Cogent Engineering

ISSN: 2331-1916 (Online) Journal homepage: www.tandfonline.com/journals/oaen20

Blockchain-based secure and transparent data storage on process level for traceability and data integrity in the continuous mixing process in battery cell manufacturing

Simon Otte, Lennard Reuscher , Sebastian Schabel & Jürgen Fleischer

To cite this article: Simon Otte, Lennard Reuscher , Sebastian Schabel & Jürgen Fleischer (2026) Blockchain-based secure and transparent data storage on process level for traceability and data integrity in the continuous mixing process in battery cell manufacturing, Cogent Engineering, 13:1, 2712034, DOI: 10.1080/23311916.2026.2712034

To link to this article: https://doi.org/10.1080/23311916.2026.2712034

Published online: 07 Aug 2026.

COGENT ENGINEERING
2026, VOL. 13, NO. 1, 2712034
https://doi.org/10.1080/23311916.2026.2712034

PRODUCTION AND MANUFACTURING | RESEARCH ARTICLE

OPEN ACCESS Check for updates

Blockchain-based secure and transparent data storage on process level for traceability and data integrity in the continuous mixing process in battery cell manufacturing

Simon Otte, Lennard Reuscher, Sebastian Schabel and Jürgen Fleischer

wbk Institute of Production Science, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany

ABSTRACT

The protection of production data and the cell-chemistry formula is very important in battery cell production. The potential of blockchain technology in this context is significant. This article focuses on the integration of blockchain technology into the continuous mixing process of battery cell production to securely and transparently store process data. A private blockchain architecture was implemented, using SHA-256 as a hash function and a Proof-of-Authority (PoA) consensus mechanism. The system supports both Linux and Windows environments and was connected directly to an extruder at the process level. Validation tests showed complete consistency between real process values and blockchain-stored records, confirming data integrity. A Failure Mode and Effects Analysis (FMEA) was conducted, and it is shown that none of the five highest-risk scenarios are related to blockchain technology. The first blockchain-specific risk (potential software failure) is ranked in seventh place. The results demonstrate that a private PoA-based blockchain is a suitable and effective solution for ensuring transparency, traceability, and security in industrial production environments. However, ensuring data authenticity prior to blockchain entry remains essential, highlighting the need for robust upstream data security.

ARTICLE HISTORY
Received 25 February 2026
Revised 21 July 2026
Accepted 27 July 2026

KEYWORDS
Blockchain; battery cell production; FMEA; continuous process; production

SUBJECTS
Chemical engineering; process control; manufacturing engineering; manufacturing technology; production systems and automation; production engineering; distributed network systems; technology

1. Introduction

Batteries are an integral part of modern life. They are widely used in everyday consumer electronics, as well as in numerous safety-critical areas, such as medical technology, defense technology, aerospace, and e-mobility (Colombo et al., 2024). A battery failure can result in high economic damage and loss of reputation for the manufacturer, as well as being a significant risk to life, especially in safety-critical applications. For instance, a defect in an implantable medical device, such as a pacemaker, or in an aircraft, can be an immediate threat to life and could have serious legal consequences (Hayashi et al., 2017; Pokorney et al., 2014).

Therefore, these industries have correspondingly high requirements for traceability and documentation. In the context of the production of medical and safety-critical products, complete and tamper-proof documentation of production process data is often required (DIN Deutsches Institut für Normung e. V., 2021; International Electrotechnical Commission [IEC], 2020; U.S. Food and Drug Administration (FDA) and Department of Health and Human Services, 1996). Hereby, a key challenge is the balance of the three competing goals: transparency, data integrity and protection of sensitive information. Manufacturers must demonstrate to customers and regulatory authorities that they comply with tolerance limits and process specifications while ensuring that recorded production data has not been manipulated (European Parliament and the Council, 2017; Gokulakrishnan & Venkataraman, 2025).

CONTACT Simon Otte simon.otte@kit.edu wbk Institute of Production Science, Karlsruhe Institute of Technology (KIT), Kaiserstrasse 12, 76131 Karlsruhe, Germany

On the other hand, the protection of their know-how (like production data and the cell chemistry formula) and intellectual property from unauthorized access and industrial espionage is of major importance to manufacturers in battery cell production, as it protects their innovative lead and know-how.

This 'trilemma' poses a significant challenge for data-based quality assurance in the production of battery cells. In battery cell production, the mixing process is important, as it significantly affects the subsequent process steps and defines the principal electrochemical properties of the battery cells (VDMA Batterieproduktion, 2023). In this process step, active materials, additives, and solvents are mixed to form an electrode paste. This paste is coated on a thin metal foil, dried, and calendered afterward. For pouch cells, sheets are made from this electrode coil and stacked. This electrode stack is housed and builds up the final battery cell. Because this process step affects the following process steps and the battery cell performance, it is important to protect the recipe and process parameters used (Keppeler et al., 2021; Li et al., 2022).

Blockchain technology is an excellent approach to solving this trilemma, especially when combined with zero-knowledge proof. This is an ideal solution for applications requiring high security and confidentiality (Morais et al., 2019; Prasad et al., 2024). When used with a privately operated blockchain, production data can be stored in a tamper-proof manner without complete disclosure. Previous research shows that using a private blockchain with a Proof-of-Authority (PoA) consensus mechanism in battery cell production is a suitable, energy-efficient approach. Production data is encrypted using cryptographic methods like SHA-256 and stored with metadata, such as timestamps, nonces, and product IDs, in a hash value (Otte et al., 2024). The generated hash value can be attached to the final product or stored with an independent authority. In the event of a recall or regulatory review, the manufacturer can provide the original data in response to a justified request. The integrity of the data can be verified by comparing it with the originally stored hash value. This prevents subsequent manipulation and provides traceable proof of compliance with production specifications without disclosing sensitive process details.

There are no studies in which blockchain technologies have been implemented directly at the process level of battery cell production or in continuous mixing processes. Furthermore, there is a lack of in-depth analyses of industrial integration risks and a systematic assessment of remaining risk potential after implementation. Therefore, this article investigates the integration of blockchain technology into the continuous mixing process in battery cell production to close that research gap.

2. State of the art of blockchain technology in production

Blockchain technology is already part of industrial applications, particularly in the context of global supply chains. Most times, it is used to increase transparency, data integrity and security, as well as blockchain-based product passports to meet regulatory requirements while ensuring tamper-proof traceability along the value chain. For example, Minespider offers the 'Open Battery Passport', a solution based on a PoA consensus mechanism for securely documenting material origin and carbon footprint in the battery supply chain (Minespider GmbH (Ed.), 2025). Circulor, in collaboration with Volvo Cars, provides a permissioned blockchain that ensures compliance with ESG criteria, and it is used in the Volvo XC40 model (Circulor Ltd (Ed.), 2025). Rufino Júnior et al. demonstrate the use of blockchain to trace the life cycle of battery cells, from raw material extraction to end use. The blockchain serves as the basis for a digital battery passport that stores safety and quality-related information (Rufino Júnior et al., 2022). These use cases illustrate that the current industrial application of blockchain technologies is predominantly focused on optimizing the supply chain. Direct integration at the level of production processes remains largely unexploited.

However, some scientific papers address approaches with process-oriented use. Kohl et al. (2022) developed a blockchain architecture based on Hyperledger Fabric for the traceability of rolled materials along the cold-forming process chain. The system uses a raft-based ordering service and the SHA-256 algorithm. Sensor data can be integrated via an OPC UA interface. The evaluation proved the functionality and shows high data integrity and low hardware requirements, but also performance limitations. Angrish et al. (2018) demonstrate a decentralized production network based on a private Ethereum blockchain with a PoA consensus mechanism in regulated industries such as medical technology and aerospace. In particular, the aspect of transparency in networked production systems was addressed.

Wong et al. (2021) are developing a blockchain-based framework for decentralized quality assurance in cyber-physical production systems (CPPS), in which each production step is documented and quality-related data is written to the blockchain. The solution is based on a proof-of-work (PoW) mechanism and aims to increase data security and transparency in accordance with Industry 4.0 principles. Lechner et al. (2020) are implementing a permissioned blockchain for the secure transmission of production data in sheet metal processing. The architecture uses SHA-256 and channel-based data transmission between authorized participants. Successful integration into series production demonstrated advantages in terms of material usage, scrap reduction, and seamless traceability.

The mentioned work above demonstrates the potential of blockchain technologies in industrial data processing and security. However, to date, implementation has primarily focused on discrete manufacturing processes and the supply chain. A connection of a blockchain at the process level has not yet been researched. Especially in the context of continuous production with liquid-paste media, as occurs in battery cell production when mixing electrode pastes, has not been documented.

3. Blockchain setup

Blockchains exist in a variety of different forms, which can be specifically adapted to the respective application. A morphological box for the uniform, standardized description of all relevant characteristics of a blockchain has been developed previously. This enables a systematic and transparent representation of the characteristics of any blockchain system. Regarding the specific use case of the continuous mixing process in battery cell production, a private blockchain was chosen to securely and traceably store sensitive production data (Figure 1). This design ensures the company has complete data sovereignty and prevents unauthorized external access. Access control is node-specific and uses asymmetric encryption, whereby write, read, or authorization rights can be assigned individually (Otte et al., 2024).

The SHA-256 hash function is used to ensure data integrity. It is characterized by high efficiency, broad acceptance, and cryptographic security. PoA is chosen as a consensus mechanism because it is energy-efficient, offers low latency, and is robust against denial-of-service and 51% attacks. To ensure maximum transparency and data integrity, all relevant production data is stored on the blockchain. At the same time, a limited block size is defined to ensure system efficiency despite varying data volumes.

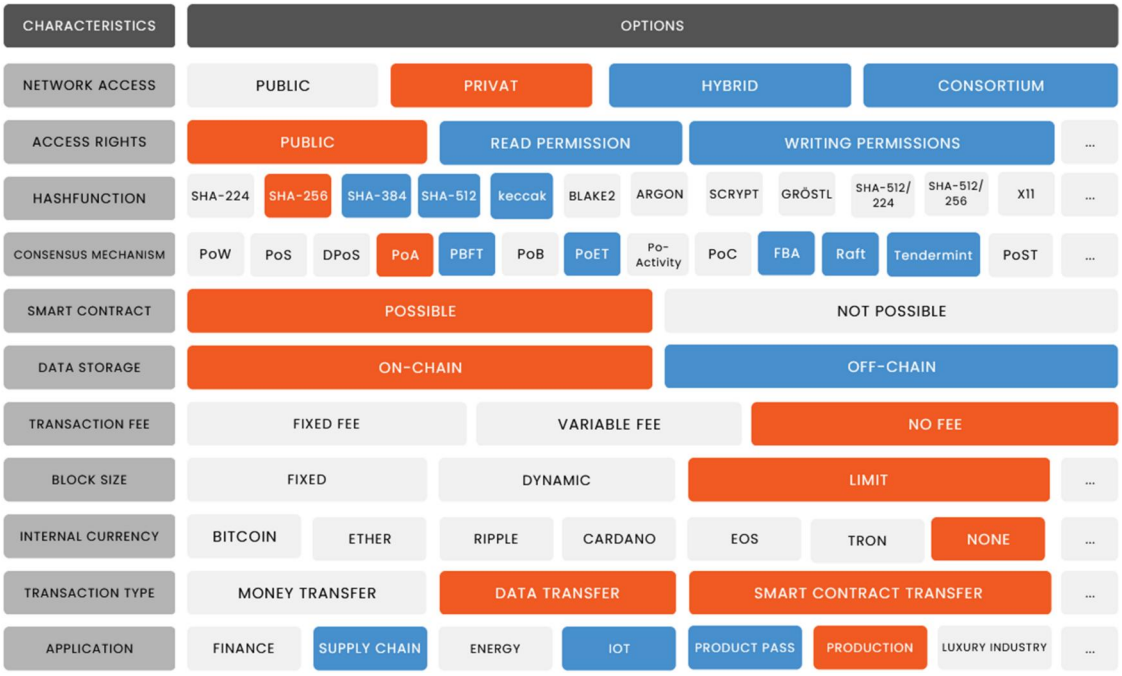

Figure 1. Morphological box of possible industry-suitable attributes (blue and orange) and the attributes selected for the present use case (orange) (Otte et al., 2024).

To maintain economic efficiency in the production environment, transaction fees and internal tokens are eliminated (Otte et al., 2024).

The Ethereum platform seemed unsuitable for this use case due to requirements for data protection, transaction costs, and transparency, which are more consistently addressed by permissioned architectures (Otte et al., 2024; Polge et al., 2021). Hyperledger Sawtooth was not considered because of its hardware-bound consensus mechanisms, limited industrial applications, and comparatively low reliability. Hyperledger Fabric was chosen as the base platform because of its widespread industrial acceptance and modular architecture. The blockchain architecture uses five nodes so that consensus can still be achieved even if up to two nodes fail. Each node acts as an authority instance. The selected five-node topology provides fault tolerance against the loss of up to two validator nodes while maintaining consensus availability. In the event of validator failure, the remaining authorized nodes continue operation and preserve blockchain integrity. Consequently, individual node failures primarily affect redundancy rather than data integrity itself. A heterogeneous hardware configuration was chosen to ensure system availability and robustness against partial failures. Therefore, four of five nodes run Linux, and one runs Windows 11. Visual Studio Code is used for cross-platform development, providing a consistent development environment across Linux, Windows, and macOS. The implementation is in JavaScript, which offers high compatibility and flexibility when integrating different system components.

3.1. Integration of a private blockchain architecture into the continuous mixing process

Depending on where the data is generated, it enters the blockchain in two ways. The control variables of the extruder system and the actual process variables are collected in a plant-side control system. Measurements from sensors, which are permanently installed in the twin screw extruder, are also transmitted to this control system. From there, the data is sent to a central control system (CCS-PLC) for the entire process via a put-get protocol. Data from external sensors integrated outside the process or system, such as sensors that record measurements after the mixing process, is transmitted directly to the CCS-PLC (see Figure 2).

The CCS-PLC collects and time-stamps all data. Then, the data is transferred to one of the blockchain nodes using the MQTT protocol (TLS 1.3) without being routed through a manufacturing execution system (MES) or any other central system (OASIS Open, 2022; Rescorla, 2018). The CCS-PLC acts as the publisher, which can only publish the data in a topic channel called SENSOR_TOPIC. The blockchain node acts as the subscriber that reads the encrypted channel. Unauthorized clients on the network do not

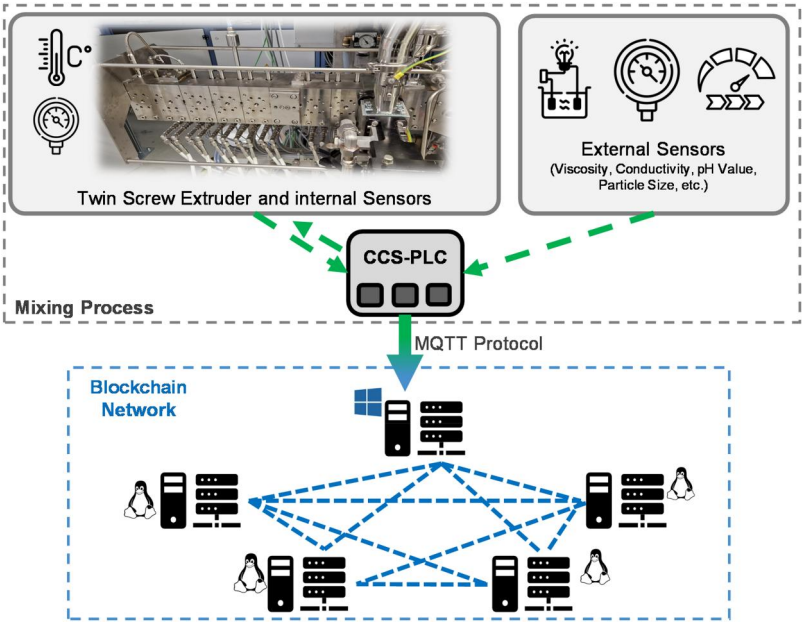

Figure 2. Illustration of the connection between the blockchain and the process, as well as the data streams.

have read or write permissions. Authentication is performed via mutual TLS (mTLS), also known as client certificate authentication. Both the CCS PLC (client) and the MQTT broker (server) must identify themselves to each other with valid X.509 certificates. Each of the five authority nodes (blockchain nodes) authenticates itself to the broker using its own mTLS certificate. The X.509 certificates have a maximum validity period of 90 days. Certificate issuance and rotation are managed centrally by an internal Certificate Authority (CA) and performed automatically to ensure consistent and secure operation.

The distribution within the blockchain network takes place from the blockchain node, which is the subscriber of the encrypted channel SENSOR_TOPIC. Final storage takes place via the blockchain module, which securely stores all processed information on the blockchain. Due to the limited data volume, complete on-chain storage is technically and economically feasible. As the system is optimized for storing process data with low latency, the architecture is not limited to a fixed block size (e.g. in MB), but rather to a transaction-per-block granularity. This means that a message with process data from the CCS PLC is transferred in a transaction or block. This ensures a high transaction rate.

The relevant data from the mixing process is heterogeneous and comes from various sources. This includes data on fill levels, dosing rates, rotational speed of the side feeder, twin-screw speed in the process section, target and actual temperatures in each process section, and motor currents. Additionally, external sensors measure the conductivity, particle-size distribution, and density of the electrode paste. However, a study has shown that not all parameters are equally relevant in the context of traceability. For the continuous mixing process in particular, 28 parameters are relevant, including solids content, recipe, dynamic viscosity, homogeneity, particle size distribution, screw configuration, and screw speed (Otte et al., 2024). This data is collected and summarized in a time-stamped data block.

4. Validation of performance, data integrity and remaining risks

4.1. Experimental determination of performance and data integrity

Achieving digital traceability in industrial production processes requires the reliable acquisition, processing, and storage of process data. To validate the functionality and robustness of the implemented blockchain-based data acquisition and storage system, extensive experimental investigations were conducted under realistic industrial operating conditions.

The experiments were conducted using a ZSK18 twin-screw extruder provided by Coperion GmbH (Germany). The experiments were conducted using an anode recipe (see Otte et al., 2025), that is, representative of the industrial battery cell manufacturing recipe. The selected formulation reflects typical industrial slurry compositions used in lithium-ion battery production and, as such, provides a realistic validation. The performance of the system was evaluated through a comparative analysis of various scenarios (i.e. different throughputs, solids contents, and screw speeds) that are analogous to industrial applications (see Table 1). The selection of these parameter variations was made to reflect the realistic production ranges observed in industrial continuous mixing processes.

The experimental results of point P9 are used to illustrate the analysis, with the following parameters: a throughput of 11 kg/h, a screw speed of 750 rpm, and a solid content of 35 wt%. The process data from both internal and external sensors were continuously recorded and stored using three independent

Table 1. Overview of the experimental points tested for performance determination and data integrity.

Experimental point	Screw speed [rpm]	Mass flow [kg h^{-1}]	Solid content [%]
P1	482.43	11.00	20
P2	482.43	11.00	50
P3	482.43	5.65	35
P4	482.43	16.35	35
P5	750.00	5.65	20
P6	750.00	5.65	50
P7	750.00	16.35	20
P8	750.00	16.35	50
P9	750.00	11.00	35
P10	1017.57	11.00	20
P11	1017.57	11.00	50
P12	1017.57	5.65	35
P13	1017.57	16.35	35

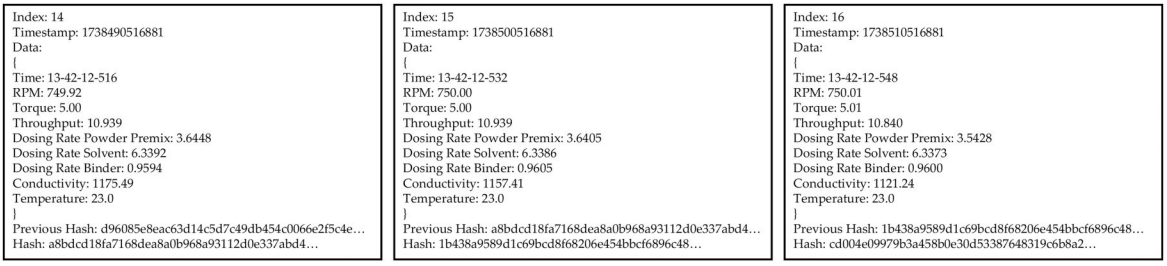

Figure 3. Illustration of three blocks of the blockchain with real process and plant data recorded during experiments.

Table 2. Exemplary excerpt from the data from experimental point P9 for validating data integrity using data sequence and data values.

	Data stored by the PLC data logger			Data stored in blockchain		
Timestamp (ms)	Screw speed [rpm]	Throughput [kg h^{-1}]	Conductivity [µS cm^{-1}]	Screw speed [rpm]	Throughput [kg h^{-1}]	Conductivity [µS cm^{-1}]
1769704463197	750.00	11.00	1364.29	750.00	11.00	1364.29
1769704501189	749.93	11.00	1372.63	749.93	11.00	1372.63
1769704540087	750.00	11.00	1383.05	750.00	11.00	1383.05
1769704578537	749.93	11.00	1395.42	749.93	11.00	1395.42
1769704617637	749.93	11.01	1410.22	749.93	11.01	1410.22
1769704656461	749.93	10.99	1425.81	749.93	10.99	1425.81
1769704696081	750.00	11.00	1442.15	750.00	11.00	1442.15
1769704735398	750.15	11.00	1464.30	750.15	11.00	1464.30
1769704775615	749.93	11.00	1489.80	749.93	11.00	1489.80

approaches: First, using the data storage tool integrated in the Siemens TIA Portal as an industrially proven solution. Second, the data was read from the CCS-PLC using a MATLAB script and stored in an Excel file. The third option was to store the data directly in the blockchain using the method described in the previous section (see Figure 2). There, the data was processed, a consensus was reached, and the data was stored in individual blocks. Figure 3 shows an excerpt from the resulting blockchain for experiment point P9. For the selected exemplary point, a total of over 90,000 measurement points were recorded under constant process conditions, corresponding to an experimental runtime of 2.5 h. The sensor data that was acquired included relevant process variables, such as screw speed, dosing rates, temperature profiles in the process section, and material properties.

An important aspect of evaluating the system is ensuring the accuracy and completeness of the data stored in the blockchain. The integrity of the system was evaluated by comparing time-synchronized datasets obtained from the two independent storage solutions. Two criteria were used to verify data integrity: first, whether the data sequence was chronologically consistent over time, and second, whether the data was identical at the same timestamps. Analyses of a randomly selected timestamp series and three parameters (screw speed, throughput and conductivity) show no differences or deviations (see Table 2). No deviations were identified for other randomly chosen data points in time and time series from the test data set, nor for other parameters (dosing rates, temperatures, etc.). Consequently, it can be stated that data integrity is assured.

The latency was determined by calculating the difference between the timestamps. Therefore, identical pairs were defined for all stored data points, and the corresponding timestamps were compared. In summary, the minimum latency was 9.5 ms, and the maximum latency was 126.3 ms. The mean value is 18.0 ms, and the median is 13.4 ms (Figure 4). The statistical evaluation of the latency times results in a minimum variance with a standard deviation of 20.3 ms. No significant delays or performance losses were detected. Therefore, these latency times are considered sufficient compared to typical processing behavior, which is typically in the range of minutes.

To ensure performance appropriate for the process of continuous mixing, a minimum transaction rate of 35 transactions per second is required (see Otte et al., 2024). The results show that this can be achieved for all points in Table 1. With serial batch processing and an average commit latency of 18.0 ms, the theoretical transaction rate is 55.6 transactions per second (TPS). In conclusion, the current system performs very well and exceeds expectations.

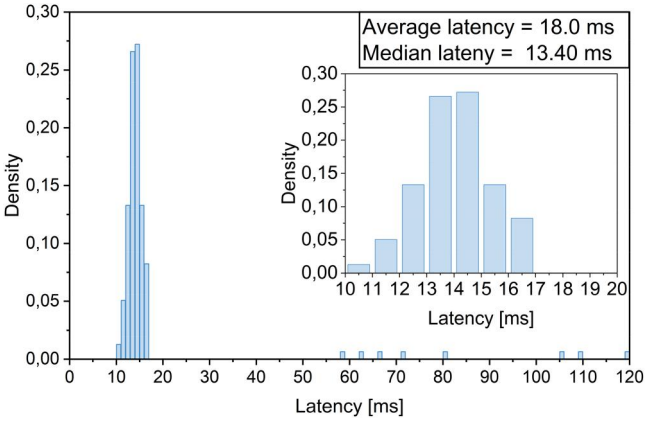

Figure 4. The latency distribution shows a strong concentration in the range of 10 ms to 18 ms, with isolated outliers in the range of 60 ms to 120 ms.

4.2. Failure mode and effects analysis (FMEA) of the remaining points of possible data manipulation

Despite the implementation of a blockchain-based solution, potential vulnerabilities may remain that compromise the security of data transmission from the process to the data storage and thus pose a threat to data integrity. These threats must be systematically identified and evaluated in terms of their risk potential. Therefore, a structured FMEA was carried out in accordance with the DIN EN 60812 standard, as it is a proven method for the preventive identification, evaluation, and prioritization of technical risks in complex system architectures (DIN Deutsches Institut für Normung e. V, 2006). A five-person team was formed to conduct the FMEA, consisting of a moderator, a process and data analyst, an IT network specialist, an IT technician, and a process engineer. The FMEA focused on the structured analysis of potential failure modes, their underlying causes, and their effects on the functionality and reliability of the system. Three key evaluation parameters are used for each identified failure mode (Tietjen & Decker, 2020):

- Occurrence (O): The probability of the failure occurring under the given conditions.
- Severity (S): The potential impact of the failure on safety, function, or quality.
- Detection (D): The probability that the failure will be detected before it has an impact.

These three parameters define the Risk Priority Number (RPN), calculated as $RPN = O * S * D$. It is used to prioritize the relevance of identified failure modes and to define appropriate risk mitigation measures. The methodological approach is based on the FMEA steps outlined in the DIN EN 60812 standard. In the following, the structural analysis is focused. First, the objectives, scope of analysis, and level of consideration were defined. The analysis focused on the data flow from the sensor to storage in the blockchain during the continuous mixing process (see Figure 2). As part of the structural analysis, a comprehensive understanding of the system was established by identifying all functional and physical interfaces. A functional analysis of the system's elements provided a basis for identifying potential failure modes during error analysis. Both human and technical causes of errors were considered. To further systematize the identified error modes, a classification was carried out. To achieve this, the errors were subdivided according to their cause. Specifically, they were classified as either human-induced (e.g. incorrect maintenance or configuration, deliberate manipulation) or technically determined (e.g. software and hardware defects, communication problems). A technology-related differentiation was also made, divided into blockchain-specific error modes and cross-technology error modes (general network failures, latency, hardware failures, etc.).

A cause-and-effect analysis was conducted, in which the 25 identified error modes were examined systematically with regard to their underlying causes and potential effects on the overall process (see Table 3). When it was not possible to clearly assign an error mode to a category, a pragmatic assessment was made based on the highest probability, even if a different approach was required in exceptional

Table 3. Overview of the assessments of the identified failure types as well as classification.

Failure type	S	O	D	RPN	Classification	
Man-in-the-middle (MitM) attack	9	7	6	378	human-induced	cross-technology
Inadequate encryption	8	6	6	288	human-induced	cross-technology
Unauthorized external access	9	3	7	189	human-induced	cross-technology
Communication failures	6	5	6	180	technically determined	cross-technology
Manipulation of sensor data	7	4	6	168	human-induced	cross-technology
Firewall misconfiguration	7	4	6	168	human-induced	cross-technology
Software failure in PoA	9	3	6	162	technically determined	blockchain-specific
Network overcrowding	6	5	5	150	technically determined	cross-technology
Misconfiguration of user rights	6	4	6	144	human-induced	cross-technology
Lack of virus protection	7	5	4	140	human-induced	cross-technology
DDoS attack on the MQTT server	9	3	5	135	human-induced	cross-technology
MQTT vulnerabilities	7	3	6	126	technically determined	cross-technology
Sensor malfunction (defect, calibration)	5	5	5	125	technically determined	cross-technology
Voltage or current fluctuations	5	5	5	125	technically determined	cross-technology
Environmental influences (dust, moisture)	5	5	5	125	technically determined	cross-technology
Incorrect or missing software updates	6	4	5	120	technically determined	cross-technology
Phishing attacks on users	7	3	5	105	human-induced	cross-technology
Internal unauthorized access	7	2	7	98	human-induced	cross-technology
Abrasion caused by continuous operation	5	3	6	90	technically determined	cross-technology
Delayed provision of data	4	4	5	80	technically determined	cross-technology
Data inconsistency between devices	5	3	5	75	technically determined	cross-technology
Hardware failure due to a hard drive defect	8	2	4	64	technically determined	cross-technology
Hardware failure due to a power outage	9	2	3	54	technically determined	cross-technology
Malicious manipulation of the blockchain code	8	1	5	40	human-induced	blockchain-specific
Misconfiguration of the MQTT broker	6	1	3	18	human-induced	cross-technology

cases. The results show that the majority of error modes are cross-technology and independent of blockchain; they are mostly human in nature.

The top seven error modes are described below. The man-in-the-middle (MitM) attack offers the highest risk potential (RPN = 378). This type of attack poses a particularly serious threat to Industry 4.0 networked environments. The threat arises from unencrypted protocols, inadequate authentication, and poor certificate management. These vulnerabilities make it possible to listen and manipulate sensitive process data, as well as falsify status values in the blockchain, which are recorded in a non-reversible manner.

Inadequate encryption (RPN = 288) is another relevant failure mode. Using outdated or weak cryptographic methods due to performance requirements or a lack of guidelines puts the confidentiality and integrity of data at risk. Attacks on encryption can lead to undetected data corruption. This would enable attackers to access process data and confidential information. In the worst case, this could result in reputational damage and economic losses due to data leaks or control errors.

Vulnerabilities, such as unprotected interfaces or default passwords, enable digital and physical attacks. These vulnerabilities allow for unauthorized external access (RPN = 189) and can lead to transaction manipulation or data leaks. The high probability of detection underscores the need for robust technical safeguards and clearly defined responsibilities.

The technical complexity of industrial communication architectures can lead to communication failures (RPN = 180). Although network failures or signal interference rarely cause permanent damage, they disrupt processes. Targeted network monitoring and redundancy concepts are suitable approaches to avoid these issues and minimize the risk. Another failure mode is the manipulation of sensor data (RPN = 168), which can compromise automated decision-making processes. Without plausibility checks, detection is difficult, so robust validation mechanisms and operator training are essential. A firewall misconfiguration (RPN = 168) can reduce network segmentation, allowing unauthorized access and disrupting legitimate communication. This is especially important for blockchain nodes. A software failure in the PoA system (RPN = 162) is the most critical blockchain-specific failure mode because the loss of validation nodes can disrupt consensus, cause downtime, and interrupt data storage, thereby impairing transparency.

The analysis shows that many security-related weaknesses arise in the early stages of the process, such as data collection and transmission. The vulnerabilities remain in the preceding stages of the process, particularly during data collection, processing, and transmission. Blockchain technology only takes effect once data has been added to the database. Subsequent manipulation of stored data is impossible

due to their cryptographic chaining. This ensures a high level of data integrity in the long term. Nevertheless, securing the upstream process chain remains a central component of a comprehensive security strategy. The FMEA shows this clearly. To address these risks, some actions have been formulated. These measures are intended as initial design proposals for the structured development of a holistic security concept.

From a technical perspective, automated configuration auditing using Center for Internet Security (CIS) benchmark-compliant tools enables the early detection and remediation of critical security misconfigurations, such as incorrect firewall rules or improper permission settings. This reduces exposure to human or systemic errors. Redundant system architectures, including parallel server infrastructures and alternative network paths, enhance system availability and fault tolerance, particularly for distributed blockchain node environments. Additionally, system hardening and malware protection through trusted antivirus solutions and continuous security reinforcement aligned offer essential protection against malicious intrusions and unauthorized access.

From an organizational point, IT security training for staff, including practical formats such as online courses, increases security awareness and reduces the likelihood of configuration errors. Role-based access control, based on the principle of least privilege, minimizes unnecessary permission allocations and constrains potential attack vectors. Furthermore, mandatory two-factor authentication (2FA) strengthens access control by maintaining security in the event of compromised credentials.

Together, these technical and organizational measures form a robust security baseline for distributed, blockchain-based production systems. Further prioritization and evaluation are required to balance security impact, implementation effort, and system compatibility.

5. Discussion

The experimental results demonstrate the efficiency of the integrated blockchain within the continuous mixing process. An analysis of the process characteristics indicates that process times tend to have a typical range of 1–15 min. A typical product batch requires 0.5–5 min to manufacture. Consequently, blockchain performance is not the limiting factor. The theoretical throughput of ∼56 TPS offers an enormous safety reserve by a factor of ∼3600 compared to the actual requirement (∼0.015 TPS). Instead, the efficiency of the complete data transmission and block-building process is more important. However, the current latency is not a problem, as it is below 20 ms on average. Consequently, the current system performance of the blockchain is more than adequate, and there is no necessity for performance optimization in terms of speed. From an operational perspective, the investigated process generates data at a comparatively low rate relative to the storage and computing capacities of contemporary industrial server infrastructures. Furthermore, the selected PoA consensus mechanism avoids energy-intensive mining processes and is therefore considered substantially more resource-efficient than proof-of-work-based blockchain architectures. Nevertheless, the cumulative effects of long-term operation, including storage growth, computational overhead, and energy consumption over extended deployment periods, should be evaluated in future industrial implementations to support lifecycle-oriented system design. The FMEA shows that blockchain technology improves system reliability by preventing data manipulation after data storage. Once data is stored, it cannot be changed anymore. A manipulation is only possible before adding data to the blockchain. For instance, in a MitM attack, conventional systems can be compromised at multiple points, whereas blockchain technology restricts the potential attack window to the moment before data is stored. Similarly, in cases of unauthorized external access (failure type 3), attackers can view stored data but cannot modify it without being detected because any change would be immediately traceable.

However, blockchain's security benefits only take effect after data entry. Upstream processes, such as data collection, transmission, and processing, remain vulnerable. To ensure the authenticity of data before it is stored, it is essential to implement additional cryptographic safeguards, including digital signatures, hashing, and end-to-end encryption. Without these measures, erroneous or manipulated data could be stored irreversibly on the blockchain.

The effectiveness of blockchain also depends on the integrity of the surrounding infrastructure and the chosen trust model. PoA's tamper resistance relies on the trustworthiness of the authorized

validators. In a single-company private network, where all nodes are operated by the manufacturer, the security model differs fundamentally from a distributed trust environment. However, it still provides protection against data tampering after block generation. One approach to solving the problem is to integrate external, certified validators into the network. These can act as certifiers for the network's trustworthiness. Another aspect is weaknesses in sensor technology, communication systems, or configuration management, which can result in incorrect data being recorded as valid. For instance, incorrect sensor assignment may produce misleading measurements. This is a problem blockchain cannot detect or correct on its own. Thus, there is a need for complementary technical and organizational quality assurance measures. AI-based anomaly detection methods applied upstream of the blockchain entry point could provide an additional layer of validation, enabling the identification of physically implausible sensor readings before they are irreversibly stored. Currently, the blockchain and mixing plant operate as an isolated solution. The machines, sensors, and blockchain nodes are physically and network-technically isolated from the outside world, which minimizes the risk of external manipulation (e.g. man-in-the-middle attacks) in this test scenario. The present validation was conducted in an isolated industrial test environment, which minimizes exposure to external attack vectors and allows the analysis to focus on process-level integration, performance, and data integrity. The investigation of cybersecurity resilience under externally connected operating conditions, including formal penetration testing and controlled attack simulations, therefore remains a relevant topic for future industrial deployment studies. Additionally, many failure types, like manual entry mistakes, sensor failures, and configuration errors, can occur independently of blockchain implementation. Blockchain technology does not prevent these errors; it merely ensures that, once recorded, the data remains unchanged. Addressing these risks requires measures beyond blockchain technology.

In summary, cryptographically secured and immutable data storage provides a high degree of transparency. It also provides traceability and integrity. However, challenges still remain. In industrial contexts, blockchain enables continuous and verifiable process documentation. This is useful in critical steps in battery cell production, such as the mixing process. It also supports regulatory compliance. Enhanced data quality and process traceability increase operational reliability and strengthen long-term competitiveness in safety-critical industries.

In the long term, the solution should be scalable to other production plants and lines, resulting in a blockchain network that supports traceability. In the context of a production line, each node represents a machine integrated into the network. For instance, expanding the battery cell production line by adding new machines would mean integrating additional nodes into the network. Provided the expansion remains within reasonable scope (i.e. 10–15 nodes), it is considered unproblematic and should have a negligible impact on performance in the context of typical process times. However, significant performance losses are expected with a much larger expansion involving multiple production lines or a production network consisting of several sites. In the case of multiple production lines, though, each line could have its own blockchain network. This study provides the first experimental validation that blockchain integration at the process level is feasible under industrial-scale conditions at a research facility. The subsequent industrial validation phase should include a transfer to full multi-line and multi-site industrial deployment, as well as a dedicated quantitative scalability analysis that benchmarks transaction throughput and consensus latency as a function of node count and network topology.

6. Conclusion

A blockchain architecture was developed using SHA-256 encryption, PoA consensus, fee-free on-chain data storage, and MQTT as the standardized industrial interface. The system offers flexibility in operating systems, supporting both Linux and Windows environments. The developed blockchain was integrated with an extruder in a continuous mixing process for battery cell production and tested at the process level. Data integrity validation demonstrated complete alignment between real-time process values and blockchain-stored records. The FMEA-based manipulation risk assessment revealed that none of the five highest-risk scenarios were related to blockchain technology. The first blockchain-specific risk, associated with potential software failures, appeared in seventh place. Other residual blockchain-related risks

include possible PoA mechanism malfunctions, temporary inter-node data inconsistencies, and intentional source code manipulation.

The findings support the conclusion that a private, PoA-based blockchain architecture with an integrated MQTT interface is well-suited for transparent and secure data management in continuous mixing processes. The immutable recording of process information ensures high levels of transparency and traceability, thereby enhancing reliability in industrial production environments. However, further research must be conducted in the area of data generation to ensure data integrity and secure transmission to the blockchain network. Furthermore, a quantitative scalability analysis under multi-line and multi-site conditions, formal cybersecurity validation including penetration testing, and the integration of AI-based upstream anomaly detection are identified as concrete directions for future work.

Acknowledgments

This work contributes to the research performed at KIT-BATEC (KIT Battery Technology Center) and at CELEST (Center for Electrochemical Energy Storage Ulm Karlsruhe).

Author contributions

CRediT: **Simon Otte**: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Software, Validation, Visualization, Writing – original draft, Writing – review & editing; **Lennard Reuscher**: Data curation, Formal analysis, Investigation, Software, Validation, Writing – review & editing; **Sebastian Schabel**: Writing – review & editing; **Jürgen Fleischer**: Funding acquisition, Writing – review & editing.

Funding

This research was funded by German Federal Ministry of Research, Technology and Space (BMFTR) for supporting the project 'IntelliPast' (funding code: 03XP0343A).

Disclosure statement

The authors declare no conflicts of interest.

Supplementary materials

No supplementary materials are supplied.

ORCID

Simon Otte http://orcid.org/0000-0003-4938-8184
Sebastian Schabel http://orcid.org/0000-0001-7415-6655
Jürgen Fleischer http://orcid.org/0000-0003-0961-7675

Data availability statement

The data that support the findings of this study are openly available in figshare at https://figshare.com/projects/Blockchain-Based_Secure_and_Transparent_Data_Storage_on_Process_Level_for_Traceability_and_Data_Integrity_in_the_Continuous_Mixing_Process_in_Battery_Cell_Manufacturing/272055, DOI: 10.6084/m9.figshare.31407723 (Otte, 2026).

References

Angrish, A., Craver, B., Hasan, M., & Starly, B. (2018). A case study for blockchain in manufacturing: 'fabrec': a prototype for peer-to-peer network of manufacturing nodes. *Procedia Manufacturing*, *26*, 1180–1192. https://doi.org/10.1016/j.promfg.2018.07.154

Circulor Ltd (Ed.). (2025). Mandated digital battery passports. Circulor. https://circulor.com/battery-passport

Colombo, C. G., Longo, M., & Zaninelli, D. (2024). Batteries: Advantages and importance in the energy transition. In: Passerini, S., Barelli, L., Baumann, M., Peters, J., Weil, M. (Eds.) *Emerging battery technologies to boost the clean*

energy transition. The materials research society series (pp. 69–82). Springer. https://doi.org/10.1007/978-3-031-48359-2_5

DIN Deutsches Institut für Normung e. V. (2006). *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (IEC 60812:2006); German version EN 60812:2006. (DIN EN 60812:2006-11)*. DIN Media GmbH.

DIN Deutsches Institut für Normung e. V. (2021). *Medizinprodukte - Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke (ISO_13485:2016); Deutsche Fassung EN_ISO_13485:2016_+ AC:2018_+ A11:2021. (DIN EN ISO 13485:2021-12)*. DIN Media GmbH.

European Parliament and the Council. (2017). Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (2017/745). European Union. https://eur-lex.europa.eu/eli/reg/2017/745/oj

Gokulakrishnan, D., & Venkataraman, S. (2025). Ensuring data integrity: Best practices and strategies in pharmaceutical industry. *Intelligent Pharmacy*, *3*(4), 296–303. https://doi.org/10.1016/j.ipha.2024.09.010

Hayashi, Y., Takagi, M., Kakihara, J., Tatsumi, H., Atsushi, D., & Yoshiyama, M. (2017). A case of unexpected early battery depletion caused by lithium cluster formation in implantable cardioverter-defibrillator. *Journal of Cardiology Cases*, *15*(6), 184–186. https://doi.org/10.1016/j.jccase.2017.02.007

International Electrotechnical Commission (IEC). (2020). Secondary cells and batteries containing alkaline or other non-acid electrolytes - safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications, (IEC 621332). International Electrotechnical Commission.

Keppeler, M., Tran, H.-Y., & Braunwarth, W. (2021). The role of pilot lines in bridging the gap between fundamental research and industrial production for lithium-ion battery cells relevant to sustainable electromobility: A review. *Energy Technology*, *9*(8), 2100132. https://doi.org/10.1002/ente.202100132

Kohl, B., Krüger, M., Dietl, T., Lechner, M., Trunzer, E., Merklein, M., Sedlmaier, A., & Vogel-Heuser, B. (2022). Analysis of distributed-ledger-technology for the exchange of design, production and simulation data in roll forming. *IOP Conference Series: Materials Science and Engineering*, *1238*(1), 012070. https://doi.org/10.1088/1757-899X/1238/1/012070

Lechner, M., Christ, T., Frey, P., Wituschek, S., Arzhanov, A., Petrov, F., & Merklein, M. (2020). Blockchain in der Blechverarbeitung. *Wt Werkstattstechnik Online*, *110*(10), 704–708. https://doi.org/10.37544/1436-4980-2020-10-60

Li, J., Fleetwood, J., Hawley, W. B., & Kays, W. (2022). From materials to cell: State-of-the-art and prospective technologies for lithium-ion battery electrode processing. *Chemical Reviews*, *122*(1), 903–956. https://doi.org/10.1021/acs.chemrev.1c00565

Minespider GmbH (Ed.). (2025). Open battery passport - The most advanced in the market. Minespider GmbH. https://www.openbatterypassport.com/

Morais, E., Koens, T., van Wijk, C., & Koren, A. (2019). A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, *1*(8), 1–17. https://doi.org/10.1007/s42452-019-0989-z

OASIS Open. (2022). MQTT version 50. OASIS Open. https://www.oasis-open.org/standard/mqtt-v5-0-os/

Otte, S. (2026). *Data set supporting the findings of Publication 'Blockchain-Based Secure and Transparent Data Storage on Process Level for Traceability and Data Integrity in the Continuous Mixing Process in Battery Cell Manufacturing': Data Repository of publication* https://figshare.com/articles/dataset/Data_set_supporting_the_findings_of_Publication_Blockchain-Based_Secure_and_Transparent_Data_Storage_on_Process_Level_for_Traceability_and_Data_Integrity_in_the_Continuous_Mixing_Process_in_Battery_Cell_Manufacturing_/31407723?file=62150418. https://doi.org/10.6084/m9.figshare.31407723

Otte, S., Maelger, J., Schabel, S., Nirschl, H., & Fleischer, J. (2025). Systematic investigation of the residence time distribution in a twin-screw extruder for the continuous mixing process of electrode slurry in the battery cell production. *Energy Technology*, *13*(9), 202402196. https://doi.org/10.1002/ente.202402196

Otte, S., Reuscher, L., Keller, D., & Fleischer, J. (2024). *Blockchain architecture for process-level traceability of continuous mixing process in battery cell production* [Paper presentation]. 2024 1st International Conference on Production Technologies and Systems for E-Mobility (EPTS) (pp. 1–14). IEEE. https://doi.org/10.1109/EPTS61482.2024.10586718

Otte, S., Sufian, N. N. A. M., Schabel, S., & Fleischer, J. (2024). Identification of relevant parameters for traceability in the continuous mixing process in battery cell production. *Energy Technology*, *12*(7), 2400493. https://doi.org/10.1002/ente.202400493

Pokorney, S. D., Greenfield, R. A., Atwater, B. D., Daubert, J. P., & Piccini, J. P. (2014). Novel mechanism of premature battery failure due to lithium cluster formation in implantable cardioverter-defibrillators. *Heart Rhythm*, *11*(12), 2190–2195. https://doi.org/10.1016/j.hrthm.2014.07.038

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, *7*(2), 229–233. https://doi.org/10.1016/j.icte.2020.09.002

Prasad, S., Tiwari, N., Chawla, M., & Tomar, D. S. (2024). Zero-knowledge proofs in blockchain-enabled supply chain management. *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications* (pp. 47–70). https://doi.org/10.1007/978-981-97-0088-2_3

Rescorla, E. (2018). *The transport layer security (TLS) protocol version 1.3*. Advance online publication. https://doi.org/10.17487/RFC8446

Rufino Júnior, C. A., Sanseverino, E. R., Gallo, P., Koch, D., Schweiger, H. -G., & Zanin, H. (2022). Blockchain review for battery supply chain monitoring and battery trading. *Renewable and Sustainable Energy Reviews*, *157*, 112078. https://doi.org/10.1016/j.rser.2022.112078

Tietjen, T., & Decker, A. (2020). *FMEA-Praxis: Einstieg in die Risikoabschätzung von Produkten, Prozessen und Systemen* (4 überarbeitete Auflage). Hanser eLibrary (Hanser). https://doi.org/10.3139/9783446465640?locatt=mode:legacy

U.S. Food and Drug Administration (FDA), Department of Health and Human Services. (1996). *Quality system regulation (21 CFR Part 820)*. Electronic Code of Federal Regulations (eCFR). https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-820

VDMA Batterieproduktion. (2023). *Roadmap Batterie-Produktionsmittel 2030: Update 2023*.

Wong, P.-M., Sinha, S. R. K., & Chui, C.-K. (2021). Blockchain in manufacturing quality control: A computer simulation study. *PloS One*, *16*(3), e0247925. https://doi.org/10.1371/journal.pone.0247925