Blockchain Enabled Traceability – Securing Process Quality in Manufacturing Chains in the Age of Autonomous Driving

Marlene Kuhn
Friedrich-Alexander
University Erlangen-Nürnberg
marlene.kuhn@faps.fau.de

Huong Giang Nguyen
Friedrich-Alexander
University Erlangen-Nürnberg
huong.nguyen@faps.fau.de

Heiner Otten
Friedrich-Alexander
University Erlangen-Nürnberg
heiner.otten@fau.de

Jörg Franke
Friedrich-Alexander
University Erlangen-Nürnberg
joerg.franke@faps.fau.de

Abstract—**Autonomous driving (AD) promises to disrupt current process management practices in the automotive industry, as processes now have to fulfill increasing requirements for safety, quality and liability. This paradigm change especially manifests itself among electrical system suppliers, as the electrical components transmit the vehicle's energy and communication flow, determining safety critical functions in the vehicle such as steering and braking. In this research, we conducted a multiple embedded case study in the electrical supplier industry in order to derive current challenges as well as future requirements for production processes of safety critical products in the age of autonomous driving. Our data suggest, that the established manufacturing process and practices are unable to fulfill the increasing need for digital continuity, transparency and documentation. To overcome those barriers, we propose a blockchain (BC) and Internet of Things (IoT) enabled traceability system. Through the application of BC, processes can be interconnected, tracked and audited, achieving higher security, liability and quality. This is the first paper, which investigates manufacturing of electrical systems for self-driving vehicles as a suitable use case for BC application.**

Keywords—traceability, blockchain, autonomous driving, IoT

I. Introduction

The production of autonomous and electrified vehicles will compose a great challenge for automotive original equipment manufacturers (OEM) and their electrical system suppliers. The electrical system contains the wiring harness, which transfer signals and energy to all relevant actors in the vehicle, as well as its adjacent E/E components, which are connected to the wiring. As vehicles are becoming increasingly electrified, the harness fulfills a growing amount of functions and commands, which need to be transmitted over the wiring system and its electrical components. In the past, the harness used to be a price-driven commodity product for the vehicle with the majority of functions outside the vehicle operation mode. Failures, like for example a disconnected parking sensor, could induce inconveniences for the final customer, but would not entail massive material damage or threats to individuals.

Most failures in the electrical system could therefore be classified as minor failures [1]. In an autonomous vehicle, the wiring harness fulfills a new role, as it is one of the most expensive and quality critical physical components, enabling safety critical functions such as steering and braking [2]. Failures would then have to be classified as critical failures, which could endanger the physical integrity of passengers or other road users such as pedestrians or cyclists. The assumption of a rise in critical failures in the electrical system (software and hardware) led to the development of the ISO 26262 norm for the automotive industry, which classifies failures according to automotive safety integrity levels [3]. The quality and safety of a product is highly influenced by the quality of the processes applied to develop and produce this product. Consequently, production processes need to be aligned to the requirements and specifications of their corresponding products based on internal and external customer expectations. Accordingly, we expect autonomous driving and electrification to initiate a paradigm shift in the automotive electrical system supplier industry concerning their production practices. Nowadays, the production process is designed from a cost-driven perspective. A traceability system is usually not established for the electrical products and its sub-components, which composes a typical strategy for a commodity product with mostly minor failure consequences [4]. As the product is now becoming increasingly quality critical, the production processes are now experiencing a change of requirements towards higher safety.

A key component in preventing safety and quality deficiencies in manufacturing processes is a state-of-the-art traceability system. Traceability describes the ability to reconstruct a product's composition (product history) as well as its value generation (process history) throughout the entire product's life cycle in form of an interlinked and consistent data set. With the use of a traceability system, safety problems and failures can be managed timely and effectively when they occur or even prevented in the first place. Additionally, a traceability system helps to avoid costly recalls and to manage the communication and containment of failures. [4], [5], [6] In the case of autonomous driving, this could not only offer economic benefits, but could even safe human lives.

This research work is part of the FAU project E|Connect, funded by the Bavarian "Investment for growth and jobs" project, which is part of the European Regional Development Fund (ERDF), 2014-2020.

978-1-5386-4315-0/18/$31.00 ©2018 IEEE

II. Methodology

The goal of this research is to analyze current traceability practices in the electrical supplier industry as well as the future requirements that arise within the paradigm shift of autonomous driving. To the best of our knowledge, there has been no empirical research conducted on this topic. To fill this research gap, we designed a multiple embedded case study, which addresses key stakeholders within this industry. Within our case study, we opted for two research questions (RQ):

1) RQ1: How can the state-of-the-art production process in the electrical supplier industry be characterized?

2) RQ1: What are future requirements for the production processes of safety critical components in autonomous vehicles and how can these requirements be implemented?

A case study is a systematic methodology, which allows to explore relations and variables within industry-driven topics in early phases of research and development [7]. In our research, we followed the methodology as presented by [7] and [8] throughout our study for company and expert selection, data acquisition, analysis and interpretation. We designed a multiple embedded case study, in which 18 companies participated. The companies ranged from big automotive OEMs, to first-tier suppliers (harness and electronic component producers). Furthermore, software suppliers for harness manufacturing as well as small and medium sized companies (SME) producing specialized sub-components were included to allow a holistic and multi-perspective investigation of the paradigm shift within this industry. The 45-90 minute interviews were conducted between October 2017 and April 2018, while a semi-structured interview guide was applied. Overall, 29 industry experts were interviewed resulting in transcripts of 170 pages in total. The data were acquired and analyzed according to our research framework consisting of four perspectives on traceability, as depicted in Fig. 1. This framework was adapted from the research on traceability for food safety conducted by [4].

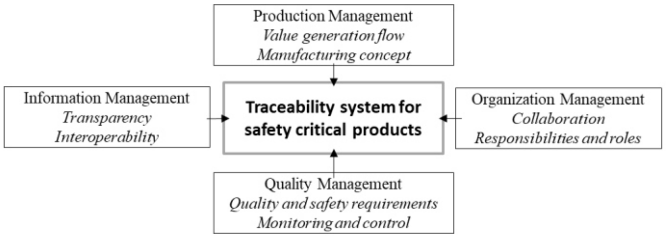


Fig. 1. Traceability research framework adapted from [4].

A traceability system for safety critical products needs to consider a multi-perspective analysis, incorporating the production management, the organizational collaboration strategy as well as the quality management practices and the technological implementation of the traceability data (information management). Accordingly, the case study data were coded with a qualitative data coding software (MAXQDA), deriving future requirements for the production process using the four perspectives of the framework. Based on our findings, we then demonstrate why BC technology could help to overcome the identified requirements and barriers, and propose the electrical supplier industry as a novel use case for BC application.

III. Case study results

In order to ensure traceability for safety critical products, the four perspectives production management, organization management, quality management and information management need to be taken into consideration. We discussed the value generation process with the industry experts according to the four clusters, leading to the following results.

A. *Production Management*

The production process is characterized by high volatility and flexibility according to the companies interviewed. The majority of products are produced in lot size one based on a specific customer order. The electrical system is a highly customized and structurally complex product, which is assembled and shipped Just in Sequence (JIS) to the OEM. While sub-components are pre-fabricated in batches using automated or semi-automated machines, the final system is assembled with manual labor. In general, it was stated that between 50-70% of the value generation of the electrical system is accomplished manually. The value network of every Tier1 is spread globally over various production sites, ranging from North Africa, to Asia, Mexico and North America as well as Europe. The production process is generally designed with a low degree of automation and standardization and all interviewees stated, that production practices and improvements are always considered from a cost-perspective first. Consequently, the majority of companies have not established a continuous traceability system, as it has not been profitable due to the nature of the product as a cost-driven commodity with limited failure impact and scope.

B. *Organization Management*

The electrical system of a car is designed and produced in multi-partner networks that are spread around the globe. According to two thirds of the interviewees, these multi-partner networks show a clear power distribution, in which the OEMs take over the central leadership role. As each OEMs has very distinctive specifications for their product and its production process, the Tier1s and SMEs face great challenges managing these different and sometimes even contradictory requirements within one production line. Some companies produce for several OEMs in one plant, which can only be accomplished by flexibly adapting process steps, material or machines according to the differing specifications. Alternatively, Tier1s build specific production lines for each OEM according to their specifications, but this often results in suboptimal production resource occupancy and increases their supply chain dependency. The requirement management is further complicated by changes (up to 100 per day), that are initiated by the OEM or the final customer. These changes are often communicated by telephone, fax or on paper and are therefore challenging to properly integrate and trace along the production process. In general, it was stated by the Tier1s and SMEs that the unequal power distribution causes high transaction, communication and reconciliation costs for the companies in the beginning of the value stream.

The organizational relations are established with a long-term perspective according to the interviewees, meaning the interchange and cooperation last many years. All cases agreed, that the value generation process of the harness and electrical system has too many organizational interfaces, which display a high error rate and error probability. At those interfaces, information is often lost or altered when transferred. Many companies stated that lacking trust hinder joined data usage and sharing, which is further emphasized by an expert silo culture within this industry. The power gap further accentuates a culture of mistrust, hindering information sharing and process visibility.

C. Quality and Safety Management

All companies stated, that quality control and safety management are rising challenges in the production process. As all harnesses are unique products, standardized in-line testing is difficult to implement. Additionally, the product is increasingly complex in structure and configuration options, entailing growing efforts for requirement management and documentation. Every requirement set includes product as well as process specifications, which have to be transparently monitored, tested and documented throughout the production process. Process monitoring is done partly digitized, but often the so-called four-eyes principle is applied as quality control. The majority of the cases stated, that the companies are facing increasing problems to realize consistent and automated quality control throughout the manufacturing process. Some companies suggested, that the high amount of variants and a lacking digital continuity are the main causes, that the quality management and safety management causes excessive costs for this industry in the forms of additional labor and supplementary process steps and testing. These costs are assumed to rise exponentially in the context of AD. Within the case study, OEMs and Tier1s stated, that errors in the electrical system are often assigned to the Tier1's or SME's responsibility, although the error might have occurred during the assembly process at the OEM. Tier1s and SMEs then have to undergo excessive iteration loops to prove that the error was not caused within their responsibility.

D. Information Management

Our analysis showed, that for this industry, the information management maturity highly depends on the process automation degree in the value stream. In the automated production areas, data are stored digitally and interlinked to a consistent product and process history, allowing to retrace the product's origin and quality history. In automated production areas, traceability and data continuity are achieved through barcode labeling and the utilization of manufacturing execution systems (MES). However, the majority of production steps are accomplished through manual labor. In the manual areas, information are often stored in an analogous format (e.g. on paper). Moreover, information management is disrupted in these areas, as barcodes are not further scanned or interlinked with process data. As the manual production follows the automated production, the internal traceability data can not be associated with the final product that is shipped to the OEM. All interviewees stated, that process interfaces are very heterogeneous and nontransparent from a data perspective, while information exchange procedures are often unclear. The experts estimated that the information flow is currently disrupted by 6-10 interfaces, while each interface increases the probability of failures. The SMEs of the study mentioned, that they often can not prove that the failure did not occur within their responsibility due to the lacking documentation along the entire value chain. The Tier1s and SMEs expect 30-40% efficiency increases, if a consistent, data continuous and digital information flow was to be established.

E. Process requirements induced by autonomous driving

In the second part of the case study, we focused on the new requirements and process characteristics that arise within the paradigm shift of AD. Analogously to the first analysis, we focused on the process from a traceability perspective using the four clusters of our research framework. The changing process structure can be classified by increasing documentation and liability requirements, which can only be met through a higher degree of process standardization, automation and digital continuity, as shown by table 1.

TABLE I. PROCESS PARADIGM CHANGES FOR AUTONOMOUS VEHICLES

	Process characteristics	**New characteristics & requirements**
Production	• Customized products (build-to-customer order) • High degree of individualization and complexity are handled using manual labor • Cost-driven process flow • Low visibility and transparency	• Standardized products (mobility fleets) • Standardization and increasing safety requirements require automated manufacturing • Safety-driven process flow • Full traceability and liability
Organization	• Power concentration and central leadership at OEM • Failures often assigned to suppliers or SMEs (power gap) • Established long-term value networks with minor fluctuation • Pressure and power as part of cost-driven strategy	• Increasing supplier role due to shared AD responsibility • Clear liability and transparent responsibilities required • Fast integration of new companies to gain momentum in AD • Trust and integration to achieve innovations in AD
Quality	• Ad-hoc quality management due to individualization and high volatility • Minor errors with quality impact • Documentation is low (IATF 16949:2016 requirements) • End of line quality tests • High costs and efforts for failure allocation	• Standardized and digital quality management enabled trough automation and data continuity • Critical errors with safety impact • High documentation requirements (ISO 26262) • Real-time quality status along process flow (automated) • High transparency and fast recalls to safe human lives
Information	• Data integration depends on company size and power (SMEs often not integrated) • Data is lost or manually changed at process interfaces • Data is kept in expert silos (redundant data) • Data exchange procedures (analog and digitized) using different tools	• Fast and efficient data integration of all participants building AD vehicle • Immutable and consistent data management • Trustful and reliable data distribution • One consistent data flow for each product flow

All cases, especially the OEMs, stressed that safety and failure prevention will be the determining element of manufacturing processes for safety critical electric components. The safety and quality requirements must be 100% transparent and fully monitored throughout the supply network. This implies increasing documentation efforts for all companies involved in producing autonomous vehicles, whereby traceability becomes a must for all components performing safety critical tasks in the electrical system. The OEMs stated, that they will not only demand end-of-line quality tests to be documented, but the documentation of all safety and quality relevant process steps, as well as in-line testing and monitoring efforts. The amount of traceable quality gates will therefore increase significantly, which will be distributed across SMEs, Tier1s and OEMs alike. Additionally, the traceability data need to be analyzed automatically and continuously (e.g. through advanced analytics) to prevent failures to happen in the first place. Traceability can only be achieved by increasing the automation degree in the manufacturing process, while process interfaces need to be decreased and efficiently interconnected. Some companies suggest, that production processes of the electrical system need to be 100% automated, while machines are expected to monitor and report quality data without human interference. The increased automation will be facilitated by an increase of standardization, as autonomous vehicles will not primarily be produced based on a customer order but for mobility fleets. Our data show that all companies involved clearly follow two goals for their value generation process within the paradigm shift of autonomous driving: The primary goal is to ensure safety and quality for all critical components in order to prevent failures. This can only be achieved with a consistent and transparent traceability information set, which allows errors and deficiencies to become transparent and facilitates preventive measures. Secondly, all companies want to assure that failures are not falsely assigned to them, as this could entail high recall and liability costs, brand damage and customer churn. Accordingly, a traceability system of high integrity, equal distribution and mutual benefit is needed to ensure trusting collaboration among all companies involved in the production of an autonomous vehicles. Data integration, data quality and data continuity thereby play the most important role to ensure traceability and trust in this multi-stakeholder production processes. However, the companies were uncertain how to implement their requirements. The majority rejected ideas and technologies like a cloud solution, as many feared it would centralize the data power and competencies with either the OEMs themselves or a service provider assigned by the OEMs. Alternatively, they required a solution that would emphasize cooperation and mutual responsibility for all companies involved in the production flow. This solution should enhance transparency, data sharing and process automation, while at the same time being accepted by all participants to offer the traceability information needed in liability cases and recalls, which will happen more frequently in the future. None of the participants were familiar with BC technology and therefore this solution was not proposed in any of the cases. However, the requirements stated can be aligned with the characteristics of BC, which could therefore be used to solve the traceability issue of safety critical components in the electrical supplier industry. Based on our research data, we therefore propose BC technology as a suitable solution to overcome the barriers and requirements presented in the four clusters of traceability systems of safety critical products. Furthermore, BC can offer further benefits which go beyond the barriers discussed in the case study.

IV. PROPOSED BLOCKCHAIN ENABLED TRACEABILITY SYSTEM

BC is a peer-to-peer exchange network, maintaining a distributed ledger database [9]. The transaction history is agreed upon without an intermediate party, making BC highly applicable for direct value exchange procedures. BC was first presented by Satoshi Nakamoto in the form of the cryptocurrency Bitcoin [9]. However, the technology's application potentials have been discussed far beyond cryptocurrencies, involving use cases in supply chain management, IoT as well as government and administration [10], [11], [12]. BC functions as a record of transcripts in form of time-stamped blocks, which are created and stored by all participants of the network. Through the BC's consensus algorithm, such as Proof of Work (Pow) or Proof of Stake (PoS), new blocks are created and added to the chain of transactions [9], [13]. A block usually consists of the primary transaction data, a block header, the merkle tree root and the hash value of the previous block [13]. Hashes are applied to interlink all data into a chain, allowing members to verify and trace the history of transactions. Alterations in the primary data would change the hash value und therefore lead to an invalid reference chain. BC therefore creates high data integrity, transparency and trust among participants [14]. In a BC, only the rightful owner can authorize value transfers to other members of the network. This is achieved by applying asymmetric cryptography in the form of public and private keys. Asymmetric cryptography therefore helps to verify transaction authorization, which creates ownership visibility and liability in value exchange networks. Additionally, BC allows the integration of so-called smart contracts, which are self-executing digital contracts that allow to automate process steps based on defined if-then premises [15]. Summarizing, BC is a technology creating a valid and immutable record chain of events in a decentralized network of non-trusting participants. Those characteristics make it highly applicable for traceability use cases, which have been discussed among researchers and practitioners alike, such as diamond tracking (Everledger), pharmaceuticals anti-counterfeiting (Block-verify) or ensuring food safety (Walmart and IBM). Most of those use cases, however, are presented from a business perspective and lack detailed information regarding architectural design, role allocation or consensus, which could then be transferred to the use case of the electrical system supplier industry. Nevertheless, the traceability projects demonstrate, that BC is applicable for traceability purposes of critical products. In the following we will propose a BC traceability system to overcome the barriers of increasing process safety, monitoring and documentation as well as shared responsibility in the automotive supplier industry.

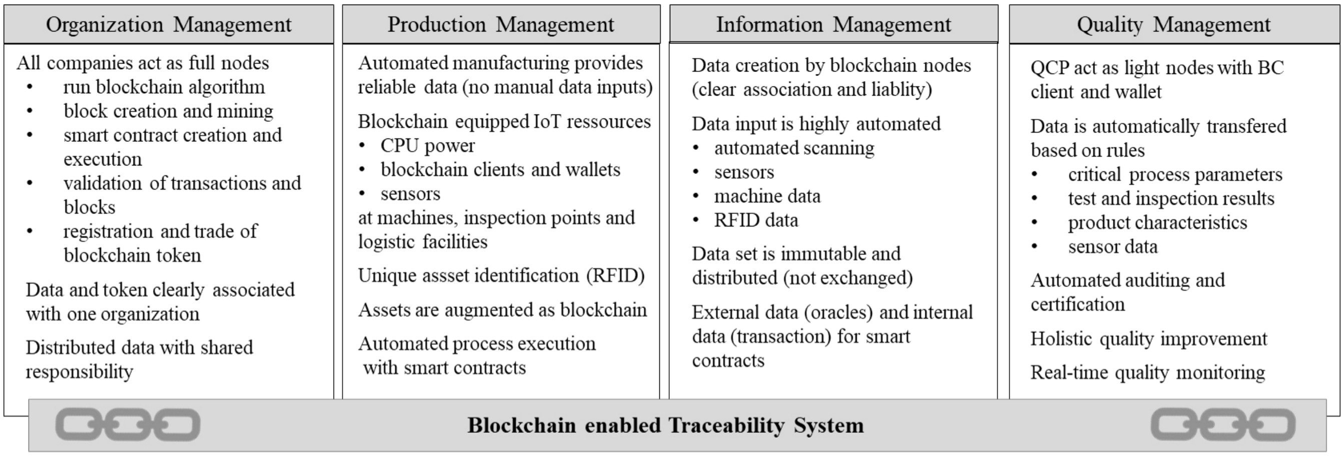
A. *Architectural design*

Based on the primary work on BC of [9], [13] and [15], we conceptualized the BC architectural design to meet the specifications derived from the case study. As a solution to our RQ2, we propose a consortium BC based on Ethereum or Hyperledger, in which every company participating in the value creation provides at least one full BC node. All network members (OEMs, Tier1s and SMEs) have full control over the

BC network and collaborate at eye level. All nodes are responsible for running the BC algorithm as well as the creation and validation of new blocks and the mining. Additionally, they register BC token, ore more specifically products and modules with their unique identity provided by an RFID chip or barcode, to the BC network. Then they can trade the token using BC transactions, meaning that products digital equivalents are transferred between two nodes. As a consensus method, we propose to apply a resource-efficient method like PoS or byzantine fault tolerance (PBFT) algorithm. Using PoS, miners are chosen randomly based on probability figures such as the token share in the network [14]. With PBFT blocks are accepted after a two-third vote of miners voted for it. In small consortium networks of organizations with long-term business relations, PoS or any similar algorithm determining miners by chance can be applied. Every node should select quality critical points (QCP) along its process flow to be part of the BC network. A QCP could compose a machine or quality testing area, in which safety relevant tasks are performed and where traceability relevant data is generated to be stored in the BC [16]. QCP should be equipped with appropriate IoT technology to participate in the BC network. We propose that all QCP are provided with a BC light client, transforming all QCP into light nodes. Using simplified verification methods, light nodes can download and verify parts of the BC, as well as engage in transactions and smart contracts [9], [13], without needing the full CPU power to run the entire BC and participate in mining. Each light client would further include a BC wallet, allowing machines to directly compensate each other for services and transactions. BC allows to solve the barriers presented for each cluster in the traceability framework, creating transparency and visibility across organizational boundaries for safety critical products, as shown in Fig 2. From an organizational perspective, all companies participating in the production of the autonomous vehicle are connected over the BC technology. BC therefore significantly increases interoperability and equality in the network, as every participant has an equal share and responsibility ensuring traceability and process quality. As every token can be associated to a specific node (full or light node), the product history can be tracked throughout the supply chain. Furthermore, quality critical process parameters and safety relevant measurements are stored in the BC database, which immutably registers all safety relevant information with the product ID. Data input should be highly automated, meaning that no humans should be able to insert data into the BC database. This requires high IoT capabilities within the production, as only machines, sensors or software should create BC data. Through smart contracts, processes can be automated based on pre-agreed if-then premises. Exemplarily, the Tier1 could get paid for its final product, when the product ID reaches the "shipped-status" in the BC database. Additionally, the smart contract could check, if all quality tests were conducted with a positive result or if the product arrived at the OEMs RFID gate on time. Time delays could cause deduction from the prices, based on pre-defined rules. The presented traceability system would allow companies to monitor processes in-real time from a quality and safety perspective. These processes could be distributed across departments, companies or even countries, but would be connected and trusted over BC technology. The traceability data could further be used to automatically generate certificates and audit processes.

B. Application use case

In order to deepen the understanding of our proposed solution, we describe a simplified application use case, detailing the functionalities of the BC traceability system. All companies (Tier1, OEM, SME and software) in this example comprise a full node in the BC network, providing the necessary computing resources to store the database, run the algorithm and mine new blocks. Moreover, they openly broadcast smart contracts to the network. The production flow starts by registering the supplier material, which could comprise wires, crimps and terminals, at the Tier1s inbound logistic area (QCP_1) to the BC. Traceability information are further linked with the product batch ID, exemplarily including supplier name, supplier location, production date and batch size. Automated machines then cut the wiring into certain lengths and attach terminals to their ends. These newly created modules get a new ID. This identity can now be traded and transferred as a token among nodes in the BC network. Safety relevant process parameters such as crimping force are also associated with the new ID and stored in the database (QCP_2). As QCP_1 transfers the token to QCP_2, the transaction gets time-stamped and authorized by the node's private key.



Organization Management	Production Management	Information Management	Quality Management
All companies act as full nodes • run blockchain algorithm • block creation and mining • smart contract creation and execution • validation of transactions and blocks • registration and trade of blockchain token Data and token clearly associated with one organization Distributed data with shared responsibility	Automated manufacturing provides reliable data (no manual data inputs) Blockchain equipped IoT ressources • CPU power • blockchain clients and wallets • sensors at machines, inspection points and logistic facilities Unique assset identification (RFID) Assets are augmented as blockchain Automated process execution with smart contracts	Data creation by blockchain nodes (clear association and liablity) Data input is highly automated • automated scanning • sensors • machine data • RFID data Data set is immutable and distributed (not exchanged) External data (oracles) and internal data (transaction) for smart contracts	QCP act as light nodes with BC client and wallet Data is automatically transfered based on rules • critical process parameters • test and inspection results • product characteristics • sensor data Automated auditing and certification Holistic quality improvement Real-time quality monitoring

Fig. 2. Proposed blockchain enabled traceabilty system

Each ownership transaction is therefore highly visible and product liability can be established. Additionally, QCPs function as decentralized and autonomous light nodes in the BC network, which transfer products and parts as well as store and interlink traceability data without an intermediary. Through smart contracts, the production process can be automated and accelerated. In-line quality monitoring is installed to scan all crimps and terminals for failures using cameras. If a failure is detected, the machine requests part replacement from a 3D printer. Using a smart contract, the machine could order parts from the printer directly, compensating it over the installed wallet in the BC light client. All companies of the network work analogously; they create value with the associated product or module and store the product ID with quality and safety relevant parameters to the BC network. Software suppliers for example store the ID of their software version, which is interlinked with the ID of the control unit, on which the software is installed. In the JIS outbound, the last QCP of the Tier1, the product is transferred to the inbound area of the OEM using the Tier1's digital signature. From this point on, the product and all value steps can be associated with the OEM. Using smart contracts, the OEM and Tier1 could agree on automated certification and audits based on process parameters and quality results that are stored to the BC. These results could be accessed by an auditor over a light client. As all data could be accessed based on pre-defined reading and writing rights, the auditor only reads the data relevant to the auditing or certification process. As auditing costs for safety critical products are higher compared to commodity products, BC can provide a cost-efficient and transparent certification system for critical components for autonomous vehicles.

C. Discussion

One could argue that traceability can be established with conventional technologies, while other barriers presented in the case study section could be overcome with specific organizational agreements and improvements. The proposed BC solution, however, would compose a holistic system addressing the majority of the derived requirements. From an organizational perspective, BC would allow to decentralize power, creating a network of increased mutual benefit and trust, instead of centralized control. From an information management point of view, all participants can trust and monitor the traceability relevant data, ensuring inter-organizational transparency and interoperability. Additionally, BC would push investments in automated manufacturing and IoT resources, which will be required by the OEM to increase quality and safety in the production process. A higher automation and IoT maturity would facilitate accurate data inputs as well as automated process execution using smart contracts. From a quality management perspective, BC would facilitate quality improvements based on a holistic and trustworthy database. Moreover, the database would comprise the documentation needed for fast recalls and liability cases. Certification and auditing could also rely on the BC database, which also provides the opportunity to automate parts of the auditing process. Instead of implementing specialized solution for this multi-dimensional problem, BC could offer an integrated system with multilateral benefits.

V. Summary

In the age of autonomous driving, the automotive electrical system supplier industry faces increasing pressure and quality requirements concerning their production processes. Through a blockchain enabled traceability system, the production process can be monitored and holistically improved across companies and country boarders. Blockchain allows to comprehend and retrace the product history and all relevant process steps of this safety critical product. Moreover, the technology would allow to interconnect process interfaces with one consistent system. Blockchain could therefore provide a holistic and continuous data set, which can be harnessed for quality improvement, failure prevention and reliability predictions. Blockchain further paves the way for equal responsibility distribution, facilitating collaboration as well as failure allocation and recalls in the network.

References

[1] A. T. Bahill and A. M. Madni, *Tradeoff Decisions in System Design*, Springer, 2016.

[2] A. Weber, "Wiring autonomous vehicles", *Assembly Magazine*, Oktober 5, 2017. [online], Available: https://www.assemblymag.com/articles/93998-wiring-autonomous-vehicles. [Accessed: Jul. 2, 2018].

[3] *ISO 26262 Road vehicles – Functional safety*, International Organization for Standardization (ISO), 2011.

[4] H. Ringsberg ,"Perspectives on food traceability: a systematic literature review", *Supply Chain Management: An International Journal*, vol. 19, no.5/6, pp.558-576, 2014.

[5] P. F. Skilton and J. L. Robinson, "Traceability and normal accident theory: how does supply chain network complexity influence the traceability of adverse events?", *Journal of Supply Chain Management*, vol. 45, no. 3, pp. 40-53, 2009.

[6] A. Regattieri, M. Gamberi, and R. Manzini, "Traceability of food products: general framework and experimental evidence", *Journal of Food Engineering*, vol. 81, no. 2, pp. 347-356, 2007.

[7] R. K. Yin., *Case Study Research Design and Methods*, CA: Sage Thousand Oaks, 2014.

[8] K. Eisenhardt, "Building Theories from Case Study Research", *The Academy of Management Review*, vol. 14, no. 4, pp. 532-550, 1989.

[9] S. Nakamoto, "Bitcoin. A peer-to-peer electronic cash system", 2008. Available: https://bitcoin.org/bitcoin.pdf, [Accessed: Jun. 5, 2018].

[10] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger", *International Journal of Research in Engineering and Technology*, vol. 05, no. 09, pp. 1-10, 2016.

[11] A. Bahga and V. K. Madisetti, " Blockchain Platform for Industrial Internet of Things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, pp. 533- 546, 2016.

[12] M. Conoscenti, A. Vetro and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review", In Proc. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications, '11, 2016, pp. 1-6.

[13] V. Buterin, "Ethereum: a next generation smart contract and decentralized application platform", 2013. Available: https://github.com/ ethereum/wiki/wiki/White-Paper, [Accessed: Jun. 13, 2018].

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey", *International Journal of Web and Grid Services*, 2016.

[15] N. Szabo, "Smart Contracts: Formalizing and Securing Relationships on Public Networks", *First Monday*, vol. 2, no. 9, 1997.

[16] M. Kuhn, M. Paul, F. Schaefer, and H. Otten, "Potentials of Blockchain Technology for the Quality Management of Interconnected Processes" In Proc. International Conference on Quality Engineering and Management '07, 2018, pp. 438-457.