Private Multi-Hop Accountability for Supply Chains

Jan Pennekamp*, Lennart Bader*, Roman Matzutt*, Philipp Niemietz†,
Daniel Trauth†, Martin Henze‡, Thomas Bergs†, Klaus Wehrle*
*Communication and Distributed Systems, RWTH Aachen University, Germany · {lastname}@comsys.rwth-aachen.de
†Laboratory for Machine Tools and Production Engineering, RWTH Aachen University, Germany
{p.niemietz, d.trauth, t.bergs}@wzl.rwth-aachen.de
‡Cyber Analysis & Defense, Fraunhofer FKIE, Wachtberg, Germany · martin.henze@fkie.fraunhofer.de

***Abstract*—Today's supply chains are becoming increasingly flexible in nature. While adaptability is vastly increased, these more dynamic associations necessitate more extensive data sharing among different stakeholders while simultaneously overturning previously established levels of trust. Hence, manufacturers' demand to track goods and to investigate root causes of issues across their supply chains becomes more challenging to satisfy within these now untrusted environments. Complementarily, suppliers need to keep any data irrelevant to such routine checks secret to remain competitive. To bridge the needs of contractors and suppliers in increasingly flexible supply chains, we thus propose to establish a *privacy-preserving* and *distributed* multi-hop accountability log among the involved stakeholders based on Attribute-based Encryption and backed by a blockchain. Our large-scale feasibility study is motivated by a real-world manufacturing process, i.e., a fine blanking line, and reveals only modest costs for multi-hop tracing and tracking of goods.**

***Index Terms*—supply chain; multi-hop tracking and tracing; blockchain; attribute-based encryption; Internet of Production**

I. Introduction

Traditionally, companies relied on few (trusted) supply chain partners within long-lasting relationships [1]. This approach enabled a close and simple interconnection of mutually trusting and well-known partners. Novel paradigms, such as the Internet of Production (IoP) [2], revise these patterns and instead envision to improve production processes by shifting to highly flexible supply chains and business relationships. These changes mandate research to enable secure and privacy-preserving industrial collaborations. Companies can then react and adapt their processes to the quality of received parts or products as digital information of the physical workpiece is transparently available along the supply chain, i.e., they are expected to exchange more information across company borders. Likewise, companies can more easily look for (new) temporary suppliers for specific customer change requests.

Both aspects increase the need for reliable accountability guarantees in highly distributed supply chains, as more and more partners and their information are untrusted [3]. Especially, the anticipated cross-border relationships raise this challenge as different companies of a single supply chain can operate in jurisdictions with different legislative requirements [4]. Consequentially, companies might refrain from such relationships to mitigate risks. However, even in digitized environments, the available information is usually not shared over multiple hops of a supply chain due to its sensitive nature, i.e., information is only available (and retained) locally [5]. This constraint hinders any statements or queries about the complete supply chain of a product and its origin.

The straightforward solution to provide the required data to all involved companies would be centralized data sinks breaking the hop-by-hop information flow of today's opaque supply chains. However, collaborators need to protect their business secrets, including a list of suppliers or their utilization and scale of production [5]. This need is especially evident within the IoP, where strong trust assumptions are lacking, and thus no universally trusted potential operator of such a data sink exists. Hence, both accountability and confidentiality of production processes and data need to be carefully gauged.

To establish accountable-yet-confidential supply chains for the IoP, we present an architecture that enables disclosing past events relating to the supply chain in a privacy-preserving and accountable manner. Particularly, our architecture enables to trace and track parts and products across multiple hops in the supply chain without active participation of companies. While tracking can be employed to follow a single component to its final product and customer, tracing enables companies to investigate root causes of product failures or damages. Thereby, our approach mitigates trust barriers stemming from more volatile collaborations in the IoP while still enabling companies to seize the potential of increased flexibility.

Contributions. The main contributions of our paper are:

- **(a)** We present a novel blockchain-backed architecture to enable *privacy-preserving multi-hop accountability* for supply chain data even in dynamic settings based on the concept of attribute-based encryption,
- **(b)** we conduct a *large-scale feasibility* study based on a real-world scenario, i.e., we consider the supply chain of a fine blanking manufacturing process, and
- **(c)** we show that the functionality offered by our design incurs only *modest costs for (multi-hop) tracking and tracing* of specific components within supply chains.

With our contributions, we improve trust and information exchange in existing supply chains as well as foster the establishment of new and volatile business relationships.

II. The State of Digital Supply Chains

As a foundation for our work, we first provide an overview of previous research in the field of supply chains (Section II-A), before introducing industry-desired accountability features for highly-dynamic supply chains (Section II-B).

Author manuscript.

A. Related Work

Improving well-established behavior in the context of supply chains is a complicated endeavor due to the opaque structure of relationships and the involvement of sensitive, valuable data. In the following, we briefly look into approaches that propose to make this information more broadly available, e.g., to improve the verifiability of product origins.

Supply Chain Transparency. In the past, companies mainly considered the supply chain from their local perspective [6]. Therefore, issues such as the bullwhip effect [7] still occur. However, increased collaboration between companies along supply chains is expected to be beneficial in various dimensions [6], [8]. Yet, such advances require joint planning and information exchange, i.e., participating companies have to act transparently. While Flynn et al. [1] conduct a performance study on supply chain collaboration, they neglect the potential of multi-hop transparency. We refer to related work [9] for a general evaluation of different collaboration models. Even though the benefits of transparency are well understood, the impact of data sharing over multiple hops is insufficiently studied. We believe that a lack of a supporting architecture is a main reason for this situation.

Digitized Supply Chains. Digitized supply chains can help to improve automation and transparency between two parties. Korpela et al. [10] identify the requirements and needs of such collaborations. Digitizing not only the monitoring of items and processes but also the specification of delivery criteria are seen as a potent enhancement to enable fine-granular adjustments at subsequent production steps [3]. However, the digitalization of all aspects of the supply chain is an ongoing research area, and uncertainties regarding privacy-preserving data sharing remain.

Blockchain-Backed Supply Chains. Blockchain technology promises to be a natural fit for supply chains as it offers verifiable and tamperproof storage without requiring a trusted third party [10], [11]. Achieving that no single entity has control over all information is strongly desirable in a setting with distrustful parties. Wüst et al. [12] provide guidelines on whether blockchain technology is a fit for a specific scenario, and they consider supply chains as one of their use cases.

Various works integrate this technology into their designs. For example, Malik et al. [13], [14] introduce blockchain-backed approaches to improve trust and product traceability, especially focusing on food chains and governmental oversight. However, their assumption of trustworthy participants contradicts our presumption of low-trust environments and the resulting requirement for advanced privacy protection.

Abeyratne et al. [15] study the applicability of blockchain technology and propose to record all interactions of a product during its lifecycle in a blockchain while limiting access to data with role-based access control. Therefore, the role of a supplier must be known in advance, and involved companies are visible to all participants. Further work [16], [17] proposed to realize multi-hop tracing in supply chains by utilizing Ethereum-based smart contracts. However, these approaches do not look into more sophisticated data privacy needs.

Takeaway. Overall, blockchain established itself as a suitable approach in the domain of supply chains, especially due to its decentralized nature. While research identified the need for traceability, they do not yet offer fine-granular privacy the protection of information for the involved companies.

B. Desired Accountability Features

The digitalization of supply chain information and the increasing flexibility of relationships in the industrial setting mandate more sophisticated accountability features to ease the identification of root causes. For example, appropriate information can help to improve business processes as tracking of batches with inferior quality is simplified. Besides, this data can help companies to trace the origin of faulty parts or components more easily. At the same time, companies expect protection of their sensitive business data. In particular, we identify three desired accountability features in this setting.

Multi-Hop Tracking. If a company needs to identify products or components that contain its workpieces, traditionally, it has to query all companies in the supply chain as tracking data is not globally available. To simplify this process, the supply chain environment should provide this information without the need for repeated queries to all companies. Today, especially defunct or merged companies make this process challenging.

Multi-Hop Tracing. Similarly, companies might need to identify the origin of a product or components which they have used during production. For example, they want to know about the source of faulty components, or they want to verify originality. Again, such an inquiry currently requires the on request participation of all involved companies in the supply chain. An improved environment should return this data without (mandatory) participation by all involved companies.

Minimization of Data Revelation. Naturally, previously introduced multi-hop features raise privacy issues for the involved companies as their business relationships and secrets might be revealed. Hence, an important aspect is to create a balance for the trade-off between privacy concerns and the required transparency. While merely providing all data to all companies by default is not an option due to its sensitive nature, sticking to today's environment with limited data exchange prevents the named multi-hop features. Moreover, the trade-off between privacy and transparency should be adjustable depending on the companies' level of trust and their desired level of collaboration and data exchange.

III. Attribute-Based Encryption

To realize this trade-off, we rely on attribute-based encryption (ABE) as a key building block of our proposed design. This novel form of public-key encryption shifts access control from *who* may decrypt data items to *which properties* or *attributes* are required for legitimate data access [18]. To this end, access policies are defined through formulas, and all entities which are able to satisfy a formula can gain access to encrypted information. Consequentially, in contrast to traditional public-key cryptography, encrypted ciphertexts are not bound to the recipient of information.

For our setting, we use Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which allows linking ciphertexts to a logical formula of attributes [18]. It supports efficient one-to-many applications, even if the recipient is unknown at the time of encryption. A party can only decrypt the ciphertext if it is able to satisfy the linked formula with attributes in its possession. For example, a ciphertext with the policy $A \wedge B$ can only be decrypted if the party has access to both attributes A and B. Even two colluding parties with only attribute A respectively B in their possession cannot decrypt this ciphertext, i.e., entities cannot join their attributes to satisfy additional policies. While attributes are traditionally assigned by a central authority, the control over attributes can also be distributed to multiple authorities, each responsible for a set of attributes without a central coordinator [19].

ABE has diverse use cases. For example, it is suitable for broadcast encryption [18], has been proposed for cloud storage [20], or mobile cloud computing [21]. Other areas of application include access control in general, but more sophisticated privacy protection in social networks [22]. Similarly, ABE has been proposed for an application in smart health to address potential data security concerns [23]. Overall, research tailored ABE to diverse areas. However, due to its limited performance, most designs using ABE are targeted to a specific use case.

IV. Design Goals

Based on our analysis of related work and the desired accountability features, we identify six distinct design goals to privacy-preservingly support dynamic supply chain settings.

G1: Accountability. To implement a trustworthy system that records (all) interactions of supply chains, our design must offer a persistent and tamperproof solution for all parties. Furthermore, the desired accountability features (cf. Section II-B) have to be integrated while hampering manipulations or the spreading of misinformation to improve its reliability.

G2: Verifiability. As the recorded interactions are only valuable if the made claims are verifiable, our system must support this aspect as well. In particular, we do not only want to detect manipulations, but also identify cheating or misbehaving parties to allow for reparations. Such information could further help to implement a reliable reputation system.

G3: Privacy Preservation. As industry settings pose different requirements on privacy than consumer settings, we have to ensure that (sensitive) business secrets remain private whenever possible. This goal opposes **G1** and **G2**, however, it is essential for real-world applicability as companies are cautious when sharing data with (potentially untrusted) parties.

G4: Security. We have to establish a trustworthy system in the face of mutually distrusting parties. Consequentially, we have to provide (fine-granular) access control to prevent data leakage to unintended parties. Information about products and the supply chain should only be available for involved companies. Still, we cannot eliminate malicious insiders either.

G5: Scalability. To make the system usable in the real world, it must scale to (tomorrow's) industry needs. We must support a significant number of records without introducing excessive load at participating companies. This goal is not limited to processing overhead, but also takes storage requirements and availability needs (whether a party must interact within a specific time frame) into account.

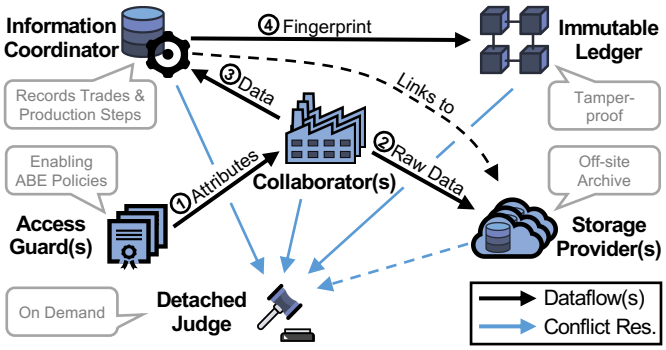

Fig. 1. Our architecture operates as follows. Collaborators retrieve attributes from Access Guards that maintain suitable ABE policies. A dedicated storage provider retains all raw data while a bundle containing a link to the raw data is sent to the information coordinator to securely record all produce and trade operations. A fingerprint of this record is stored on the immutable ledger. In case of inconsistencies, a detached judge can resolve conflicts.

G6: Autonomy. Finally, we have to make sure that companies do not have to interact with our system except when they record their own actions, as significant needs for interaction with humans and collaborating companies hinder real-world applicability. This autonomy is especially interesting regarding accountability features offered by our system as similar (supported) queries are missing in traditional supply chains.

These goals, which set functional requirements and affect the properties of the running system, will guide us through our design for multi-hop accountability in supply chains.

V. A Novel Supply Chain Architecture Enabling Secure Multi-Hop Accountability

To realize an architecture that enables secure multi-hop accountability, we leverage that every supply chain can be represented by a Directed Acyclic Graph (DAG), i.e., each part or component is "consumed" to create a newly assembled (sub-)product. The initiating contractor here constitutes the single root of the DAG, and each processing or transportation step is an edge between the contractor and its suppliers.

Building Blocks. Our design relies on three technologies: (i) *AES* to securely encrypt sensitive information, (ii) *attribute-based encryption* to fine-granularly protect AES keys with a many-to-many encryption scheme, and (iii) a *blockchain* to reliably record all actions persistently in a distributed way.

A. Design Overview

In our design, we support two different actions, (i) a *produce* operation, which combines multiple components into a newly manufactured or assembled part, and (ii) a *trade* operation, which tracks whenever an item is physically handed over to another supplier, the contractor, or a customer. These operations are sufficient to record all actions along a supply chain: Parts are either consumed or they are exchanged between different parties. Our system supports a (verifiable) versioning system to enable an update mechanism for recorded information.

To prevent data leaks, we separate the entity which controls data (*information coordinator*) from the entity managing keys. Therefore, each entity on its own cannot access stored information. We rely on ABE for fine-granular access control for multiple parties. To avoid a single party managing all keys, we use multiple independent *access guards* who each have authority over different ABE attributes. Consequentially, with appropriate ABE policies, multiple independent access guards and the information coordinator would have to collude to gain access to data. We further integrate a blockchain into our architecture to provide accountability and verifiability.

Concretely, our system, which is visualized in Figure 1, operates as follows. In Step ①, access guards enable the collaborators to encrypt their data with an ABE policy (cf. Section III) to preserve privacy. Further, access guards also distribute ABE attributes for (later) decryption to authorized entities only. To cope with significant storage demands, for Step ②, our design incorporates a dedicated, remote, off-chain storage that retains the AES-encrypted raw data. The raw data is referenced by link within the action submitted to the information coordinator (as part of Step ③). The information coordinator handles all collaborator-submitted actions and persists them in its database. Furthermore, in Step ④, a fingerprint of each action is recorded in a tamperproof manner on the immutable ledger. The collaborator submitting the data to the information coordinator has to verify the correctness of this fingerprint. Finally, our design includes an external judge for on-demand conflict resolution. In the following, we describe the different entities of our architecture in more detail.

B. Participants and Operators

Our supply chain environment consists of six logical entities that extend the companies that are part of today's supply chains. This design enables the desired multi-hop accountability features for all companies of existing supply chains.

Collaborators. We refer to participating companies as collaborators, which include both reading and writing parties. Prior to submitting (symmetrically-encrypted) supply chain actions to the information coordinator, they have to encrypt the symmetric key via ABE. Once the information coordinator confirms the reception of information, the collaborators check that the matching fingerprint is recorded on the blockchain.

Information Coordinator. The information coordinator is a central endpoint without access to encrypted data. It is responsible for (i) handling all trade and produce operations in the supply chain, (ii) submitting fingerprints of these to the blockchain, and (iii) serving as an endpoint for queries by collaborators. Thus, it is critical to ensure scalability (**G5**).

Our design is built to identify misbehaving parties among both the collaborators and the information coordinator. Through the records on the immutable ledger, collaborators can prove that they submitted correct data to the information coordinator. Further, collaborators can detect a misbehaving coordinator as it leads to missing or incorrect data on the ledger. Finally, we implement access control at the information coordinator to further fulfill our security design goal (**G4**).

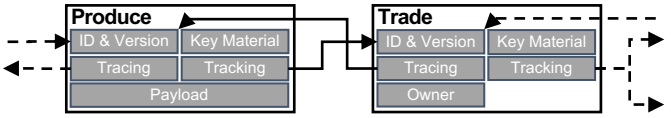

Fig. 2. The record layout of our operations contains (encrypted) tracking and tracing fields that reference other records (double-linked record structure).

Access Guards. We rely on multiple parties to serve as access guards to distribute ABE keys to collaborators. Access guards can be operated by collaborators, but they can also be run by external parties, e.g., trade associations or governments. This design decision prevents a single party from having control over all provisioned keys, as each access guard manages only a subset of ABE attributes. These aspects address the design goal of privacy preservation (**G3**).

Immutable Ledger. To realize accountability (**G1**), a blockchain is jointly maintained by, e.g., the collaborators and optionally independent external surveyors if public transparency is required for a particular supply chain. It stores *fingerprints*, i.e., cryptographic hashes, derived from all actions that were submitted to the information coordinator. The immutable ledger helps to achieve and improve verifiability (**G2**).

Storage Providers. Our architecture supports various external storage providers, e.g., offering cloud storage, to outsource data for future use and verification. This design significantly improves scalability (**G5**). When using external storage, the information provider only receives an encrypted path to the data along with a signature of the data from the collaborator. The collaborator is responsible for choosing a storage with the required availability needs, i.e., if important detailed information is missing, we deem it the data owner's fault.

Detached Judge. Optionally, a judge can be used for conflict resolution, e.g., in situations where information is (i) missing (or unavailable), (ii) (purposely) incorrect, or (iii) not decryptable. Its functionality can be further extended using smart contracts to achieve semi-automation [24]. As using a judge is fully optional, it does not impact autonomy (**G6**).

These six logical entities are sufficient to enable (secure and privacy-preserving) multi-hop accountability in supply chains.

C. Accountable Record Provision, Retrieval, and Updates

To achieve our goal of verifiable multi-hop traceability and trackability in a privacy-preserving and accountable manner, we doubly link all operations as we visualize in Figure 2.

First, a collaborator performs a *produce* operation which also contains *tracing* information, i.e., references to a set of consumed products (records). Both *payload* and *tracing* information can be encrypted via AES to enforce a desired data privacy policy. The key used for encryption is directly included in the record and is encrypted via ABE using a policy that only grants a specific set of collaborators access to it. Our data format further supports selective encryption of nested objects. Finally, the data providing collaborator can specify a policy such that the information coordinator only provides the record to collaborators who satisfy this policy. The combination of object encryption and policy enforcement for data access by

the information coordinator prohibits information disclosure to unauthorized parties redundantly (cf. Section V-D).

Subsequently, the collaborator updates the *tracking* information of records referenced in the *tracing* information of the previous step. As for *tracing*, this information is a set of references to other records. To eventually represent an ownership transfer, a collaborator performs a *trade* operation. Its structure is similar to a *produce* record, however, instead of an arbitrary payload it includes owner information. Again, we also maintain and update the tracing and tracking data.

For each of the previously covered requests, the collaborator generates a fingerprint of the request's parameters and sends it to the information coordinator along with a cryptographic signature over the fingerprint. On reception, the coordinator verifies the signatures and includes the received data in the record to enable later integrity verification. Afterward, it calculates a fingerprint on its own to persist it on the immutable ledger. This proof of existence has to be validated by the collaborator who initially submitted the message. In case of a mismatch, conflict resolution is triggered immediately.

Collaborators can track or trace products and product batches over multiple hops by receiving a *produce* or *trade* record, decrypting its tracking or tracing data, and receiving the referenced records iteratively. Retrieval of multiple records at once enables a faster traversal through the DAG. Due to the included fingerprints, record verification is possible without the involvement of other entities or the immutable ledger.

D. Security Considerations

The security of our approach relies on the security properties of the concepts of AES, ABE, public-key cryptography, and blockchain and their respective implementations in general. Besides that, we only have to assume that key material is not shared with other parties. Specifically, if an uninvolved party receives correct keys from a party with legitimate access, the corresponding information is decryptable. However, this uninvolved party first has to receive the encrypted data from the information coordinator, which is prevented through the enforcement of access control. In the following, we discuss three frequent security aspects in more detail.

Key Leakage. For the encryption of sensitive data, we rely on AES, where ABE protects the corresponding key, i.e., we do not encrypt the key individually for each recipient. This design choice not only reduces overhead, but it also ensures that single collaborators cannot be excluded from access to data (if they satisfy the ABE policy). Given that ABE attributes are bound to individual collaborators, collusion of random parties (each with a subset of attributes) will not lead to elevated access either. In general, all access guards should enforce a previously defined access control. Regardless, we further intend to define ABE policies in a way that attributes issued by n different access guards are required, i.e., no single party is responsible for all attributes. In this case, access to sensitive information is only possible if at least n access guards and the information coordinator collude. Consequentially, illegitimate data access is highly unlikely.

Misbehavior. Overall, we designed our architecture in a way that we are always able to identify misbehaving parties. Consequentially, misbehavior will also result in negative consequences, such as a loss of reputation, financial punishment, or juristic sentencing. As such, we believe that misbehavior is unlikely to occur. Still, we identify two primary threats. First, the information coordinator could misbehave, cease to respond to queries, or delete all information. Such denial of service or any deviation from the regular protocol is easily detectable. As a countermeasure, a redundant architecture could mirror all information over multiple information coordinators. Forcing collaborators to also write the fingerprint to the blockchain can help to achieve public verifiability that (i) an action took place, and (ii) both parties, i.e., collaborator and information coordinator, processed the same data.

Second, collaborators could manipulate their submitted (encrypted) information. While such manipulations might remain undetected for a long time (if records are not decrypted beforehand), the digital signature stored on the immutable ledger proves that the respective collaborator originally submitted the information. Consequentially, the responsible party can be identified (even after long periods). Besides, if data (for verification) at a storage provider is missing, we hold the data owner, i.e., the collaborator, responsible by design.

Data Control. As in most architectures, we cannot exercise control over (decrypted) data. However, through logs kept at the information coordinator, the responsible collaborator (or at least a set of responsible collaborators) for leaking the sensitive data is identifiable. Finally, we leave the integration of ABE attribute revocation for future work. Here, time-interval attributes could serve as a potential solution [25].

VI. Large-Scale Evaluation

To analyze the performance (addressing **G5**) of our design at large, we prototypically implemented our novel architecture. As a foundation for our evaluation, we first introduce our setup (Section VI-A) before presenting our covered real-world scenario (Section VI-B). We then report on the large-scale evaluation of our prototype implementation (Section VI-C).

A. Implementation and Experimental Setup

Our Python-based prototypes for collaborators, information coordinator and access guards make use of Charm [26] for ABE and AES. While MongoDB [27] serves as the database for the information coordinator, our immutable ledger is a Quorum [28] setup, which supports several hundreds transactions per second [29]. We sign all fingerprints and queries with eth-account [30]. For our evaluation, we utilized a single server (2x Intel XeonSilver 4116 and 196 GB RAM). We include the standard deviation over 20 runs for our measurements.

B. Supply Chain Scenario

We analyze the supply chain of a fine blanking production to model a realistic setting for our evaluation. A single processing step to produce a fine-blanked part consists of the following individual steps: supplied metal, operation of the different

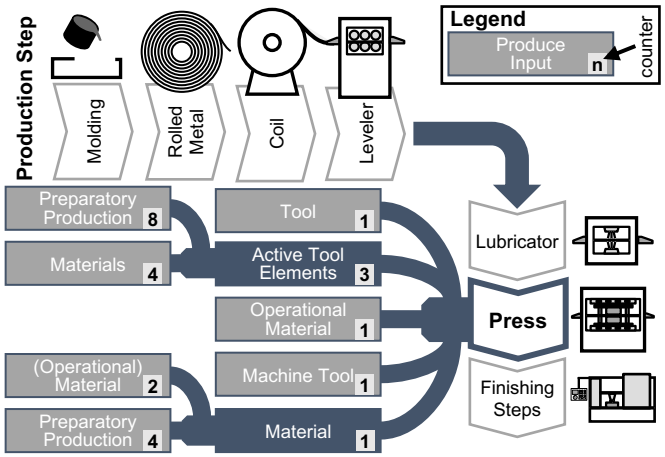

Fig. 3. Visualized excerpt of a fine blanking supply chain highlighting the number of branches for the press step of the production process. All other (production) steps (grayed out) would showcase similar branching behavior.

parts of the fine blanking line (i.e., coil, leveler, lubricator, and press) [31] and several grinding, cutting and hardening operations. Each of these steps has operating resources, tools, and a (machine) supplier, whose individual supply chains need to be taken into account. Traditionally, some steps of the production processes are done by the fine blanking manufacturer itself. Still, with upcoming concepts such as Manufacturing-as-a-Service [3], future needs for supply chain transparency might require the separation of all of these steps. However, even if all steps of the fine blanking process and its secondary finishing processes are categorized as a single supply chain step, it has multiple inputs with several preprocessing steps (e.g., molding and rolling) and subsequent assembly steps.

We extend this real-world scenario already involving a high number of companies by adding a final product that combines 100 fine blanked parts. This number is realistic, e.g., for a medium-sized automobile. In our scenario, each fine-blanked part originates from an individual supply chain, i.e., we already simulate a highly dynamic supply chain. Thus, the resulting scenario represents a realistic (future) supply chain structure in terms of branching, depth, and total production steps.

C. Performance Measurements

Based on this real-world scenario, we derived a tree (i.e., a special form of a DAG) with nodes representing the different processing steps. For the fine blanking line, we added two full binary trees of depth 10 as dependencies. With our *final product* consisting of 100 fine-blanked parts, we end up with a total of 410 001 nodes and 410 000 edges.

Produce, Trade, and Record Updates. First, we evaluate the performance of individual *produce* and *trade* operations, and record *updates*. We include an *encrypted produce* payload of ∼1 KiB and sign each operation according to our specification (cf. Section V-C). We omit transaction confirmation times as transactions are executed batchwise, and we address the blockchain performance in a dedicated analysis.

Our measurements of the DAG construction show that a single *produce* operation takes 46.85 ms ± 14.76 ms. Similarly, a single *trade* operation is executed in 45.92 ms±12.78 ms. For

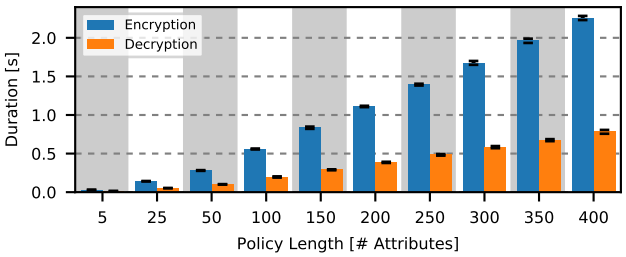

Fig. 4. Even for policies with 400 ABE attributes (e.g., 400 different access classes), the processing of 1 KiB-sized AES payloads takes only about 2 s. Shorter policies (with fewer classes) result in even shorter processing times.

both operations, encrypting the payload takes more than 70 % of the time, while the information coordinator's average runtime does not exceed 4.5 ms. The time for a single *update*, i.e., providing tracking information, averages at 12.53 ms ± 5.49 ms During our measurements, neither the information coordinator nor the underlying database operated at maximum capacity.

Tracing and Tracking. Now, we analyze the performance for *tracing* and *tracking* a product in our exemplary supply chain structure. To this end, we performed a complete trace originating from the *final product*, resulting in 204 800 individual product flow paths consisting of 820 001 *produce* and *trade* records. Here, a single process runs only 2:28 min ± 5 s on unencrypted data as the runtime is driven by the cryptographic operations on the client. However, given that the task is embarrassingly parallel, we can achieve a nearly linear speedup. For example, 30 client processes complete the tracing on encrypted data in 20:57 min ± 21 s, with still more than 80 % of the time spent for decryption. Alternatively, collaborators could only encrypt payloads and not the tracing data itself to reduce the complexity. Regardless, performing such a complete trace is a rare event as it is only of interest in exceptional cases, e.g., for the in-depth investigation of a severe car or plane crash.

To reduce the load on the information coordinator, we allow bundling requests for up to 500 records and end up with 213 917 ± 10 891 issued requests, i.e., one query for 3.83 records. Per second, 649.11 ± 5.43 records are retrieved on average. If we reuse AES keys along the supply chain, we can easily reduce the runtime by 25 % to 15:02 min ± 10 s. In contrast, tracking an initial resource to the final product took 35 requests in 1.14 s ± 43 ms using a single process.

As only the client performs the (parallelizable) cryptographic operations, the architecture's scalability is not affected negatively and can easily scale to the target setting.

Attribute-based Encryption. As each included ABE attribute increases the cryptographic complexity, we evaluate the feasibility and performance of attribute-based encryption by considering the policy length. In Figure 4, we visualize the cryptographic overhead for payloads of 1 KiB. We construct the policies as conjunction over the given number of attributes, and the results emphasize that the policy length in terms of attributes required, influences the operation's time linearly. The AES overhead further correlates linearly with the payload size [32]. Finally, decryption outperforms the corresponding encryption rocess. In principle, each attribute can be assigned to a single supplier within the supply chain. In our setting,

we expect that no constructed policy contains more than 20 attributes. However, in practice, a grouping of suppliers to a single attribute is more likely. Given that the collaborator decides over the policy, the trade-off between granular access control and performance can be set individually. Altogether, we conclude that carefully designed ABE policies and the possibility to reuse calculated keys offer satisfying performance.

Immutable Ledger. Since the transaction throughput of Quorum has been proven to exceed 2000 transactions/s [29], we focus on storage overhead of transactions. A single transaction covers a record ID and a fingerprint. Further, it includes versioning information and the collaborator's address. The raw transaction size adds up to 265 B, while the block overhead is 590 B for a single transaction. This overhead only increases minimally for multiple transactions. Due to the tunable block-time in Quorum [28], overhead can be reduced at the cost of increased transaction latency. For our scenario with more than 1.6 million requests, we end up with a total transaction size of 414.45 MiB for the final product and all its 100 disjoint supply chains to achieve multi-hop accountability. This size is a reasonable overhead for one or multiple batched medium-sized automobiles. We designed the transactions to not require coordination between collaborators and the information coordinator and to enable simple verification. Transaction sizes can be reduced by 50 % at the cost of increased verification complexity by omitting fingerprints for tracking updates as this information is part of the tracing data.

VII. Conclusion and Future Work

To satisfy tomorrow's accountability needs in dynamic supply chain environments, we proposed a novel blockchain-backed architecture utilizing attribute-based encryption (ABE). Our design tackles the trade-off between privacy and transparency in settings with cross-company information flows by introducing an oblivious coordinator that records and stores the actions of all parties. These records enable multi-hop tracking and tracing by individual entities, while access to data is protected by fine-granular policies and targeted encryption.

We evaluated a realistic supply chain scenario to yield first insights into our design's performance. For future work, we plan to generalize our evaluation by modeling complex real-world supply chains to verify our drawn conclusions. Furthermore, we envision several different extensions to our architecture. For example, for settings, such as food chains, we could implement (governmental) oversight or public verifiability through appropriate ABE policies. ABE attributes could also be sold to interested parties to obtain access to (sensitive) information, effectively establishing a data market. Finally, a reputation and rating system could improve the dynamic selection of suppliers in interconnected environments.

All these improvements increase the trust in (global) supply chains as more aspects are verifiable and reliable. Consequentially, they foster new dynamic business relationships. Furthermore, they might support new market participants in bootstrapping their business as all (desired) accountability needs are satisfied by the deployed supply chain architecture.

Acknowledgments

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – 390621612.

References

[1] B. B. Flynn *et al.*, "The impact of supply chain integration on performance: A contingency and configuration approach," *Journal of operations management*, vol. 28, no. 1, 2010.
[2] J. Pennekamp *et al.*, "Towards an Infrastructure Enabling the Internet of Production," in *IEEE ICPS*, 2019.
[3] J. Pennekamp *et al.*, "Dataflow Challenges in an *Internet* of Production: A Security & Privacy Perspective," in *ACM CPS-SPC*, 2019.
[4] J. Pennekamp *et al.*, "Security Considerations for Collaborations in an Industrial IoT-based Lab of Labs," in *IEEE GCIoT*, 2019.
[5] V. Dedeoglu *et al.*, "A journey in applying blockchain for cyberphysical systems," in *COMSNETS*, 2020.
[6] T. M. Simatupang and R. Sridharan, "The Collaborative Supply Chain," *The International Journal of Logistics Management*, vol. 13, no. 1, 2002.
[7] T. Moyaux *et al.*, "Information Sharing as a Coordination Mechanism for Reducing the Bullwhip Effect in a Supply Chain," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 3, 2007.
[8] D. M. Lambert *et al.*, "Building successful logistics partnerships," *Journal of Business Logistics*, vol. 20, no. 1, 1999.
[9] M. Attaran and S. Attaran, "Collaborative supply chain management: the most promising practice for building efficient and sustainable supply chains," *Business Process Management Journal*, vol. 13, no. 3, 2007.
[10] K. Korpela *et al.*, "Digital Supply Chain Transformation toward Blockchain Integration," in *HICSS*, 2017.
[11] N. Hackius and M. Petersen, "Blockchain in Logistics and Supply Chain: Trick or Treat?" in *HICL*, 2017.
[12] K. Wüst and A. Gervais, "Do you need a Blockchain?" in *CVCBT*, 2018.
[13] S. Malik *et al.*, "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains," in *IEEE NCA*, 2018.
[14] S. Malik *et al.*, "TrustChain: Trust Management in Blockchain and IoT supported Supply Chains," in *IEEE Blockchain*, 2019.
[15] S. A. Abeyratne and R. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 5, no. 9, 2016.
[16] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, 2018.
[17] M. Westerkamp *et al.*, "Blockchain-Based Supply Chain Traceability: Token Recipes Model Manufacturing Processes," in *Blockchain*, 2018.
[18] J. Bethencourt *et al.*, "Ciphertext-Policy Attribute-Based Encryption," in *IEEE S&P*, 2007.
[19] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in *EUROCRYPT*, 2011.
[20] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," in *FC*, 2010.
[21] A. N. Khan *et al.*, "Towards secure mobile cloud computing: A survey," *Future Generation Computer Systems*, vol. 29, no. 5, 2013.
[22] S. Jahid *et al.*, "EASiER: Encryption-based access control in social networks with efficient revocation," in *ACM ASIACCS*, 2011.
[23] Y. Zhang *et al.*, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," *IEEE IoTJ*, vol. 5, no. 3, 2018.
[24] L. Bader *et al.*, "Smart Contract-Based Car Insurance Policies," in *GC Wkshps*, 2018.
[25] S. Ma *et al.*, "Adaptable key-policy attribute-based encryption with time interval," *Soft Computing*, vol. 21, no. 20, 2017.
[26] J. A. Akinyele *et al.*, "Charm: a framework for rapidly prototyping cryptosystems," *JCEN*, vol. 3, no. 2, 2013.
[27] MongoDB Inc., "MongoDB," https://www.mongodb.com, 2009.
[28] JP Morgan, "Quorum," https://www.goquorum.com/, 2016.
[29] A. Baliga *et al.*, "Performance Evaluation of the Quorum Blockchain Platform," 2018.
[30] Ethereum – GitHub, "eth-account," https://github.com/ethereum/eth-account/, 2018.
[31] R. Glebke *et al.*, "A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems," in *HICSS*, 2019.
[32] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*. Springer, 2007.