

Scalable and Privacy-Focused Company-Centric Supply Chain Management

Eric Wagner^{*,†}, Roman Matzutt[†], Jan Pennekamp[†], Lennart Bader^{*},
Irakli Bajelidze[†], Klaus Wehrle^{†,*,} and Martin Henze^{‡,*}

^{*}*Cyber Analysis & Defense, Fraunhofer FKIE · {firstname.lastname}@fkie.fraunhofer.de*

[†]*Communication and Distributed Systems, RWTH Aachen University · {lastname}@comsys.rwth-aachen.de*

[‡]*Security and Privacy in Industrial Cooperation, RWTH Aachen University · henze@cs.rwth-aachen.de*

Abstract—Blockchain technology promises to overcome trust and privacy concerns inherent to centralized information sharing. However, current decentralized supply chain management systems do either not meet privacy and scalability requirements or require a trustworthy consortium, which is challenging for increasingly dynamic supply chains with constantly changing participants. In this paper, we propose CCChain, a scalable and privacy-aware supply chain management system that stores all information locally to give companies complete sovereignty over who accesses their data. Still, tamper protection of all data through a permissionless blockchain enables on-demand tracking and tracing of products as well as reliable information sharing while affording the detection of data inconsistencies. Our evaluation confirms that CCChain offers superior scalability in comparison to alternatives while also enabling near real-time tracking and tracing for many, less complex products.

Index Terms—supply chain management; blockchain; permissionless; deployment; tracing and tracking; privacy

I. INTRODUCTION

In 2012, the Food Safety Authority of Ireland detected significant unlabeled traces of horse meat DNA in food products [1]. What became known as the Horsemeat Scandal resulted in a lasting reduction of sales numbers and customer trust [1]. Reliable information sharing can preemptively detect issues and their underlying cause leading to such events within food and manufacturing supply chains [2]. Even during normal operation, such information sharing enables *e.g.*, the anticipation of bottlenecks in supply and demand [3] or the sharing of product-specific information for further processing [4] and with end-customers [5]. However, supply chain management (SCM) systems with the capability for such reliable information sharing are still not in widespread use, mostly due to trust and privacy concerns [2].

Consequently, recent research efforts focus on realizing decentralized SCM systems that alleviate trust and privacy issues inherent to centralized information management [6]. Lately, these efforts have concentrated on using blockchain technology as promising backbone for such decentralized SCM architectures. The resulting proposals for SCM can be broadly grouped into two categories: (i) systems built on top of *permissionless* blockchains [7]–[11], which address trust but not privacy concerns and suffer from scalability issues, and (ii) systems realized on top of *permissioned* blockchains [5].

Author manuscript.

[12]–[16], which require massive planning among collaborators to establish a trusted consortium to operate the blockchain.

While some prototypical or even production-ready decentralized SCM systems are already deployed, those deployments are restricted to small-scale operation with only a select few partners [2]. In practice, we identify two major concerns arising from these architectures. First, large numbers of (international) collaborators make it exponentially harder to establish a consortium trusted by collaborators and customers. More importantly, related work mostly ignores the dynamics of entities seamlessly joining and leaving a SCM system. This oversight is particularly limiting when SCM systems incrementally grow their user base as they gain popularity.

In this paper, we propose CCChain as an incrementally deployable, scalable, and privacy-aware SCM system. CC-Chain gives each company control over its own data and by default hides data from externals. Notably, the integrity of locally stored data is still ensured by regularly publishing a cryptographic witness over all recent events to a public ledger. Thus, no data can be retrospectively altered. Whenever an external entity needs access to particular information, *e.g.*, to identify the reason for a faulty product, exactly the information relevant to the product’s manufacturing steps can be shared, without providing access to any additional data.

II. SUPPLY CHAIN MANAGEMENT SYSTEMS

Although information sharing along supply chains offers manifold benefits [3]–[5], [17], companies are still hesitant to engage in such efforts due to privacy and trust concerns [2], [17]–[20]. Meanwhile, data authenticity and privacy in scalable SCM systems is still challenging [2], [21], as centralized solutions lead to information asymmetry that primarily benefits the powerful entities in the supply chain [14]. Here, blockchain technology shows major potential to improve the status quo by realizing decentralized SCM that mitigates many of the concerns of centralized deployments. In the following, we outline still open challenges of SCM that surface when either relying on permissionless or permissioned blockchains.

Permissionless Blockchain-based SCM. Publicly available permissionless blockchains (*e.g.*, Ethereum [22]) provide a ready-to-use trusted infrastructure that offers significant advantages for SCM systems over centralized and/or dedi-

cated alternatives. Initially, such systems only stored integrity-protected information for individual products [7], [8], before several proposals tokenized not only final products but also intermediate products to enable the tracing of a product's entire manufacturing process over multiple hops [9]–[11]. These approaches link physical goods to a unique digital representation (*e.g.*, via RFID chips), which is immutably stored on the blockchain. This digital representation is then enriched with information as the product traverses the supply chain. Although permissionless blockchains offer a high level of trust, they also suffer from scalability and privacy issues, as storing data becomes costly and all transactions are public.

Permissioned Blockchain-based SCM. Scalability and privacy issues of permissionless blockchains can partially be mitigated by permissioned blockchains, *i.e.*, blockchains operated by a set of authenticated users. Utilizing such a dedicated blockchain for the information sharing along a supply chain promises faster and better scaling networks [5], [12]–[16]. While such fragmentation limits the interoperability across supply chains and dynamic partnerships, they promise to solve privacy and scalability issues. In permissioned systems, privacy can be achieved by segmenting information and encrypting each part separately, *e.g.*, via attribute-based encryption [12], [13]. Combined with an entity that enforces access control [12]–[14], data availability and privacy concerns can be further improved. Still, it remains challenging for SCM systems based on permissioned blockchains to define and achieve transparency and being flexible w.r.t. participating companies, *i.e.*, the joining and leaving of companies.

III. CCCHAIN: A DEPLOYABLE SCM SYSTEM

Current SCM systems are either not scalable and privacy-preserving or are designed for a static setup of entities that comprise a single supply chain. The lack of support for incremental deployability of scalable systems, which is necessary for today's dynamic economy, thus limits current systems' applicability in the real world. Therefore, we present our novel **Company-Centric supply Chain** management system that addresses these limitations. CCChain orients itself on designs built on permissionless blockchains while heavily restricting the amount of published data to ensure scalability and privacy. In the following, we present CCChain's architecture in detail.

A. Immutable and Traceable Data Records

We first describe how CCChain represents the supply chain's production graph with data records that are stored locally by the entity responsible for the respective production step. Data records represent actions that describe transformations or ownership transfers of the referenced products. Hence, the gradual transformation and transfer of raw materials to the final product via actions form the final production graph. As we show in Figure 1, every action consists of a unique *action identifier* (a hash value computed over all its fields), an *action type*, and a *timestamp*. Additionally, actions reference (potentially multiple) *product identifiers* as inputs and *product records* as outputs, depending on the action type.

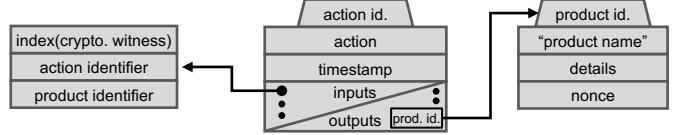


Fig. 1. CCChain maintains product records with a set of actions, and links them such that fine-granular data access to individual products is possible.

Similarly, product records have a unique *product identifier* (the hash value over all of its fields), and they contain a descriptive *product name*, a list of related *details* such as produced quantities, and a *nonce*. Crucially, actions only indicate the identifier of output product records to protect the confidentiality of non-relevant information when publishing an action. Furthermore, the nonce prevents outsiders from guessing product records. In contrast, an input product is represented by a reference to a previous output product. Each output product can only be consumed once, which has to be respected by companies since any misbehavior is retrospectively detectable during product tracing or third-party audits.

In total, CCChain supports six action types. First, companies can *create* new products that do not require previous inputs, *e.g.*, gaining resources from excavation. A company can further *produce* a product by consuming one or multiple input products. Next, one company can *export* products, which other companies then can *import* to represent an ownership transfer (cf. Section III-C). Correspondingly, companies can *buy* or *sell* components or products to external parties, *i.e.*, trade partners that still fail to support CCChain. Overall, these six action types can represent a product's full life cycle along the supply chain, enriched with supplementary collected data.

B. Ensuring the Correctness of Locally Stored Information

CCChain ensures the confidentiality of their product records by only storing them locally by default. However, CCChain has to ensure the integrity and consistency of product records to prevent fraud and to add value over existing SCM systems. Thus, these records must be immutable once they are referenced by an action. We consider potential problems stemming from generating fraudulent product records orthogonal to our work; corresponding approaches engulf, for instance, tamper-resistant sensor [21], [23], regular consistency checks [24], or detailed (lab) analyses of random product samples [25]. CCChain can easily integrate corresponding advancements and, conversely, also improve related auditing processes: For example, through the management of access rights to a company's product records, auditors can gain retroactive data access such that potential misbehavior is always detectable.

To ensure that locally stored data records cannot be altered, companies are required to periodically (*e.g.*, once a day) upload a *cryptographic witness* covering all recent products and actions to a permissionless blockchain. These witnesses consist of the Merkle roots obtained from the Merkle tree [26] over all actions generated by one company within the last period. Only after a witness is published, *i.e.*, being immutable, can other companies rely on its information. The existence of an action is then validated via exchanged Merkle proofs.

C. Transferring Products Across Company Borders

The *export* and *import* actions are unique as they connect the production graphs across two companies. These actions always occur in pairs (*cf.* Section III-C), yet, fraudulent and incorrect data must always be attributable to a single entity.

Ideally, companies create and share their export actions right before shipping goods to the receiving company and prove they have been recorded on the blockchain. This way, the receiving company learns a verifiable and retroactively publishable claim that the goods have been shipped, and it can create and publish the corresponding import action when receiving the goods. Hence, both trading companies agree that the shipment has concluded successfully and that the respective actions are properly persisted for later audits. However, this protocol enables malicious companies to misbehave, motivating a fallback protocol to resolve potential disputes.

If the exporting company receives no corresponding import action within a reasonable time, it files a complaint on the blockchain. The complaint includes identifiers of the blinded importing company, the affected products, and an indicator of whether the export action should be retracted entirely, *e.g.*, in case of problems with the shipping process, or converted into a sell action because goods were received but not registered in CCChain. The blinding is based on a secret previously established between both companies to protect the accused company's privacy during the dispute resolution.

After recognizing a complaint, the accused company has two options. First, it can choose not to respond, which we interpret as an agreement to the accusation and to reverting the previous export operation. In this case, the exporting company can overwrite the export action by consuming the corresponding product identifiers twice. Second, the accused company can publish a *Merkle proof* showing that the company previously published an import action that matches the accusing company's export action, *i.e.*, the complaint was unwarranted. If a product is shipped without a published or transmitted export action, the importing company can employ a similar protocol: It first announces the (blinded) company identifier and the relevant product identifiers. Without any response, it uses a buy action instead of an import action even if both parties use CCChain. If further questioned, the company can refer to the unanswered complaint on the blockchain. Otherwise, the exporting company publishes the proof of the export action to resolve the dispute. Consequently, both companies involved in a product transfer always own a shareable proof (for future use) about the existence of the counterpart of their respective import or export action.

D. Tracing and Tracking Product Lifecycles with CCChain

As companies and end-customers increasingly care about products' sustainable, ethical, and conflict-free sourcing and manufacturing [27]–[29], a critical feature of modern SCM systems is the ability to perform multi-hop tracking and tracing [30]. The tracking and tracing functionality in CCChain is an interactive process, where each company can decide on a case-by-case basis if it wants to share the requested

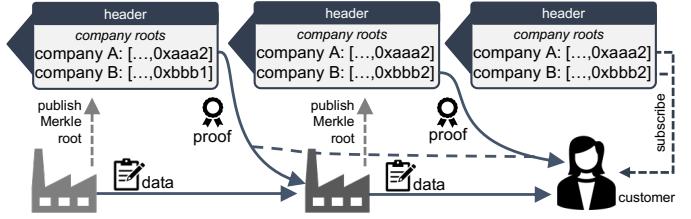


Fig. 2. In CCChain, the basic tracing and tracking operation works by iteratively requesting product-related information from its creator. This process ensures companies keep the sovereignty of their data.

information. While information can be technically withheld, without a valid reason such an approach damages a company's reputation. Similarly, companies can be required by law to share their data with regulators, for which the legal frameworks are currently extended, *by e.g.*, the German *Act on Corporate Due Diligence in Supply Chains* from 2021 [31].

Figure 2 illustrates the data retrieval process for an end-customer tracing a product in CCChain. The customer first has to retrieve the relevant companies' Merkle roots from the public blockchain. Then, a product's tracing information can be requested in an iterative manner, starting from the entity the product was brought from. The company from the supply chain can answer these requests with product-related information and the Merkle proof verifying its authenticity. By iteratively tracing a product back to its raw materials, its sources and entire lifecycle can thus be verified, while the protocol presented in Section III-C ensures that the correct supply chain predecessors are shared with the customer.

While the need for entities to remain responsive could be considered a drawback, we argue that CCChain's dynamic data access significantly outweighs this aspect, as companies never lose control over their data. In the end, we believe that this additional control over one's data is crucial for any SCM system to be accepted by a large community.

IV. PERFORMANCE EVALUATION

We have introduced CCChain as an incrementally deployable supply chain management system by design and discussed its security guarantees. In the following, we underline CCChain's excellent performance and scalability.

Experimental Setup. Our Go-based prototypical implementation covers all relevant entities and relies on MongoDB as a database. We further realize the event-based smart contract in Solidity and interface via geth with a local Ethereum instance. We run our evaluation on a single server (Intel Xeon Silver 4116 CPU, 196 GB of RAM) by deploying all entities in individual docker containers, with each container having access to a single core.

A. CCChain's Low Local Processing and Storage Overheads

Before discussing the performance on a global scale, we report on the low processing and storage overhead for a company that utilizes CCChain. Looking at CCChain's performance in terms of processed actions per second, we observe that the create and buy actions can be handled at an average rate of 79 and 61 thousand actions per second, respectively. The

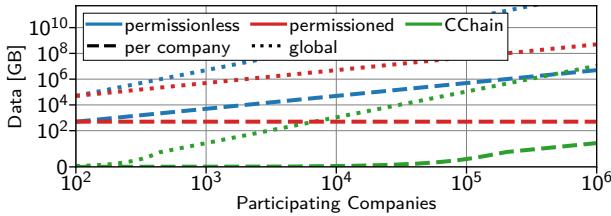


Fig. 3. CCChain is even more efficient in terms of data storage requirements than SCM systems built on top of private blockchains.

sell and produce actions, on the other hand, require a backward reference to the input products but still achieve a more than sufficient throughput of 1.6 and 1.4 thousand actions per second. As expected, the export and import actions achieve the least throughput at 240 actions per second, each. This reduced performance follows from the need to generate and verify Merkle trees, as well as the required interactions between two CCChain instances. Assuming an equal distribution of action types, with each action only carrying 200 B of data, CCChain achieves a per-company throughput of over 35 Mbit/s. Consequently, even our prototypical CCChain client demonstrates excellent performance on a company level.

B. Operational Cost of a CCChain Deployment

Besides the local CCChain client, additional costs arise from CCChain’s interaction with a public blockchain. On March 3, 2022, the recommended gas costs [32] for a Merkle root upload thus equals 0.0011 ETH or 3.18 USD. For larger businesses, the resulting annual price constitutes 1160.7 USD. Consequently, these funds are manageable even with high transaction costs, as currently observed in Ethereum. Alternatively, multiple companies could also register as a group and combine their individual Merkle roots, thereby sharing the cost of a single upload. With a threshold cryptography scheme for account management, such an approach does not impair their individual privacy. Overall, the fair operational costs of CCChain are easily manageable by most businesses, making its design optimal to achieve widespread real-world adoption.

C. Scalability Analysis of CCChain

To look at CCChain’s scalability of an entire supply chain, we now compare CCChain to abstract SCM systems that either operate fully on a permissionless or on a permissioned blockchain. In the permissionless setting, we assume that all information is stored on a public ledger and thus a copy of all data must be stored by each entity. In the permissioned setting, we expect that entities only store a copy of the blockchains corresponding to supply chains they are directly involved in. In our context, we make a conservative estimate that each company is part of supply chains with 100 collaborators.

For comparability, we assume that each entity using the network stores one 200 B action per second, which corresponds to 5.9 GB of annual data per entity. Figure 3 illustrates how the compulsory inclusion of this data in the different decentralized SCM architectures affects the required storage as the number of participating companies grows. On a per-company level, we notice that a permissioned architecture

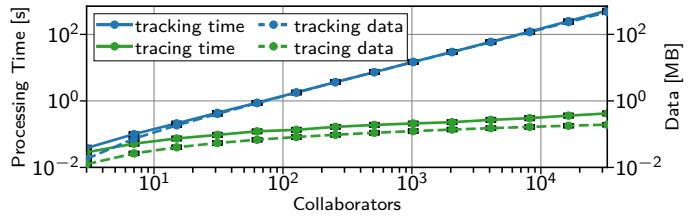


Fig. 4. CCChain allows the quick tracking and tracing of even complex products composed over thousands of manufacturing steps.

adds constant overhead to each company, given that the companies only store data from their (multi-hop) collaborators. Even worse, permissionless architectures handle exponentially growing amounts of data as every company’s data is stored. In contrast, CCChain introduces little overhead, and only in scenarios with vast numbers of participating companies, the overhead grows as the Merkle Roots of all participants must be stored. Thus, CCChain’s good scalability even allows smaller businesses to join without fearing a high financial burden.

D. Tracking and Tracing Performance in CCChain

Finally, we look at the tracking and tracing performance (*cf.* [13]). For these measurements, we consider a binary production graph where at each non-leaf node, a new (intermediate) product is manufactured by a unique company and by consuming two previous products. In Figure 4, we report on the time and network traffic to track and trace products for an increasing number of entities. We refrain from applying additional network latency as many of the requests can be parallelized. As expected, tracing produces more overhead as it requires the revelation of the entire production graph, whereas tracking only reveals one path from one node up to the final product. We observe a similar trend in the amount of exchanged data for the requests, information sharing, and authenticity proofs. In our setting, CCChain thus traces products with 64 or less manufacturing steps in less than 1 s, while exchanging less than 1 MB of data. Hence, CCChain could even be used to request verified provenance information in real-time while shopping for food in a supermarket.

V. CONCLUSION

Information sharing along the supply chain tackles the anticipation of issues and answers the customers’ and regulators’ demands for proof of the sustainable, ethical, and conflict-free sourcing and manufacturing of products. Blockchain technology now gives rise to the opportunity of designing decentralized alternatives that mitigate trust and privacy concerns of centralized systems. However, current decentralized SCM systems lack flexibility and scalability. We addressed this issue by proposing CCChain as an alternative system: CCChain supports dynamic and fine-granular data access policies, which, coupled with its scalability and incrementally deployability to support organic growth, make it an attractive alternative for today’s sophisticated and ever-changing SCM.

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

REFERENCES

- [1] L. Agnoli, R. Capitello, M. De Salvo, A. Longo, and M. Boeri, "Food fraud and consumers' choices in the wake of the horsemeat scandal," *British Food Journal*, vol. 118, no. 8, pp. 1898–1913, 2016.
- [2] P. Gonczol, P. Katsikouli, L. Herskind, and N. Dragoni, "Blockchain Implementations and Use Cases for Supply Chains-A Survey," *IEEE Access*, vol. 8, pp. 11 856–11 871, 2020.
- [3] P. Fiala, "Information sharing in supply chains," *Omega*, vol. 33, no. 5, pp. 419–423, 2005.
- [4] B. B. Flynn, B. Huo, and X. Zhao, "The impact of supply chain integration on performance: A contingency and configuration approach," *Journal of Operations Management*, vol. 28, no. 1, pp. 58–71, 2010.
- [5] S. Malik, S. S. Kanhere, and R. Jurdak, "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains," in *Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA '18)*. IEEE, 2018.
- [6] S. van Engelenburg, M. Janssen, and B. Klievink, "A Blockchain Architecture for Reducing the Bullwhip Effect," in *Proceedings of the 8th International Symposium on Business Modeling and Software Design (BMSD '18)*, vol. 319. Springer, 2018, pp. 69–82.
- [7] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM '16)*. IEEE, 2016.
- [8] 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, pp. 18–27, 2018.
- [9] M. Westerkamp, F. Victor, and A. Küpper, "Blockchain-Based Supply Chain Traceability: Token Recipes Model Manufacturing Processes," in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1595–1602, Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain '18).
- [10] S. Wang, D. Li, Y. Zhang, and J. Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario," *IEEE Access*, vol. 7, pp. 115 122–115 133, 2019.
- [11] M. Westerkamp, F. Victor, and A. Küpper, "Tracing manufacturing processes using blockchain-based token compositions," *Digital Communications and Networks*, vol. 6, no. 2, pp. 167–176, 2020.
- [12] J. Pennekamp, L. Bader, R. Matzutt, P. Niemietz, D. Trauth, M. Henze, T. Bergs, and K. Wehrle, "Private Multi-Hop Accountability for Supply Chains," in *Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops '20)*. IEEE, 2020, Proceedings of the 1st Workshop on Blockchain for IoT and Cyber-Physical Systems (BioTCPS '20).
- [13] L. Bader, J. Pennekamp, R. Matzutt, D. Hedderich, M. Kowalski, V. Lücke, and K. Wehrle, "Blockchain-Based Privacy Preservation for Supply Chains Supporting Lightweight Multi-Hop Information Accountability," *Information Processing & Management*, vol. 58, no. 3, 2021.
- [14] 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.
- [15] S. Malik, V. Dedeoglu, S. Kanhere, and R. Jurdak, "PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains," arXiv:2104.13964, 2021.
- [16] S. Malik, N. Gupta, V. Dedeoglu, S. Kanhere, and R. Jurdak, "TradeChain: Decoupling Traceability and Identity in Blockchain enabled Supply Chains," arXiv:2105.11217, 2021.
- [17] J. Pennekamp, M. Henze, S. Schmidt, P. Niemietz, M. Fey, D. Trauth, T. Bergs, C. Brecher, and K. Wehrle, "Dataflow Challenges in an *Internet of Production*: A Security & Privacy Perspective," in *Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC '19)*. ACM, 2019, pp. 27–38.
- [18] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?" *International Journal of Production Economics*, vol. 211, pp. 221–236, 2019.
- [19] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Management*, vol. 24, no. 1, pp. 62–84, 2019.
- [20] J. Pennekamp, R. Glebke, M. Henze, T. Meisen, C. Quix, R. Hai, L. Gleim, P. Niemietz, M. Rudack, S. Knape, A. Epple, D. Trauth, U. Vroomen, T. Bergs, C. Brecher, A. Bührig-Polaczek, M. Jarke, and K. Wehrle, "Towards an Infrastructure Enabling the *Internet of Production*," in *Proceedings of the 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS '19)*. IEEE, 2019, pp. 31–37.
- [21] J. Pennekamp, F. Alder, R. Matzutt, J. T. Mühlberg, F. Piessens, and K. Wehrle, "Secure End-to-End Sensing in Supply Chains," in *Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS '20)*. IEEE, 2020, Proceedings of the 5th International Workshop on Cyber-Physical Systems Security (CPS-Sec '20).
- [22] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Yellow Paper, 2014.
- [23] L. Bader, J. C. Bürger, R. Matzutt, and K. Wehrle, "Smart Contract-Based Car Insurance Policies," in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps '18)*. IEEE, 2018.
- [24] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT supported Supply Chains," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain '19)*. IEEE, 2019, pp. 184–193.
- [25] B. Düdder and O. Ross, "Timber Tracking: Reducing Complexity of Due Diligence by using Blockchain Technology (Position Paper)," in *Joint Proceedings of the BIR 2017 pre-BIR Forum, Workshops and Doctoral Consortium (BIR-WS '17)*, vol. 1898. CEUR Workshop Proceedings, 2017.
- [26] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," in *Proceedings of the 7th Conference on the Theory and Applications of Cryptographic Techniques (CRYPTO '87)*, vol. 293. Springer, 1987, pp. 369–378.
- [27] O. González-Benito, P. A. Muñoz-Gallego, and E. García-Zamora, "Role of collaboration in innovation success: differences for large and small businesses," *Journal of Business Economics and Management*, vol. 17, no. 4, pp. 645–662, 2016.
- [28] M. De Angelis, F. Adıgüzel, and C. Amatulli, "The role of design similarity in consumers' evaluation of new green products: An investigation of luxury fashion brands," *Journal of Cleaner Production*, vol. 141, pp. 1515–1527, 2017.
- [29] J. Cross, S. van der Wal, and E. d. Haan, "Rough Cut: Sustainability Issues in the Coloured Gemstone Industry," SOMO, Tech. Rep., 2010.
- [30] S. E. Chang and Y. Chen, "When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications," *IEEE Access*, vol. 8, pp. 62 478–62 494, 2020.
- [31] Bundestag, "Act on Corporate Due Diligence Obligations in Supply Chains," Federal Republic of Germany, Tech. Rep., 2021.
- [32] ETHGasStation, "ETHGasStation," <https://ethgasstation.info>, 2017.