

Hofman WJ (2020) Supply chain visibility ledger. Blockchain and distributed ledger technology use cases. Springer, Cham, pp 305–329

Howell BE, Potgieter PH, Sadowski BM (2019) Governance of blockchain and distributed ledger technology projects. SSRN. https://doi.org/10.2139/ssrn.3365519

Hrga A, Capuder T, Žarko IP (2020) Demystifying distributed ledger technologies: limits, challenges, and potentials in the energy sector. IEEE Access 8:126149–126163

Hussien HM, Yasin SM, Udzir NI, Ninggal MIH, Salman S (2021) Blockchain technology in the healthcare industry: trends and opportunities. J Ind Inf Integr 22:100217

Kaczmarczyk A, Sitarska-Buba M (2020) Enterprise architecture of the blockchain platform. J Internet e-Bus Stud 212848:1–12

Kannengießer N, Lins S, Dehling T, Sunyaev A (2020) Trade-offs between distributed ledger technology characteristics. ACM Comput Surv (CSUR) 53(2):1–37

Kuo PH, Mourad A, Ahn J (2018) Potential applicability of distributed ledger to wireless networking technologies. IEEE Wirel Commun 25(4):4–6

Lacity MC (2018) Addressing key challenges to making enterprise blockchain applications a reality. MIS Q Exec 17(3):201–222

Lamberti R, Fries C, Lücking M, Manke R, Kannengießer N, Sturm B, Sunyaev A (2019) An open multimodal mobility platform based on distributed ledger technology. Internet of things, smart spaces, and next generation networks and systems. Springer, Cham, pp 41–52

Li J, Kassem M (2019) A roadmap to achieving readiness for macro adoption of distributed ledger technology (DLT) in theconstruction industry. Creative construction conference 2019. Budapest University of Technology and Economics, pp 2–7

Liu X, Farahani B, Firouzi F (2020) Distributed ledger technology. Intelligent internet of things. Springer, Cham, pp 393–431

Lu J, Zheng X, Hu Z, Zhang H, Kiritsis D (2020) Towards a decentralized digital engineering assets marketplace: empowered by model-based systems engineering and distributed ledger technology. Preprint at https://arxiv.org/abs/2005.05415.

Maull R, Godsiff P, Mulligan C, Brown A, Kewell B (2017) Distributed ledger technology: applications and implications. Strateg Chang 26(5):481–489

Nagel E, Kranz J (2020) Smart city applications on the blockchain: development of a multi-layer taxonomy. Blockchain and distributed ledger technology use cases. Springer, Cham, pp 201–226

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Decent Bus Rev 2008:21260

Ølnes S, Ubacht J, Janssen M (2017) Blockchain in government: benefits and implications of distributed ledger technology for information sharing. Gov Inf Q 34(1):355–364

Panda SS, Mohanta BK, Dey MR, Satapathy U, Jena D (2020) Distributed ledger technology for securing IoT. 2020 11th international conference on computing, communication and networking technologies (ICCCNT). IEEE, pp 1–6
Perera S, Nanayakkara S, Rodrigo MNN, Senaratne S, Weinand R (2020) Blockchain technology: is it hype or real in the construction industry? J Ind Inf Integr 17:100125
Priem R (2020) Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. Financ Innov 6(1):1–25
Rahmadika S, Rhee KH (2018) Blockchain technology for providing an architecture model of decentralized personal health information. Int J Eng Bus Manag 10:1847979018790589
Rahman MS, Khalil I, Mahawaga Arachchige PC, Bouras A, Yi X (2019) A novel architecture for tamper proof electronic health record management system using blockchain wrapper. Proceeding of the ACM international symposium on blockchain and secure critical infrastructure. ACM, pp 97–105
Ribitzky R, Clair JS, Houlding DI, McFarlane CT, Ahier B, Gould M, Clauson KA (2018) Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. Blockchain Healthc Today 1:24
Roeck D, Schöneseiffen F, Greger M, Hofmann E (2020) Analyzing the potential of DLT-based applications in smart factories. Blockchain and distributed ledger technology use cases. Springer, pp 245–266
Rückeshäuser N (2017) Typology of distributed ledger based business models. Proceeding of the 25th European conference on information systems (ECIS). AIS, Portugal, pp 2202–2217
Shahid F, Khan A, Jeon G (2020) Post-quantum distributed ledger for internet of things. Comput Electr Eng 83:106581
Strugar D, Hussain R, Mazzara M, Rivera V, Afanasyev I, Lee J (2019) An architecture for distributed ledger-based M2M auditing for electric autonomous vehicles. Workshops of the international conference on advanced information networking and applications. Springer, Cham, pp 116–128
Sunyaev A (2020) Distributed ledger technology. Internet computing. Springer, Cham, pp 265–299
Teh D, Khan T, Corbitt B, Ong CE (2020) Sustainability strategy and blockchain-enabled life cycle assessment: a focus on materials industry. Environ Syst Decis 40(4):605–622
Tekeoglu A, Ahmed N (2019) TangoChain: a lightweight distributed ledger for internet of things devices in smart cities. IEEE international smart cities conference (ISC2). IEEE, pp 18–21
Teslya N, Ryabchikov I (2017) Blockchain-based platform architecture for industrial IoT. 2017 21st conference of open innovations association (FRUCT). IEEE, pp 321–329
Treiblmaier H, Sillaber C (2020) A case study of blockchain-induced digital transformation in the public sector. Blockchain and distributed ledger technology use cases. Springer, Cham, pp 227–244
Trump BD, Florin MV, Matthews HS, Sicker D, Linkov I (2018a) Governing the use of blockchain and distributed ledger technologies: not one-size-fits-all. IEEE Eng Manage Rev 46(3):56–62
Trump BD, Wells E, Trump J, Linkov I (2018b) Cryptocurrency: governance for what was meant to be ungovernable. Environ Syst Decis 38(3):426–430
Viriyasitavat W, Anuphaptrirong T, Hoonsopon D (2019) When blockchain meets internet of things: characteristics, challenges, and business opportunities. J Ind Inf Integr 15:21–28
Wu H, Li Z, King B, Ben Miled Z, Wassick J, Tazelaar J (2017) A distributed ledger for supply chain physical distribution visibility. Information 8(4):137
Xu Y, Ahokangas P, Yrjölä S, Koivumäki T (2019) The fifth archetype of electricity market: the blockchain marketplace. Wirel Netw 2019:1–17
Yu FR, Liu J, He Y, Si P, Zhang Y (2018) Virtualization for distributed ledger technology (vDLT). IEEE Access 6:25019–25028
Zamani ED, Giaglis GM (2018) With a little help from the miners: distributed ledger technology and market disintermediation. Ind Manag Data Syst 118(3):637–652
Zhu Q, Loke SW, Trujillo-Rasua R, Jiang F, Xiang Y (2019) Applications of distributed ledger technologies to the internet of things: a survey. ACM Comput Surv (CSUR) 52(6):1–34
Zia MF, Benbouzid M, Elbouchikhi E, Muyeen SM, Techato K, Guerrero JM (2020) Microgrid transactive energy: review, architectures, distributed ledger technologies, and market analysis. IEEE Access 8:19410–19432
Zichichi M, Ferretti S, D'Angelo G (2020) A distributed ledger based infrastructure for smart transportation system and social good. 2020 IEEE 17th annual consumer communications & networking conference (CCNC). IEEE, pp 1–6