Ph.D. COURSE IN INDUSTRIAL ENGINEERING – XXXIV CYCLE

Student: De Santis Laura

Tutor: Prof. Domenico Capriglione

Abstract of the thesis: *"Blockchain: the distributed paradigm for secure metrology digitalization"*

Digital transformation is causing products, production, and economic processes to change rapidly and dramatically. This new demand presents new challenges to the existing system of quality infrastructure.
Industry 4.0 is a concept that describes the process of providing innovative products by using smart methods and procedures. This enables seamless asset lifecycle information, from plant concept to decommissioning, and digitally integrates value chains. It introduces many ideas that are relevant to taking advantage of these opportunities. These include machine-to-machine communication (M2M), cyber-physical system (CPSs), and the Internet of Things (IoT). M2M communication is the ability of industrial components to communicate. CPSs can monitor physical processes and create virtual copies of the world. They can also make decentralized decisions. Surrogate models, metamodels, and parameterized models could create virtual documents. These models are approximations of experimental or simulation data that can answer questions when direct measurement of the outcome of interest is not possible. With the further development of telecommunication, such a system has been embedded in the IoT field, which has become a concrete reality of everyday life. IoT is a lightweight network of "objects" such as devices, sensors, and actuators that can be connected to the Internet and communicate wirelessly. This structure aggregates and manages the data produced by the sensor devices on a head node that acts as the central administrator, e.g., a server. In such a network, physical and virtual entities share attributes and communicate. Due to their versatility, IoT systems have been used in many applications such as car accident remote monitoring, control of crops for smart farms, supervision of smart cities, home automation, and optimization in the energy market through smart metering. Different trust

concerns limit the widespread adoption of the IoT systems, related both to the specific capabilities of the devices and to the high grade of connectivity supported by the system. In the case of manufacturing and Industry 4.0, under the term Distributed Sensor Services, the authors describe such systems in terms of any physical measure that digitize real-world quantities as a sensor operation, also including complex instruments that combine multiple measurements, along with the (network-) interfaces to historical and current data, and the computational resources required for data processing. The interoperability of heterogeneous distributed systems is essential for automation purposes. Functional modeling of sensors and processing modules that provide a concise added value separate from proprietary implementations is required. Moreover, to ensure the system's proper function, the devices and produced data must be considered reliable from the legislative and regulatory points of view.

The widespread adoption in a unified European Market of such technologies is sharply limited by Trust concerns for IoT devices regarding reliability, traceability, integrity, the privacy of the data, and cybersecurity of software and hardware components. In a hyperconnected society, the need for improved quality and security of interconnected devices is crucial, especially if there is a strong interdependence with human activity. Interdependence so affects the different levels of machine and system development. It is utopian to think that a final product results from a single effort in a modern market. Often, complex products result from the cooperation of different suppliers (e.g., raw materials, hardware development, software development, development, and support of the ITC infrastructure). Each development phase is subject to review by the authorities in charge of market surveillance (e.g., National Accreditation Body, National Cybersecurity Authority, etc.). Although this procedure is necessary, manufacturers often perceive it as a strong brake on the competitiveness of their products by significantly increasing the time to market. The National Institute of Standard Technologies (NIST) identifies 17 technical trust-related- concerns for IoT adoption both in people's lives and in the enterprise's environments. Trust in IoT includes four main specifications related to cybersecurity issues and data trust: Control and ownership, IoT certification criteria, Data integrity, and Security. All quality assurance processes such as certification, accreditation, and market surveillance must be digitalized to meet these challenges. All parties involved must be digitally connected and interoperable, and the network data flow needs to be traceable. One hindrance, in this case, is due to the fragmentation of legislation in the legal field. A procedure for the assessment of products and services is still being developed, the components of which are produced in different regions of the European community (e.g., a measuring device whose hardware is designed and certified in Italy, the firmware is developed and verified in Germany, the linked application is produced in Finland).

While there is a strong need for a legislative effort at the community level to standardize and standardize the legislation relating to the safety and quality certifications of the products transiting the European market, on the other hand, a key aspect to consider is the means and technological infrastructures necessary to streamline and optimize the traceability and verifiability procedures of systems and products. In such a system, it should be considered that the stakeholders involved do not necessarily trust each other. The national authorities constitute a trusted third party for the individual states, but this assumption cannot hold in a community system.

Therefore, the development of an infrastructure based on a consortium of parties is required in which each information flow is available in a decentralized manner, i.e., not under the control of a single entity but of a community of well-known and trusted parties (e.g., Authorities and Governments) and accessible to the various market stakeholders. Product information must be tracked securely. A traditional database has some limitations in this sense suffering from a single point of failure, subject to date tempering. The approach based on distributed ledger technology (aka blockchain) solves a good part of these fundamental problems while presenting other significant challenges from a technical point of view.

This thesis considers this technology's capabilities and challenges to achieve both data trust and traceability with digital certification as the point of trust.

Abstract della tesi: “Blockchain: il paradigma distribuito per la digitalizzazione metrologica sicura”

La trasformazione digitale sta modificando rapidamente e drasticamente prodotti, produzione e processi economici. Questa nuova domanda presenta nuove sfide al sistema esistente di infrastrutture di qualità.
Industry 4.0 è un concetto che descrive il processo di fornitura di prodotti innovativi utilizzando metodi e procedure intelligenti. Ciò consente informazioni sul ciclo di vita degli asset senza interruzioni, dal concetto di impianto allo smantellamento, e integra digitalmente le catene del valore. Introduce molte idee che sono rilevanti per sfruttare queste opportunità. Questi includono la comunicazione da macchina a macchina (M2M), il sistema cyber-fisico (CPS) e l'Internet delle cose (IoT). La comunicazione M2M è la capacità di comunicare dei componenti industriali. I CPS possono monitorare i processi fisici e creare copie virtuali del mondo. Possono anche prendere decisioni decentralizzate. Modelli surrogati, meta modelli e modelli parametrizzati potrebbero creare documenti virtuali. Questi modelli sono approssimazioni di dati sperimentali o di simulazione che possono rispondere a domande quando non è possibile misurare direttamente il risultato di interesse. Con l'ulteriore sviluppo delle telecomunicazioni, un tale sistema è stato integrato nel campo dell'IoT, che è diventato una realtà concreta della vita quotidiana. L'IoT è una rete leggera di "oggetti" come dispositivi, sensori e attuatori che possono essere collegati a Internet e comunicare in modalità wireless. Questa struttura aggrega e gestisce i dati prodotti dai dispositivi sensori su un nodo principale che funge da amministratore centrale, ad esempio un server. In tale rete, entità fisiche e virtuali condividono attributi e comunicano. Grazie alla loro versatilità, i sistemi IoT sono stati utilizzati in molte applicazioni come il monitoraggio remoto degli incidenti stradali, il controllo delle colture per le smart farm, la supervisione di città intelligenti, la domotica e l'ottimizzazione del mercato energetico attraverso la misurazione intelligente. Diversi problemi di fiducia limitano l'adozione diffusa dei sistemi IoT, legati sia alle capacità specifiche dei dispositivi sia all'elevato grado di connettività supportato dal sistema. Nel caso della produzione e dell'Industria 4.0, con il termine Servizi di sensori distribuiti, gli autori descrivono tali sistemi in termini di qualsiasi misura fisica che digitalizza quantità del mondo reale come un'operazione di sensore, includendo anche strumenti complessi che combinano misurazioni multiple, insieme al (rete-) interfacce ai dati storici e attuali e le risorse di calcolo necessarie per l'elaborazione dei dati. L'interoperabilità di sistemi distribuiti eterogenei è essenziale ai fini dell'automazione. È richiesta la modellazione funzionale di sensori e moduli di elaborazione che forniscano un valore aggiunto conciso separato dalle implementazioni proprietarie. Inoltre, per garantire il corretto funzionamento del sistema, i dispositivi e i dati prodotti devono essere considerati affidabili dal punto di vista legislativo e regolamentare. L'adozione diffusa in un mercato europeo unificato di tali tecnologie è fortemente limitata dalle preoccupazioni di Trust per i dispositivi IoT per quanto riguarda l'affidabilità, la tracciabilità, l'integrità, la privacy dei dati e la sicurezza informatica dei componenti software e hardware. In una società iperconnessa, la necessità di migliorare la qualità e la sicurezza dei dispositivi interconnessi è cruciale, soprattutto se esiste una forte interdipendenza con l'attività umana. L'interdipendenza influisce quindi sui diversi livelli di sviluppo della macchina e del sistema. È utopico pensare che un prodotto finale derivi da un unico sforzo in un mercato moderno. Spesso i prodotti complessi derivano dalla cooperazione di diversi fornitori (ad esempio, materie

prime, sviluppo hardware, sviluppo software, sviluppo e supporto dell'infrastruttura ITC). Ogni fase di sviluppo è soggetta a revisione da parte delle autorità preposte alla vigilanza del mercato (es. Organismo nazionale di accreditamento, Autorità nazionale per la sicurezza informatica, ecc.). Sebbene questa procedura sia necessaria, i produttori spesso la percepiscono come un forte freno alla competitività dei loro prodotti aumentando notevolmente il time to market. Il National Institute of Standard Technologies (NIST) identifica 17 problemi tecnici legati alla fiducia per l'adozione dell'IoT sia nella vita delle persone che negli ambienti aziendali. Trust in IoT include quattro specifiche principali relative ai problemi di sicurezza informatica e all'affidabilità dei dati: controllo e proprietà, criteri di certificazione IoT, integrità dei dati e sicurezza. Tutti i processi di garanzia della qualità come la certificazione, l'accreditamento e la sorveglianza del mercato devono essere digitalizzati per affrontare queste sfide. Tutte le parti coinvolte devono essere connesse e interoperabili digitalmente e il flusso di dati di rete deve essere tracciabile. Un ostacolo, in questo caso, è dovuto alla frammentazione della legislazione in campo giuridico. È ancora in fase di sviluppo una procedura per la valutazione di prodotti e servizi i cui componenti sono prodotti in diverse regioni della comunità europea (es. un misuratore il cui hardware è progettato e certificato in Italia, il firmware è sviluppato e verificato in Germania, la domanda collegata è prodotta in Finlandia).

Se da un lato vi è una forte necessità di uno sforzo legislativo a livello comunitario per standardizzare e standardizzare la normativa relativa alle certificazioni di sicurezza e qualità dei prodotti transitanti nel mercato europeo, dall'altro un aspetto fondamentale da considerare sono i mezzi e le tecnologie infrastrutture necessarie per snellire e ottimizzare le procedure di tracciabilità e verificabilità di sistemi e prodotti. In un tale sistema, va considerato che le parti interessate coinvolte non si fidano necessariamente l'una dell'altra. Le autorità nazionali costituiscono un terzo fidato per i singoli Stati, ma questa ipotesi non può reggere in un sistema comunitario. Si rende quindi necessario lo sviluppo di un'infrastruttura basata su un consorzio di soggetti in cui ogni flusso informativo sia disponibile in maniera decentralizzata, cioè non sotto il controllo di un unico soggetto ma di una comunità di soggetti noti e di fiducia (es. , Autorità e Governi) e accessibile ai diversi attori del mercato. Le informazioni sul prodotto devono essere tracciate in modo sicuro. Un database tradizionale presenta alcune limitazioni in questo senso soffrendo di un singolo punto di guasto, soggetto a tempra della data. L'approccio basato sulla tecnologia del registro distribuito (aka blockchain) risolve buona parte di questi problemi fondamentali presentando altre sfide significative dal punto di vista tecnico.

Questa tesi considera le capacità e le sfide di questa tecnologia per ottenere sia l'affidabilità dei dati che la tracciabilità con la certificazione digitale come punto di fiducia.