

Analysis of Distributed-Ledger-Technology for the Exchange of Design, Production and Simulation Data in Roll Forming

B Kohl¹, M Krüger², T Dietl¹, M Lechner³, E Trunzer², M Merklein³, A Sedlmaier¹ and B Vogel-Heuser²

¹ data M Sheet Metal Solutions GmbH, Am Marschallfeld 17, 83626 Valley, Germany

² Institute of Automation and Information Systems, Technical University of Munich, Boltzmannstr.15 85748 Garching, Germany

³ Institute of Manufacturing Technology, Friedrich-Alexander-Universität Erlangen-Nürnberg, Egerlandstr. 13, 91058 Erlangen, Germany

E-mail: b.kohl@datam.de

Abstract. Digitalization in the metal forming industry needs to be improved to achieve the goals set by Industrie 4.0. Distributed-Ledger-Technology (DLT) has been identified as a promising foundation for tackling the underlying problem of consistent information exchange. DLT-based solutions have already been developed, but none explicitly covers the roll forming use-case. This paper presents a Hyperledger-Fabric-based blockchain network to fill this research gap. This network is specifically designed for the roll forming industry, while still aiming to meet general information exchange requirements. The roll forming use-case is divided into the material supply chain and a design/simulation workflow. Participants and parameters in these two data transfer chains have been validated with the help of industry experts. Running the conceptualized network on an on-premise server has allowed for a detailed evaluation. Feedback provided by experts of the roll forming industry shows the potential of the presented network. Furthermore, the presented solution covers requirements often neglected by existing approaches like large data handling, compatibility to existing interfaces, secure communication, and access rights definition. In summary, this paper provides a pioneering implementation and evaluation of a DLT-based solution for the roll forming industry and, therefore, a foundation for the next steps towards Industrie 4.0.

1. Introduction

A system entirely in line with the concept of Industrie 4.0 requires data transfer among companies [1]. However, this transfer is rarely satisfying in the metal forming industry [2]. To tackle the challenges of information exchange in the sheet metal industry, blockchain, and with it, Distributed-Ledger-Technology (DLT), have been identified as promising technologies [2]. DLT denotes the concept of storing a blockchain decentralized on each participating node with automatic synchronization [3]. First applications of such blockchain networks for the sheet metal industry do exist, e.g., by Frey et al. [4], but the roll forming industry has been uninvestigated. In this industry, extensive supply chains with many participants are prevalent [5], providing a challenge for secure information exchange. This paper presents a pioneering approach to tackle this challenge by making use of the main properties of blockchain



networks for information exchange: proof of data ownership, maintaining data integrity, system verifiability, and no need for a central authority [4]. Concluding, the contribution of this work is the unprecedented conceptualization and implementation of a blockchain network specifically for roll forming including its evaluation against the requirements for a trustworthy information exchange solution. Chapter 2 covers the definition of requirements, chapter 3 covers existing approaches in the research field and compares these solutions and requirements. Furthermore, chapter 4 presents the conceptualized network and chapter 5 the implementation. In chapter 6, the results are evaluated and discussed, followed by conclusions and future work in chapter 7.

2. Requirements for an Information Exchange Solution

An information exchange solution must follow authentication and encryption rules (R1). Having data available to the correct parties leads to the necessity of a proper access rights definition (R2). To establish trust in data, control mechanisms to prove the validity of data need to be in place. Unwanted change of data in storage needs to be prevented or at least detected (R3). Besides, maintaining integrity during transmission is essential for information exchange (R4). The high measuring rates of modern sensors must be handled without significant delay for live applications, e.g., monitoring, (R5). In addition to R5, sensors provide data over various interfaces. For integration in existing systems, these interfaces need to be supported. One of the most used protocols is the Open Platform Communications Unified Architecture (OPC UA) [6], support for which is a minimum requirement (R6). Additionally, large files are another extreme to be considered since simulation results are stored in files of up to 50 GBs, which the system needs to handle reliably (R7). Current data transfer solutions often rely on a trusted third party, like a cloud provider, but finding a third party that every participant trusts can prove complicated. To circumvent this problem, a solution that itself is trustworthy is necessary. This trustworthiness needs to be verifiable by all participants (R8). While cloud solutions are getting much attention nowadays, industrial companies might prefer to run the system on-premise (R9). Since data might contain sensitive information, using a public system would require extreme effort to prevent unauthorized access. Thus, participation in the system should be regulated (R10). Finally, the system should be applied to a real-world roll forming use-case. This does not mean realizing an industrial setup, which would require more economic considerations. Rather, actual formats and dimensions of the transferred data need to be determined, and the system evaluated accordingly (R11). Table 1 highlights the derived requirements.

Table 1. Derived requirements for data transfer in roll forming

Requirement	Formulation
R1	Entities are authenticated and communication is encrypted.
R2	The system supports CRUD (create, read, update, delete) access rights.
R3	The system prevents or detects an unwanted change of stored data.
R4	Data integrity is maintained during transmission.
R5	The system processes data points arriving at high rates.
R6	The system accepts data via the OPC UA protocol.
R7	The system processes files with a maximum size of 50 GB.
R8	The system needs to be reviewable by all participants.
R9	The system can be hosted on local hardware.
R10	Participation in the system is restricted.
R11	The system is evaluated with a real-world roll forming use-case.

3. Current State of Research and Technology

Raj et al. [7] propose an application for integrity-based authentication and secure information transfer for hospital management systems using symmetric encryption. Integrity is maintained using hash algorithms and authentication is handled by a public-key-based system. Another cloud-based solution is proposed by Huang et al. [8]. Their main goal is a secure data storage and sharing scheme handling the specific challenges of Cyber-Physical-Social-Systems. Putz et al. [9] present a blockchain-based implementation of a digital twin, including an Ethereum-based prototype. A performance-focused approach called FastFabric is presented by Gorenflo et al. [10], achieving roughly 20,000 transactions per second. Frey et al. [4] present a small-scale production example in the metal forming industry. In their work, a strong focus is placed on the accessibility of data gathered along the supply chain. In addition to the theoretical considerations, a demo factory is established. Each machine is equipped with a blockchain interface (BCI), and each BCI acts as a node for the blockchain network with its own copy of the chain. Most of the presented solutions above do not directly store data on a blockchain but mostly in undefined off-chain storage. Baumung et al. [11] present a blockchain-based order provisioning and processing system for additive manufacturing, including cloud-based off-chain storage. Public-key encryption is used to secure data stored in the cloud. A final approach concerning additive manufacturing is presented by Schmiedel [12]. This project produces a proof of concept for the use of DLT in additive manufacturing. The project bases this proof on a machine with an OPC UA-based control system as the data provider.

Table 2 puts the above-presented approaches in relation to the defined requirements of the previous section. The table shows a lack of roll forming-specific solutions (R11). In addition,

Table 2. Solutions vs. requirements

Approach	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Bindhu Raj et al. [7]	✓	✓	✓	✓	—	—	—	—	—	✓	—
Huang et al. [8]	✓	✓	✓	✓	✓	—	✓	—	—	✓	—
Putz et al. [9]	✓	✓	✓	✓	✓	—	—	✓	✓	✓	—
Gorenflo et al. [10]	—	—	✓	✓	✓	—	—	✓	✓	✓	—
Frey et al. [4]	—	✓	✓	✓	✓	—	—	✓	✓	✓	—
Baumung et al. [11]	—	—	✓	✓	—	—	✓	✓	✓	✓	—
Schmiedel [12]	—	—	✓	✓	✓	✓	—	✓	✓	✓	—

✓: fulfilled, —: not fulfilled

integration of existing interfaces is uncommon (R6), as is the explicit handling of large files (R7). Integrity (R3, R4) is generally part of the existing solutions, be it via explicit integrity checks in cloud-based approaches or via the implicit architecture of a blockchain. Only half of the presented solutions take care of authentication and encryption (R1). The situation is similar concerning access rights definition (R2). Handling data with high measuring rates is a well-handled requirement (R5). The DLT-based solutions are reviewable by all participants, which proves to be complicated for cloud-based ones (R8). Running the approach on local hardware is mainly restricted by the use of central cloud storage (R9). All of the presented systems restrict participation in some way (R10). In conclusion, the central research gap is the explicit evaluation of an information exchange system for the roll forming use-case. This gap emphasizes the need for a trustworthy data exchange solution suited for the roll forming industry, a need covered by the considerations, implementation, and evaluation presented in this paper.

4. DLT Concept for Data Transfer in Roll Forming

This chapter defines the conceptualized system for exchanging design, production, and simulation data in roll forming based on Distributed-Ledger-Technology to fill the research gap identified in the previous chapter. This paper divides data transfer in metal forming into the material supply chain and the design-simulation workflow as described in the following sections.

4.1. The Roll Forming Material Supply Chain

An up-to-date and detailed supply chain depiction is needed in order to correctly represent this area in the blockchain network. Thus, this paper presents an unprecedented overview of the cold roll forming material supply chain shown in Figure 1. The participants and the collected parameters are carefully selected and have been validated by industry experts. In addition to this overview's use for the presented work, it provides a basis for further investigations on the roll forming industry's supply chain. The categories are chosen as defined by Frey et al. [4].

	Process	Material	Organizational
Raw Material Mining	<ul style="list-style-type: none"> Energy Consumption CO2-Footprint 	<ul style="list-style-type: none"> Raw Material Composition 	<ul style="list-style-type: none"> Mining Details
Steel Manufacture	<ul style="list-style-type: none"> Blast Furnace Temperature Pouring Temperature Flow Rate CO2-Footprint Vacuum Treatment Slab Scarfing 	<ul style="list-style-type: none"> Width Side Profile Composition Thickness Surface Defects Material Designation 	<ul style="list-style-type: none"> Storage details Customer Slab ID Heat number Heat equence Batch separation
Hot Rolling	<ul style="list-style-type: none"> Material Temperature Speed, Stand Forces Cooling Time Furnance Temperature Coiling Temperature CO2-Footprint Pickling (Y/N) and Method Input/Output in kg and m 	<ul style="list-style-type: none"> Width, Length Coil Weight, Composition Material Designation Surface Defects Geometrical Deviations Mechanical Properties Thickness over Width and Length 	<ul style="list-style-type: none"> Storage Details Customer Coil ID
Post Process	<ul style="list-style-type: none"> Circular Shear Blade Configuration Insertion Depth Input / Output in Meters 	<ul style="list-style-type: none"> Width, Length, Thickness Weight, Material Designation Cutting Burr Position Surface Defects and Position Position of Cross Welds 	<ul style="list-style-type: none"> Strip ID Strip Position on Mother-Coil Processing Line
Slitting	<ul style="list-style-type: none"> Speed Stand Forces Setup Parameters Input / Output in Meters Theoretical Output-Weight 	<ul style="list-style-type: none"> Profile Geometry Length Twist Hole Pattern Dimensions Mechanical Properties Material Designation Relevant Standard 	<ul style="list-style-type: none"> Storage Details, Part ID Customer Origin (Coil, Slitting Position) Number of Profiles/Pieces Theoretical Weight of Bundle Bundle-ID Date of Production/Shipment Date of Expiry (Corrosion Protection)
Cold Roll Forming	<ul style="list-style-type: none"> Inclusion in Assembly 	<ul style="list-style-type: none"> End Product Parameter 	<ul style="list-style-type: none"> Storage Details Customer Part ID
Use			

Figure 1. Participants and parameters in the roll forming material supply chain

4.2. The Roll Forming Design and Simulation Workflow

The long-standing industry experience of simulation engineers at data M Sheet Metal Solutions GmbH provides the foundation for the design and simulation workflow. Thus, the details of this workflow are based mainly on the software packages developed by data M. In general though, the handling of information in this workflow is software-independent. The participants are entities

handling cold roll forming, designing, simulating, and roll tool manufacturing. The roll former acts as the initiator in this workflow. First, they send a customer inquiry to the designer in the form of a pdf file containing the necessary information on how to create the design. The designer uses COPRA[®] RF [13] to create a forming strategy from this information. COPRA[®] RF is a commonly used design software in the roll forming industry and has been used in scientific papers before, e.g. by Sedlmaier et al. [14]. To validate the created forming strategy, a specific design state is exported to a proprietary archive file format. In addition, a particular function of COPRA[®] RF called “COPRA2FEA” is used to create a human-readable text file containing basic simulation parameters. The archive and this file are transferred to the simulation entity. Simulation is done using COPRA[®] FEA RF [15]. It provides a graphical user interface to create the input file for the underlying nonlinear finite element analysis solver. The solver outputs the results in a variety of files. The most important of these are the Post-File (.t16) and the Output-File (.out). The Post-File is a binary file reaching sizes of up to 50GB. The Output-File is another human-readable text file. Finally, the simulation results are sent back to the designer, who now has a validated design. This validated design is sent to the roll tool manufacturer (RTM). The RTM uses the validated design to manufacture roll tools, which are then sent to the roll former with a corresponding spec-sheet.

4.3. Covering Information Exchange Requirements with a DLT-based Solution

The participants mentioned above are defined as independent organizations, each participating in the blockchain network (concerns R11). Their authentication is based on a public key infrastructure (PKI). Each entity runs its own certificate authority (CA) to have full control over its members (R1). In addition, this authentication scheme is used to restrict access to the system by only considering CAs of eligible organizations trustworthy (R10). Encryption is also handled by a PKI. Each organization again runs its own CA for this purpose, which provides public-/private-key pairs to entities within the organization. These key pairs are then solely used for encryption, independent of the key pairs for authentication (R1). Data in the system is stored as assets with associated public and private information. Public information contains a unique AssetID, ownership information, a timestamp, and an asset description. This information is stored directly on the blockchain and is readable by everyone with access to the blockchain. Private information covers sensitive data only the asset owner should be able to read. Of this information, only a hash is stored on the blockchain. Access rights for this hash are the same as for public data. On an organizational level, access to these different types of information is defined according to Table 3 (R2). Within an organization, more fine-grained roles are defined. These roles are readers, writers, admins, and endorsements.

Table 3. Access rights on organizational level

	Public				Private			
	C	R	U	D	C	R	U	D
Owner	✓	✓	✓	—	✓	✓	✓	✓
Non-Owner	—	✓	—	—	—	—	—	—

CRUD: create/read/update/delete, ✓: allowed, —: forbidden

To analyze the handling of sensor data (R5, R6), the presented solution covers data provided by an OPC UA server, but the base principles can be transferred to other protocols. A data processing unit is inserted between the OPC UA server and the blockchain network. This

unit's primary purposes are retrieving data from the data source, identifying the asset's private information from the retrieved data, defining the asset's public information depending on the data source, and adding the asset with its private and public information to the blockchain. In addition, non-continuous data is added to the system whenever their corresponding creation occurs. Here, a retraceable path from one asset to its associated asset(s) from previous steps is established. For example, the asset created for a simulation needs to be connected to its underlying design. The retraceable path is established by including the ID(s) of the associated asset(s) in the private information of an asset. Large and binary files (R7) are handled by storing only the hash of the files in the private information of an asset. This mitigates the problem of large files overloading the system. The actual exchange can be outsourced to a solution specifically designed for such a transfer, as Baumung et al. [11] have already suggested. Having established the participants, secured communication, and creating assets, the system must allow the transfer of those assets. To achieve this, a specific smart contract for asset transfer is used, following the asset-transfer-secured-agreement example provided by HLF [16]. Smart contracts are scripts do define and automate multi-level processes. The script for this transfer logic is, like all smart contracts, stored on the blockchain. Thus, it can be reviewed by all participants (R8). Changes to the logic must be unanimously decided. Maintaining integrity during transfer (R4) is based the fact that the hash of an asset's properties is stored publicly on the blockchain during the asset's creation. Thus, before sending, the owner can verify the data against this hash, as does the receiver after getting the data. The hash on the blockchain must not to change for this concept to work. This is ensured by keeping data integrity in storage. Data integrity in storage is implicitly maintained by the blockchain architecture (R3).

5. Implementation

The developed solution is based on Hyperledger Fabric (HLF), a modular and extensible framework for running permissioned blockchain networks [17]. The fundamentals of an HLF network are organizations, channels, peers, and the ordering service. An organization is a set of members belonging together. Having the roll forming use-case in mind, every participant represents their own organization. Channels allow multiple organizations to communicate with each other. Each channel comes with its own blockchain and smart contracts. In the roll forming use-case, a separate channel is created for the material supply chain and the design and simulation workflow, as they are largely independent of each other. While communication between two participants over these channels is secure, establishing additional sub-channels would also be possible. Either way, the use of Transport Layer Security (TLS) ensures, that only the intended recipient can decrypt the transferred information. Peers (or peer nodes) host the ledgers and smart contracts. They belong to an organization and are the actual channel participants. In the designed network, each organization runs exactly one peer for each channel in which it participates. Thus, in the roll forming use-case, each organization runs one peer, except for the cold roll former running two peers, as it is part both of the material supply chain and the design and simulation workflow. Orderer nodes have two base functions. First, they order transactions and add them to new blocks. Second, they host the configurations of channels. Other entities, called clients, participate in the network as well. They are not nodes but belong to an organization, e.g. an administrator for an organization.

Setting up and running a PKI for HLF is streamlined by the Fabric CA framework [18]. The deployment guide of the Fabric CA framework is the foundation of the conceptualized networks PKI. Nodes in the network are hosted using Docker [19] images provided by Hyperledger. The (access) rights definition in Hyperledger Fabric is a multi-layered system. The configuration of channels only allows specific organizations to participate. This configuration is stored on the ordering nodes and can only be changed unanimously. Private data collections [20] provide secrecy for private information by storing only a hash on the blockchain, while the actual private

data is stored in the owner's state database. If private data is transferred, it is sent directly from peer to peer without passing the orderer. Each HLF peer comes with an implicit data collection only readable by itself. The smart contracts, which allow clients to create, transfer, and verify assets, are based on the asset-transfer-secured-agreement example by HLF [21]. This example provides chaincode to transfer assets while keeping details of the asset and transaction private. In HLF, chaincode is the code implementing smart contracts. A central control hub is added to the system to act out the roll forming use-case. This control hub is a web-based user interface providing access to the blockchain network for different organizations. The design layout was provided by data M Sheet Metal Solutions GmbH, as was the basic structure of the underlying web-server and OPC UA Client. All virtual machines (VMs) and containers necessary to run the network are hosted on the same server. This server is equipped with an eight-core processor, 32 GB of RAM, and a PCIe 3.0 x4 NVMe SSD. The server runs Proxmox VE [22], an enterprise-grade, open-source server management platform for virtualization.

6. Evaluation of the Presented System

Evaluation of the system is based on hosting it on the hardware described in the previous section. Fulfillment of requirements is evaluated either with behavior/performance tests or analyzed with the help of research on the underlying technology. Furthermore, the evaluation of the roll forming use-case is based on the other requirement's fulfillment and additional expert's feedback.

The PKI handling the authentication is secure as long as the private key of an entity remains secret and as long as the underlying signing concept is not broken. Leaking of a private key, if detected, can be mitigated by revoking the certificate it belongs to and issuing a new certificate/private-key combination. The underlying signing algorithm is the Elliptic Curve Digital Signature Algorithm (ECDSA) [23]. As of January 2022, ECDSA is not considered broken, but approaches to enhance its security, especially for blockchain use-cases, do already exist [24]. HLF version 2.2 uses TLS 1.3 in its default configuration, which has been proven secure [25]. Thus, secure communication (R1) is achieved with modern algorithms and no known security flaws. However, as the situation in IT security is fluid and new weaknesses are detected regularly, the security of the used algorithms and their implementation have to be monitored.

The implementation of HLF is crucial for the system behavior, i.e., whether access rights control (R2) behaves as defined depends on the software. The following test cases are analyzed by by invoking the respective functions in the chaincode or HLF without the necessary rights:

- (i) Joining a channel the organization is not allowed to join
- (ii) Committing chaincode not approved by all organizations on a channel
- (iii) Changing the public description of an asset not owned by the organization
- (iv) Reading the private data of an asset not owned by the organization

All these calls result in an error and, thus, the system based on HLF 2.2 behaves as expected.

Ensuring the integrity of stored data (R3) is implicitly handled by the DLT/blockchain architecture. To test the behavior of the system in case of an unexpected change of one participant's ledger, the ledger is edited directly on the file system. Unfortunately, HLF does not automatically detect the corruption of a peer's ledger file. Manual detection of unwanted changes can be realized by hashing the ledger file on each peer and comparing the hashes. If an integrity breach is detected, it can be fixed by obtaining a ledger file with integrity from another organization of the same channel and replacing the faulty ledger file. Thus, data integrity in storage is achieved but needs constant monitoring. An automated solution would be preferred to reduce administration efforts and susceptibility to errors.

The integrity of transferred data (R4) can be verified by comparing the hash of the current asset's properties against the hash of the asset's properties at creation. This can be done using

a specific chaincode function called `VerifyAssetProperties()`. It takes as arguments the `assetID` and private asset properties and returns whether the given properties match the ones stored on the blockchain. If sender and receiver verify the sent asset's properties before and after the transfer process, data integrity is preserved throughout the transaction.

Performance of the system (R5) is evaluated by how long it takes to create an asset, which is around 100 ms. This is far from the potential of HLF-based solutions, as performance-optimized solutions like FastFabric achieve around 20,000 transactions per second [10]. In addition, this performance is insufficient to cover the continuous gathering of sensor data. Thus, only sensor information should be stored on the blockchain, while sensor data is exchanged off-chain.

How an existing data-providing interface can be integrated into the system (R6) is investigated with OPC UA as an example. In general, retrieving data from an OPC UA server, processing it, and continuously writing to the blockchain works. This is tested by connecting to an OPC UA server, subscribing to one of its variables, and writing the processed data point as an asset to the blockchain. However, this process is limited by the performance of the system.

The handling of large files (R7) is realized by hashing them, adding the hash to the private properties of the corresponding asset, and transferring the large files off-chain. SHA256 [26] was used as the hashing algorithm, as programs for its calculation are readily available on almost every platform. Besides, it provides an adequate performance/security ratio. Even with the low spec setup used in the presented network, calculating the SHA256 hash of a 50 GB file took less than four minutes. Considering that these large files occur only after complex simulations, four minutes do not present a problem, as the duration of these simulations is significantly longer. Secure off-chain storage was not investigated in the scope of this paper and could be added in the future. One approach for off-chain storage could be a self-hosted cloud solution which, compared to cloud service providers, leaves full control of the system to the participants. Another approach, as proposed by Baumung et al. [11], could be based on the InterPlanetary File System (IPFS) [27], a peer-to-peer protocol for data exchange

To evaluate the verifiability of the system (R8), it is subdivided into channel setup and chaincode behavior. The configuration block of a channel can be fetched by any channel participant. Thus, every organization can verify the channel setup independently. In addition, the influence each organization has on the logic of the system, defined in smart contracts, is even more substantial. Smart contracts can only be added to a channel if every organization approves. Thus, each organization can verify the transaction logic independently. In addition, considering the explained setup, each VM and container runs with little resources. Each peer and ordering node is assigned two GB of RAM and four vCPUs comparable to small single-board computers. This allows the system to be hosted on-premise (R9) with low expenses. Restriction of participation (R10) is realized by explicitly listing the authorized organizations in the channels' configuration blocks. Trying to join a channel without the authorization to do so results in an error, ensuring a permissioned network.

The roll forming use-case (R11) is implicitly evaluated with the previous points, as the general requirements are also valid for the roll forming use-case. In addition, the presented network is explicitly designed to represent the material supply chain and the design and simulation workflow of roll forming. The system provides a variety of benefits:

- (i) No participant needs to trust statements of a third party about setup and behavior as they can independently verify the system.
- (ii) Asset ownership is unambiguously defined. The owner has full control over their assets.
- (iii) An asset's properties are immutable, except for its owner and the public description. Verifying that information has not been changed is, therefore, possible at any given time.
- (iv) Every asset's transaction history is retraceable. Combining this with an asset's immutable properties allows verification of an asset's origin and content, even over several transactions.

These benefits are the main reasons companies in the roll forming industry would introduce DLT. Since the system itself can evaluate ownership and integrity of data, the need to engage a third party for this evaluation is made obsolete. This leads to potential cost savings and more trust among the participants. Such incentives are needed, as adopting a new data handling system is associated with high expenses. Especially the material supply chain participants face a high effort, as production and sales departments would have to be integrated for the system to function as described. Production-ready prototypes in publicly funded research projects could be a first step for the introduction of DLT in this context. In the design and simulation workflow data M Sheet Metal Solutions GmbH provides a comprehensive software package with their COPRA[®] Eco System which is uniformly used by the participants. Presented with a live demonstration of the blockchain network, feedback from multiple data M experts with longstanding experience in the industry has been highly encouraging, especially concerning the integration of DLT into the existing software. This integration could reduce the effort and knowledge required from each participant while maintaining the system's benefits.

7. Summary and Outlook

Secure communication is achieved by PKIs for authentication and encryption, utilizing ECDSA and TLS 1.3. Clear access rights are defined for data within the system. Data integrity in storage is maintained by manually checking the ledger files for inconsistencies. Hashing files at creation and using this hash for comparison in the transaction process provides data integrity during transmission. System throughput is unsatisfactory, with ten transactions per second. OPC UA-provided data can be added to the system, representing existing interfaces, but the low system performance interferes with this integration. Large files are hashed, and only the hash is stored on the blockchain, while the actual data is transferred off-chain. Integrity verification and ownership proof are thus still achieved for these files. Every participant can view the necessary configurations and behavior-defining programs. The system runs on low spec hardware, making it feasible to run it on-premise. Organizations can only join the network if explicitly stated in a channel's configuration, making it non-public. Finally, the material supply chain and design and simulation workflow in roll forming have been defined and used to evaluate the system.

Future work on this topic starts with the slow performance diminishing the system's usability in a production environment. Here, more investigation of the reasons for the slow performance is needed, as the problems could be software- or hardware-related. Furthermore, the compatibility to existing interfaces needs expansion. On one side, this expansion could focus on communication protocols like Message Queuing Telemetry Transport (MQTT) [28]. On the other side, research could focus on using technology-independent data collection as described by Trunzer et al. [29] for a more general interface integration into the system. Another aspect could be a test in an industrial environment. The system's reliability needs to be improved for industrial use, as the current network does not include node redundancy. The introduction of DLT to the roll forming industry would then be another research topic, e.g., by setting up an industrial prototype in production or by doing a detailed cost-benefit analysis.

Because the presented solution tackles step three, networking and integration, of the five-step model presented by Bauernhansl et al. [1], it provides a basis for research covering the next stage towards Industrie 4.0. According to Traub et al. [30], autonomous processes are the next step in roll forming. With smart contracts, modern DLT frameworks provide an intriguing concept for this step. In conclusion, the presented DLT-based network fills the detected research gap by providing a pioneering conceptualization and implementation of a DLT-based information exchange solution for roll forming. In addition, it provides an unprecedented overview of the cold roll forming supply chain as well as detailed insight into the design and simulation workflow of the industry. Consequently, it provides a foundation for further research on DLT-based information exchange, on industrial applications, and on the next step towards Industrie 4.0 in roll forming.

References

- [1] Bauernhansl T, Krüger J, Reinhart G and Schuh G 2016 *WGP-Standpunkt Industrie 4.0*
- [2] Hagenah H, Schulte R, Vogel M, Hermann J, Scharrer H, Lechner M and Merklein M 2019 4.0 in metal forming – questions and challenges *Procedia CIRP* **79** 649–654
- [3] Ranathunga T, Marfievici R, McGibney A and Rea S 2020 A dlt-based trust framework for iot ecosystems *2020 Int. Conf. on Cyber Security and Protection of Digital Services (Cyber Security)* pp 1–8
- [4] Frey P, Lechner M, Bauer T, Shubina T, Yassin A, Wituschek S, Virkus M and Merklein M 2019 Blockchain for forming technology – tamper-proof exchange of production data *IOP Conf. Series: Materials Science and Engineering* **651** 012046
- [5] English M, Castellucci M and Mynors D 2006 Eco-efficiency of the cold roll formed product supply chain *J. of Materials Processing Technology* **177** 626–629
- [6] IEC TR 62541-1:2020 2020 *OPC unified architecture - part 1: overview and concepts* International Electrotechnical Commission
- [7] Raj L B, Vandana R and Kumar B J S 2020 Integrity based authentication and secure information transfer over cloud for hospital management system *2020 4th Int. Conf. on Intelligent Computing and Control Systems (ICICCS)* pp 139–144
- [8] Huang L, Zhang G and Yu S 2020 A data storage and sharing scheme for cyber-physical-social systems *IEEE Access* **8** 31471–31480
- [9] Putz B, Dietz M, Empl P and Pernul G 2021 Ethertwin: Blockchain-based secure digital twin information management *Information Processing & Management* **58** 102425
- [10] Gorenflo C, Lee S, Golab L and Keshav S 2019 Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second *2019 IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC)* pp 455–463
- [11] Baumung W and Fomin V V 2018 Increasing the utilization of additive manufacturing resources through the use of blockchain technology for a production network *CEUR Workshop Proc.* **2158** 135–141
- [12] Schmiedel C Vertrauen 4.0 URL <https://www.ipk.fraunhofer.de/de/publikationen/futur/futur-online-exklusiv/vertrauen40.html>
- [13] data M Sheet Metal Solutions GmbH COPRA RF URL <https://www.copra.info/en/crf>
- [14] Sedlmaier A, Dietl T and Harraßer J 2019 Digitizing roll forming with smart sensors *AIP Conf. Proc.* **2113** 170017
- [15] data M Sheet Metal Solutions GmbH COPRA FEA RF URL <https://www.copra.info/en/fea>
- [16] Hyperledger Fabric Fabric CA Deployment Guide URL <https://hyperledger-fabric-ca.readthedocs.io/en/release-1.4/deployguide/ca-deploy.html>
- [17] Androulaki *et al* 2018 Hyperledger fabric: A distributed operating system for permissioned blockchains *Proc. of the 13th EuroSys Conf. EuroSys '18* (New York, NY, USA: ACM)
- [18] Hyperledger Fabric URL <https://github.com/hyperledger/fabric-ca>
- [19] Docker Inc URL <https://www.docker.com/>
- [20] Hyperledger Private data URL <https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html>
- [21] Hyperledger Fabric asset-transfer-secured-agreement URL <https://github.com/hyperledger/fabric-samples/tree/master/asset-transfer-secured-agreement>
- [22] Proxmox Server Solutions GmbH URL <https://www.proxmox.com/en/proxmox-ve>
- [23] ANSI X9.62 2015 *Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ecdsa)* American National Standards Institute
- [24] Basha S J, Veeram V S, Ammannamma T, Navudu S and Subrahmanyam M 2021 Security enhancement of digital signatures for blockchain using eddsa algorithm *2021 3rd Int. Conf. on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* pp 274–278
- [25] Levillain O 2021 Implementation flaws in tls stacks: lessons learned and study of tls 1.3 benefits *Risks and Security of Internet and Systems* ed Garcia-Alfaro J, Leneutre J, Cuppens N and Yaich R (Springer International Publishing) pp 87–104
- [26] FIPS PUB 180-4 2015 *Secure hash standard* National Institute of Standards and Technology
- [27] Protocol Labs IPFS URL <https://ipfs.io/>
- [28] ISO/IEC 20922:2016 2016 *Information technology - message queuing telemetry transport (mqtt) v3.1.1* International Organization for Standardization
- [29] Trunzer E, Prata P, Vieira S and Vogel-Heuser B 2019 Concept and evaluation of a technology-independent data collection architecture for industrial automation *IECON 2019 - 45th Annual Conf. of the IEEE Industrial Electronics Society* pp 2830–2836
- [30] Traub T, Gregório M G and Groche P 2018 A framework illustrating decision-making in operator assistance systems and its application to a roll forming process *The Int. J. of Advanced Manufacturing Technology* **97** 3701–3710