2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)

Reducing Automotive Counterfeiting using Blockchain: Benefits and Challenges

Donghang Lu
Purdue University

Pedro Moreno-Sanchez
TU Wien

Amanuel Zeryihun
Ford Motor Company

Shivam Bajpayi
Purdue University

Sihao Yin
Purdue University

Ken Feldman
Ford Motor Company

Jason Kosofsky
Ford Motor Company

Pramita Mitra
Ford Motor Company

Aniket Kate
Purdue University

***Abstract*—Counterfeiting constitutes a major challenge in current supply chains leading to millions of dollars of lost revenue for the involved parties every year. Hardware-based authentication solutions built upon physically unclonable functions (PUF) and RFID tags prevent counterfeiting in a multiparty supply chain context. Unfortunately, these solutions cannot prevent counterfeiting and duplication attacks by supply chain parties themselves, as they can simply equivocate by duplicating products in their local and unique activity ledger.**

In this work, we study the benefits and challenges of using distributed ledger technology (or blockchain) to prevent counterfeiting even in the presence of malicious supply chain parties. In particular, we show that the provision of a distributed and append-only ledger jointly governed by supply chain parties themselves, by means of a distributed consensus algorithm, makes permissioned blockchains such as Hyperledger Fabric a promising approach towards mitigating counterfeiting. At the same time, the distributed nature of the ledger also possesses a privacy challenge as competing supply chain parties strive to protect their businesses from the prying eyes of competitors. Additionally, we show our efforts to build a blockchain-based counterfeiting prevention system for automotive supply chains, albeit the lessons learned are seamlessly applied to other supply chains. From our experience, we highlight two lessons: (i) the requirement of adding identities other than supply chain entities themselves to facilitate the tracking of goods; and (ii) the challenges derived from privacy enforcement in such a permissioned scenario. We thus finalize this work with a set of challenges that need to be overcome to achieve the best of both worlds: a solution to the counterfeiting problem using distributed ledger technology while providing the privacy notions of interest for supply chain parties.

***Index Terms*—Blockchain, supply chain, privacy, access control, Hyperledger Fabric**

I. Introduction

The U.S. automobile industry is a key driver of the nations economy, with auto parts representing a significant component of the industry. Retail auto components sales were estimated at $143 billion in 2015 by the Auto Care Association, and online sales is also a rapidly growing segment of that market. Online sales of auto components is projected to exceed $10 billion for the first time this year, a 16 percent increase from 2017, and projected to jump 60 percent over the next three years. However, the high global demand for a wide breadth of automotive components and enormous profit opportunities makes them an extremely attractive target for counterfeiters. Advances in design and manufacturing technology, for example 3D printers, make it increasingly easier to replicate all part commodities only exacerbating the problem going forward. Frost & Sullivan [1] estimated that automotive suppliers worldwide lost $45 billion to counterfeiting in 2011. In 2016, Organization for Economic Cooperation & Development (OECD) reported the global trade-related counterfeiting accounts to be $461 billion, or 2.5% of the world trade [2]. What's worse, automotive counterfeiters are not typically concerned with quality, performance, durability or safety and this put customers in dangerous, life-threatening situations. As a result, enhancing automotive supply-chain traceability and deterring counterfeiting of goods has become a key challenge for automotive companies.

This environment causes the opportunity for counterfeiters to thrive. There is a large demand created for new components in order to fix consumers cars in a highly competitive market. A counterfeit component might allow you to replace a malfunctioning part, shut off warning lights, or even use it to replace a deployed product. The legitimate manufacturers work hard to service the aftermarket and ensure Original Equipment (OE) parts are available for vehicle repair regardless of service facility. Counterfeiters take advantage of the marketplace by offering alleged OE parts for a discounted price while generating huge profit opportunities. Therefore, in order to reduce the risk of counterfeiting in the supply chain (and to protect vehicle owners), there is a need for improved part traceability through the complete supply chain.

In addition to counterfeiting, there are also enormous opportunities to dramatically improve the recall process, replacing a defective component in a vehicle originating from the vehicle manufacturing process. Track and traceability with individual component supply across the sub-tier network creates opportunities to significantly improve containment of a defective component, reduces costs, and customer inconveniences. Moreover, recalled components such as airbags would potentially be identified and prevented from re-entering the aftermarket for vehicle installation. Solutions like physically unclonable functions (PUF) [3] and RFID [4] help in identifying and authenticating the goods but they cannot prevent the counterfeiting from insiders (i.e., players who are part of the supply chain themselves). The adversarial supply chain

978-1-7281-1264-0/19/$31.00 ©2019 IEEE
DOI 10.1109/DAPPCON.2019.00015

players can easily equivocate (and modify the supply chain logs) to present conflicting views to other players and to the end-consumers proactively during transmission as well as reactively during security audits.

Blockchain [5]–[10] is a decentralized ledger where the records are append-only and cannot be altered. This allows the participants to verify and audit transactions. It is initially used as platforms for cryptocurrencies like Bitcoin [5]. With the appearance of Ethereum [7] and Hyperledger Fabric [6], the conception of smart contract is proposed and can be used to enforce business logic through programming and without human interaction. As a result, several applications are built based on blockchain when people see the potential of decentralization, transparency and immutability [11], [12]; e.g., Walmart has been working with IBM to building a blockchain for food tracing and safety. [13] In this collaborative work between industry and academia we present a blockchain-based tractability solution for automotive supply-chains.

a) Contribution: We aim to reform the current automotive supply-chain management system by executing the supply and tracking of components using blockchains. The blockchain technology forms a distributed source of shared truth for supply chain, which along with smart contracts and cryptographic primitives helps mutually distrusting sets of players/companies with possibly adversarial interests to collaborate with a secure set of rules. The identity and transfer of genuine components are added to the ledger at each step by the appropriate supply chain player.

We propose to make the vehicle "blockchain-aware" such that it is capable of querying the blockchain ledger via a proxy server. Such blockchain-aware vehicles would enable enhanced transparency across the value-chain, all the way to the end customer. For instance, the vehicle should be able to tell the owner or the repair shop whether a replacement component being installed is a counterfeit (has no record on blockchain) or a Frankenstein module (made of authentic components taken from different models across the original equipment manufacturer). The proposed system enables traceability through the entire life cycle of components, i.e., starting from components assembly at sub-tiers through aftermarket till the components (or the vehicle itself) is retired/scrapped. Aftermarket traceability is important not only in counterfeit detection but also in resolving insurance frauds. It is also helpful in detecting Frankenstein components, i.e., components which are made of components taken from different models for an original equipment manufacturer (OEM).

Besides, we study and provide an overview to privacy problems introduced by the combination of supply chain and blockchain. Privacy goals such as confidentiality are not trivial to achieve when the blockchain is design to maintain a ledger where all actions are traceable [14]–[16]. We also implemented the prototype using Hyperledger Fabric v1.1 and summarize some general principles regarding applying Hyperledger Fabric to supply chains.

II. Background

A. Automotive Supply Chain and the Issue of Counterfeiting

In this section, we first outline the process flow of a safety-critical part, e.g., an airbag is assembled and installed in a vehicle. The automotive supply chain involves the OEM (i.e., original equipment manufacturer, the automaker in this case), tier 1 supplier and multiple sub-tiers [17]. The final assembly of an airbag module consists of three major components which are the airbag itself, the inflator, and the breakaway plastic horn pad cover. These three components are individually assembled at various sub-tiers (tier 2 or 3) and the final assembly is done at tier 1, where the airbag module is given a unique serial number. The three components are individually serialized, and the serial number of the components are paired up with the airbag serial number into the tier 1 tracking system. Next, the tier 1 ships a batch of airbags to the OEM, who then places them into vehicles, while creating a log of paired up Vehicle Identification Number (VIN) and airbag serial number into their tracking system. The traceability ends when the vehicles leave the factory.

There are several ways how counterfeits enter the value chain. For instance, the journey of a counterfeit part in the aftermarket can start with the end customer, i.e., owner of a vehicle for auto part replacements. The customer has a number of options to choose from, i.e., an authorized dealership, a parts store (e.g., Auto Zone), collisions center, or independent service repair shops. The authorized dealership can order serialized parts from OEM distribution center (direct shipment), and also update the cars computer with the new part serial number. However, an independent shop or collisions center would not have the ability to provide the same kind of verification. Small-scale repair shops often choose cheap parts to increase their profit margin, and may end up servicing counterfeit parts [18]. As a result, the owner is placed at a significant safety risk without their knowledge. For instance, a counterfeit airbag might explode during a crash, causing serious harm to the driver or passengers. In addition to auto part replacements, there are a few other channels for detecting counterfeit parts in the aftermarket, such as sample purchases by the OEM brand protection teams, warranty returns, investigations by government and law enforcement, etc.

During the investigations, quality teams at OEM itself (or at OEM and Tier 1 supplier) work together to identify the issue. To that end, OEM first tries to identify if the part being inspected has the right OEM branding. A subset of counterfeits, especially for the OEM unique parts, could be detected in this method. On the other hand, for parts that are not OEM specific but rather are sold as a "black box" by Tier 1, detecting counterfeit involves asking the Tier 1 to provide verification. The entire process is fairly manual and incurs less than optimal cost and latency, as the traceability is fragmented across the tracking systems of various supply chain players. Also, for "black box" parts where Tier 1 owns the intellectual property, the cause of the counterfeiting is not always shared seamlessly with the OEM. For instance, for "black box" parts,

OEM may not have full visibility if one of the components (e.g., inflator of an airbag) manufactured by a Tier 2 or 3 is the source of the counterfeits. Lack of a single, shared source of part traceability through its lifecycle (i.e., from sub-tiers all the way to aftermarket) prevents the OEM from performing adequate and timely risk analysis and mitigation strategies.

B. Distributed Ledgers aka Blockchains

A blockchain [5]–[10] is an append-only database maintaining a distributed ledger among a group of peers. It is a growing list of records, called blocks, with each block including a cryptographic hash of previous block. Blockchains can offer high resistance to modification of the history of the data due to this append-only property. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks. Besides, blockchains provide higher availability in the sense that we do not need to trust any single peer to maintain the database. Instead, all peers maintain it together consistently using consensus protocols.

Blockchains today are typically divided into two types: permissioned blockchain and permissionless blockchain. [19] Permissionless blockchain [5], [7] puts no restriction on which users can interact with the network, submit transactions and maintain the ledger. A permissioned blockchain, on the other hand, is a closed ecosystem where blockchain nodes have to be known pre-defined entities. As a result, permissioned blockchain is preferred by traditional organizations who plan to use blockchains for internal business operations. Permissioned blockchains often achieve better performance than permissionless blockchains since all users are known and no extra cost needs to be spend on stopping Sybil attacks.

This paper considers automotive supply chain use cases. An automotive supply chain is usually structured like a pyramid with the original equipment manufacturer (OEM) at the top and multiple tiers of suppliers and dealers at the bottom. As a result, permission blockchain is preferred since the identity of participants of supply chains are known to connected parties.

a) Permissioned/Consortium Blockchains: Consortium blockchain [20] refers to blockchain with consensus and validating processes controlled by groups of known and predefined nodes which are authorized. In consortium blockchains only authorized and authenticated parties are allowed to view/transact with the ledger. While providing all the advantages of public blockchain such as decentralization, security and tractability, it also provides efficiency and possibility of different levels of privacy protection.

b) Hyperledger Fabric: Hyperledger Fabric [6] is an open source permissioned distributed ledger technology platform designed for use in enterprise contexts. Fabric has a highly modular and configurable architecture, enabling innovation, versatility and optimization for a broad range of industry use cases. In Hyperledger Fabric, the participants are known to each other. As a result, although participants may not fully trust each other, a network can still be operated under a governance model that is built off of what trust does exist between participants, such as a legal agreement or framework for handling disputes.

Hyperledger Fabric supports smart contracts (here called chaincode), which are stored and executed by endorsing peers, who maintain the blockchain (the ledger). Other roles in Fabric includes clients who sends transaction proposals, certificate authorities who issue certificates to other network nodes, ordering nodes who provide consensus and validating peers responsible for validating transactions again after ordering. Besides, Hyperledger Fabric allows users to define endorsement policies defining which peers are responsible to agree on the result of transaction after executing the transactions. We summarize a general transaction flow (see Fig. 1) from Hyperledger Fabric [6] as follows:

- Clients generate a transaction and send it to endorsing peers for endorsements. A transaction contains information such as the chaincode name, channel name, parameter field, client's signature and some optional fields like transient field. This information is required because several chaincodes are simultaneously supported. Moreover, each chaincode specifies an *endorsement policy* that defines which endorsing peers must receive this transaction for a valid endorsement.
- Endorsing peers, upon reception of a client transaction, first check if the transaction is well formatted and if the client is authorized to perform the transaction. Then, endorsing peers will execute the transaction and generate a read set and write set containing the result of the execution together with endorsing peers' signatures. Importantly, at this point the state of the ledger is not modified yet. The transaction is just being "simulated" to generate the expected output.
- Clients eventually receive the endorsement from the endorsing peers, check its content, attached signature and if all endorsements have consistent read set and write set. Then, when clients receive enough of such endorsements (as required by the aforementioned endorsement policy), it will combine them together to form an envelope and send it to ordering service.

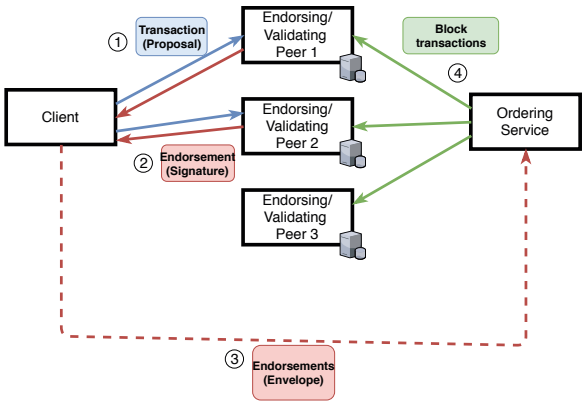

Fig. 1: Transaction Flow of Hyperledger Fabric

- The ordering service is carried out by a set of nodes (possibly different from the endorsing peers) that execute a consensus protocol to agree on the order of transactions, independently of their content. The sorted list of transactions is then included in blocks which are finally sent to the validating peers.
- Validating peers will validate the transaction inside the envelope again to confirm that the endorsement policies are satisfied and that the current state of the blockchain is consistent with read set in the envelope. Once all checks pass, peers will apply the change to their current state and append the received block to the blockchain.

Separation between the transaction execution and updating the ledger can bring us useful benefits [6]. For example, all peers are supposed to update the ledger, however, not all peers need to execute the transaction. As a result, chaincodes can be kept confidential from peers outside of endorsement policy. Besides, the separation can improve the throughput in the sense that transactions can be executed before ordering service, allowing transactions to be executed in parallel.

III. Blockchain for Automotive Supply Chains

A. System Model

We illustrate our system model in Fig. 2. We model a supply chain as a combination of a set of objects O, a set of entities E and a blockchain technology $\mathcal{B}$. Each object $o \in O$ represents a traceable item within the supply chain while each entity $e \in E$ represents a party involved in the production and distribution of objects all the way from the supplier to the consumer.

Each object $o \in O$ is composed of several components. Additionally, each entity $e \in E$ has associated a tuple (*role*, *actions*) that defines the entity's role in the supply-chain and the list of allowed actions for this entity, correspondingly. In the following, we describe the possible values for each of the elements of this tuple.

a) Roles: Each entity can take any of the following roles:

- *Supplier*. An entity that introduces legitimate objects into the supply chain.
- *Manufacturer (OEM)*. An entity in charge of mounting objects into the cars for the first time. Moreover, the manufacturer can recall a set of objects that have been detected faulty.
- *Dealer*. An entity that replaces objects included in a car that are either damaged or recalled by the corresponding manufacturer.
- *Car*. An entity that represents the car in the supply chain.

One of the novelties in our system model is the inclusion of Cars as one of the entities in the supply chain (and not only as a traceable object itself). We observe that it is important that each car is a "self-aware" entity in that it can verify the validity of the objects that are mounted on it (see "Car as self-aware entity" paragraph for a detailed discussion.)

b) Actions: Each entity might perform any of the following *actions*:

- *Add Component*. This action represents the introduction of new components into the supply chain.
- *Transfer Component*. This action considers the transferring of an object among different entities. Only the current owner of an object (i.e., the entity who holds it currently) can transfer the component.
- *Mount Component*. This action represents the assembly of an object into an entity whose role is a car.
- *Replace Component*. This action represents the replacement of a damaged or recalled object from a car. The replaced object should never been introduced again into the supply chain.
- *Recall Component*. This action represents the recalling of a component (e.g., a defective production line has been detected).
- *Check Component*. This action represents the checking of the validity of a given component.

c) Role-action Mapping: We restrict the possible combinations of roles and actions to those that suffice to faithfully represent the possible interactions in a supply chain. In particular, as shown in Table I, suppliers are the only ones to add new components into the supply chain. The manufacturer is the only entity in charge of mounting airbags for the first time in the cars and recall the defective components. The car must be self-aware of its components and check for their validity. Finally, all the entities can transfer a component that they hold to other entities in the supply chain.

d) Car as "Self-aware" Entity: With the development of the car industry, it is possible now to abstract cars as "self-aware" entities which can verify the mounted components and send signals to invoke or query the blockchain. These advances will bring us plenty of benefits since now a car can check its components occasionally and report faulty components itself. This also build up traceability of components after

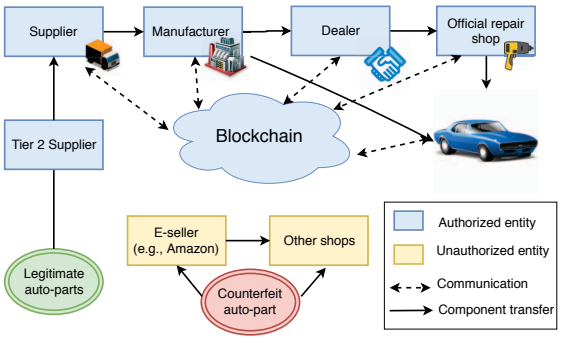

Fig. 2: Use Case: Supply chain scenario

Role	Action
Supplier	Add, Transfer
OEM	Mount, Transfer, Recall
Dealer	Transfer, Replace
Car	Check

TABLE I: Role-Action Mapping

they are put into markets and mounted into the cars.

B. System Assumptions and Threat Model

We consider two types of entities in the supply chain: *authorized* and *unauthorized* entities. Authorized entities are considered honest but curious as they represent entities in a consortium for supply chain willing to respect the consortium rules and yet eager to learn the business from competitors. On the other hand, unauthorized entities are considered fully malicious as they are not part of the consortium.

Regarding the blockchain $\mathcal{B}$, we trust the ordering service to correctly perform its operations (as whole) but we do not trust it for privacy. That is, the ordering service could be provided by either supply chain players or third party services as long as the correctness of ordering service is ensured. Entities such as suppliers, OEM and dealers will play as endorsing peers who maintain the same complete ledger. Moreover, we assume that endorsing peers can be fully malicious except OEM itself. Such trust model is enforced by endorsement policies and more details regarding it is are available in subsection D. We assume that each (sub)component has a unique identifier that cannot be detached/removed from the component. It should not be possible for the adversary to create new valid identifiers. The adversary may indeed collect used identifiers from working, recalled, malfunctioning or salvaged components; however, our design should ensure that the adversary cannot introduce counterfeit components from such identifiers.

C. Security and Privacy Goals

The system aims for the following security guarantees:

- *Confidentiality:* The adversary must not learn information for those objects that he does not own.
- *Authorization:* The adversary must not be able to execute actions that are not associated to its role.
- *Accountability:* If the adversary misbehaves while using an action associated to its role, the system must provide a proof of misbehavior.

We note that achieving these security and privacy goals is not trivial. The confidentiality goal is specially challenging in a supply chain. While the blockchain principle is to maintain a record where all actions are traceable, we aim to achieve confidentiality even from supply chain participants. For instance, the supplier may want to hide its data in the blockchain from other competing suppliers, and yet the supply-chain should provide a tracking mechanism for the objects in the supply. Moreover, accountability might seem easy to achieve as all transactions are recorded in the blockchain. However, it becomes challenging when confidentiality is preserved (e.g., some data may be encrypted).

D. Solution Overview

We illustrate the structure of our proposed blockchain for a representational automotive supply chain in Fig. 3. At the core of our solution lies a permissioned blockchain technology (e.g., Hyperledger Fabric), where we envision three endorser peers executed by the entities with roles supplier, manufacturer and dealer. Each endorser peer locally runs a copy of the *chaincode* and several chaincodes are in the system. The cornerstone of our solution is that each chaincode serves the authorization, confidentiality and accountability guarantees for a single action. For instance, the endorser peer run by the Dealer locally executes a copy of the chaincode that enforces that only components transferred to the Dealers are visible to this endorsing peer.

In the following, we present details about how our approach leads to provide authorization, confidentiality and accountability guarantees.

a) Authorization: We use multiple chaincodes to ensure authorization. The cornerstone of this approach is that each chaincode can have a different endorsement policy and thus different policies can be applied to enforce different business logic. We can thereby ensure that all transactions are endorsed by the correct set of endorsing peers. Moreover, since chaincode is an abstraction of the business logic and in some cases we want to keep business logic private, it is necessary that each endorsing peer only has the chaincode which he needs to endorse. For instance, in our example, suppliers are supposed to send Add-Component transaction to add components into system. However, without proper policies, everyone can endorse such transaction including dealers since they are also peers of blockchain although they have totally no knowledge about Add-Component. Therefore, we need to avoid it by setting up a policy enforcing "Only suppliers can endorse Add-Component transactions".

In a bit more detail, we define three chaincodes $CC1$, $CC2$ and $CC3$, for which we set the endorsement policies as follows. Endorsement policy of $CC1$ is set to *Supplier AND OEM* and it contains the business logic for the actions *Add-Component* and *Transfer-Component*. $CC2$ has the policy *OEM* and it includes the business logic for the actions *Mount-Component*, *Recall-Component* and *Transfer-Component*. Finally, $CC3$ implements the business logic for *Transfer-Component* and *Replace-Component* with the endorsement policy *OEM AND Dealer*.

There are some subtleties that need to be overcome to put this approach into practice. First, an endorsing peer must maintain a separate database to handle queries to each chaincode that it implements. Thus, our conception of multiple chaincodes requires multiple separate databases at each endorsing peer. Second, the different policies at each chaincode hinder the free invocation among chaincodes. Thus, communication among chaincodes must be carefully designed so that every chaincode can get its required data. For example, if a chaincode x depends on the functionality of other chaincode y, chaincode x must invoke a function in chaincode y to pass the corresponding information. This invocation will only be possible if their endorsement policies are compatible. Hyperledger Fabric has highly restricted policies regarding the invocation from a chaincode to another. We defer the discussion on this matter to section V. Finally, actions implemented at a given chaincode might require information only available in

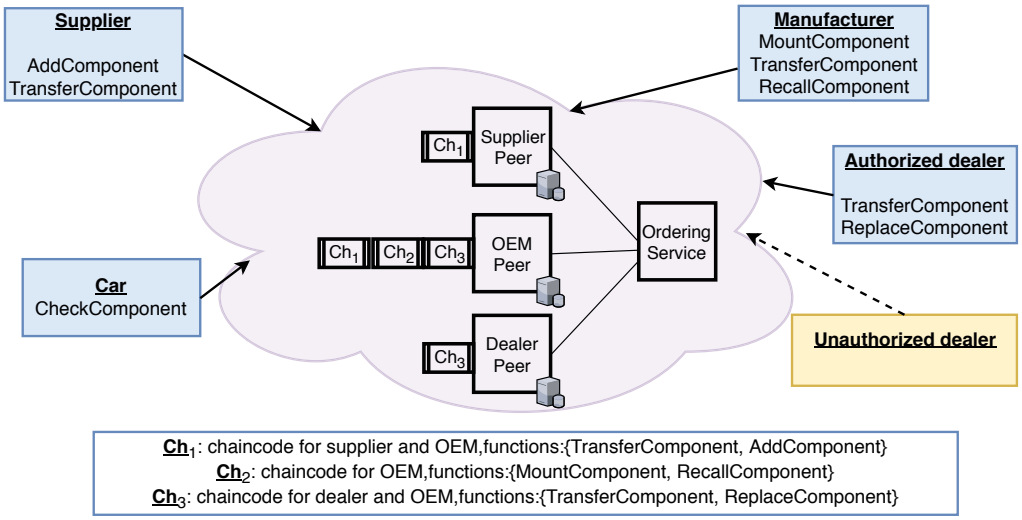

Fig. 3: Overview of our proposed structure of a blockchain for a representational automotive supply chain.

the database of another chaincode. An illustrative example of the aforementioned case is the *Mount-Component* operation. Assume that *Mount-Component* is invoked at $CC2$ to mount a component to a car. In doing so, $CC2$ must check that the component is delivered from the supplier and this info is only available in $CC1$ since it is relevant to *Transfer-Component*. As a result, $CC2$ will have to invoke $CC1$ to confirm availability of component and mark component record in $CC1$ to be "mounted".

b) Confidentiality: In Hyperledger Fabric v1.1 all endorsing peers share the same ledger, thus share the same view of the blockchain and database. In this state of affairs, we design our solution for confidentiality by encrypting appropriate parts of the transactions and the corresponding data. Intuitively, by doing that we can achieve different levels of confidentiality protection.

In a bit more detail, we ensure the confidentiality of the transactions in two steps. First, a client encrypts the transaction using symmetric encryption so that only the receiver could access the content of the transaction. Moreover, this ensures that the transaction is included in the blockchain in its encrypted form, so that other peers cannot see its content.

Second, the endorser peer decrypts the transaction and parses it according to the chaincode instructions. The response message from the peer must be also hidden as it goes over other entities in the architecture (e.g., ordering service and other peers). Therefore, the endorsing peer encrypts his response so that it provides confidentiality.

As a result, although blockchain is available to all endorsing peers, the contents are encrypted so only the ones with the appropriate confidentiality level can see the plaintext of transactions and ledger changes. On subtlety to consider here is that in Hyperledger Fabric 1.1, a transaction is composed of many fields such as chaincode name, parameter field and submitter signature. It is not necessary to encrypt all these fields and different levels of encryption could be achieved by encrypting different fields based on use cases. We discuss about this in more detail in section V.

Our current implementation is as follows: we pick AES as our encryption scheme and it is supported and implemented by Hyperledger Fabric Blockchain Crypto Service Provider (BCCSP). To achieve fundamental privacy, we propose to encrypt the "parameter field" of the transaction which usually contains sensitive data. The corresponding encryption key will be sent to peers through the "transient field" of a transaction so that only the receiver gets it. Besides, we also encrypt the read/write set of the endorsements so that finally all data recorded in the blocks are encrypted.

c) Accountability: Our accountability approach is based on two principles. First, the fact that every single transaction is logged in the blockchain (possibly in an encrypted form), ensures that each entity in the system can be challenged a posteriori for a proof of correct behavior. Second, even if the transaction data is encrypted, the encrypted data will be authenticated (i.e., accompanied by the corresponding signatures) so that certain party will be caught if it misbehaves.

As an illustrative example, after a component has been transferred to the OEM in our current architecture, the endorsing peer executed by the OEM will have access in the clear to this component during its entire life cycle. So our architecture design ensures the accountability of OEM. However, this also enables that OEM can check that all operations carried out are as expected. In particular, OEM stores all the credentials used for the encryption in the different chaincodes. Thus it is possible to ask the OEM for all his credentials and verify the correctness of its operations.

This can be extended to almost all supply chain use cases. There is always a party in any supply chain case who will act as the manager of the supply chain (e.g. OEM in automotive supply chain). This manager will be responsible for monitor-

ing all transaction flows in the whole supply chain. Although the data in blockchain is encrypted using different keys, this manager still should have access to all plaintext value and maintain the system's accountability. Since every transaction is recorded on a block and the manager has access to the plaintext transaction, if some peer misbehaves, the manager will notice it and the misbehaving proof (e.g., the transaction in a block) cannot be deleted.

In summary, we enforce business logic using chaincodes, and the access control is achieved by the design of multiple chaincodes with different endorsement policies. We leverage encryption to implement different levels of privacy protection.

E. Our System: Solution to Avoid Counterfeiting

In this section we describe different counterfeiting cases and explain how these can be prevented by our design.

a) From Unofficial Dealers: Previously, unofficial dealers can directly provide counterfeiting components to car owners during components replacements with or without car owners' admission. Car owners have no way to check the validity of components since there does not exists a trusted, shared log recording all valid components. However, in our design this counterfeiting can be easily prevented since now there is a distributed, trusted ledger recording all components information and cars are "self-aware" so they can trigger signals to the blockchain to check if the mounted components are (still) valid. Through our blockchain architecture we also build up records of the whole life cycle of components from being added until retired.

b) From Supply Chain Parties: With the help of hardware IDs like RFID [4] and PUF [3], components now have unique IDs which are helpful for tracing and management. But sometimes official suppliers can be malicious. No one stops them to generate components with same IDs and sell them to OEM or even unofficial dealers. This fraudulent behavior becomes impossible by using blockchain. Since now we have a single and shared ledger, replicated IDs will be immediately detected when transactions are received. Besides, since official suppliers have access to getting valid IDs, they can also generate IDs and sell these IDs to other counterfeiters to produce counterfeit components. This can also be prevented by blockchain since now the only way to add a component to blockchain is sending a "Add Component" transaction with the signature of corresponding supplier. Since counterfeiters are not players of blockchain, they cannot send or sign any transaction and thus they cannot add any components into the distributed ledger.

c) From Reusing Retired Components: Unofficial dealers can generate "valid" counterfeiting components by reusing IDs of retired components. Then unofficial dealers can just produce fake logs and provide fake components with valid IDs. However, this will never happen if blockchain is in use since once a component is retired, its record in the blockchain will be marked as retired forever given the append-only nature of blockchain and the guarantee that all previous blocks cannot be altered.

d) From Totaled Cars: Even with the use of hardware IDs, counterfeiting could still occur. Although unofficial suppliers have no access to generating valid hardware IDs, they can still get them by finding valid components in a totaled car, get their IDs and produce counterfeiting components with these IDs. This is hard to detect previous since components just lose tractability aftermarket. But with the help of blockchain, we can define the state of components to be one of three: "new", "mounted" and "retired". In this way, all components in totaled cars will be treated as "mounted" and only components with state "new" are treated as valid; thus, malicious suppliers cannot play any trick on totaled cars.

F. Security Discussion

Our system is resistant to malicious endorsing peers in both proactive and reactive manners. First, the business logic that a peer can do is enforced through chaincodes. For example, in our design, a Supplier has no access to all other operations except *AddComponent()* while *AddComponent()* has to be endorsed by both Supplier and OEM. Any invalid transaction will be rejected since the check on OEM will fail, and the malicious supplier cannot cheat. Besides, every malicious activity will be recorded permanently into blockchain in the form of transactions and the entities could be punished a reactive manner.

G. Extending The Structure

Although our solution illustrates how to build up a system with three endorsing peers, this can be easily extended to include more peers into the system. For each new $Supplier_i$, we just need to set up a new chaincode with the endorsement policy $Supplier_i$ *AND OEM* and use this chaincode to enforce the business logic of $Supplier_i$ such as *AddComponent*. Adding a new dealer is exactly the same as a supplier. However, if the added supplier or dealer does not introduce a new endorsing peer and wishes to employ a set of existing endorsing peers in a privacy-preserving manner, we may have to introduce fault-tolerant multi-party computation [21] among the endorsing peers.

Moreover, for a new OEM, we need to carefully build up the connection between new OEM and its suppliers using chaincodes and also the connection among OEMs if necessary. Besides, data standardization among multiple OEMs is a challenge itself and we leave it as our future work.

IV. A Usability Study

As blockchain started to get deployed, user interfaces for end users will be crucial to allow them to access distributed ledgers. This will indirectly also involve building the interface between the blockchain nodes and the blockchain applications. As one of the outcomes of the project, we have built a mobile app that interacts with our blockchain and offers transaction history for safety-critical automotive components to their owner. We also exhibited our end-to-end solution at an internal expo and collected extensive feedback. In this section, we describe our mobile app and its utility to the end users, and

offer feedback we received during the expo from participants at all ranks inside the organization.

A. User Interactions

The customers mobile phone can be used to learn information pertinent to the provenance of the vehicles components. Since the vehicle is "self-aware", it can periodically scan and verify the identities of its parts by acting as a node on the blockchain (see note below on other connection types). As a blockchain node, the vehicle identifies itself using a public address that is viewed by the OEM/Supplier blockchain consortium. The vehicle's public address is established beforehand using a Membership Service Provider. The vehicle can communicate this information to the customer through the vehicle dashboard and the mobile application. In the event that a significant change (part replacement, recall, collision) occurs, the vehicle can automatically notify the customer through the mobile application. This is useful in a variety of circumstances.

a) Counterfeit Detection: In the case where the airbag of a car is replaced, the vehicles airbag interface would be able to see that the original airbag has been removed and that a new airbag has been installed. The vehicle would query this newly installed airbag ID against the blockchain. Since this airbag ID was not introduced into the supply chain by the supplier or OEM, the query would return a warning to the vehicle to notify the customer that the part is unauthorized and a likely counterfeit. The vehicle could then automatically make the driver aware by sending a distress signal via the drivers mobile application. The vehicle could also send this signal to an authority and the OEMs support team. Furthermore, the vehicle reports this event to the blockchain, where the history and provenance of a vehicle and its parts are stored persistently.

b) Customer Verifies Parts Before Buying Used Vehicle: Another use case to consider is that a person desires to buy a vehicle and verify that the safety critical parts connected to the vehicle are legitimate. The customer would simply place her mobile phone over the vehicles identification sticker. Upon scanning the identification sticker, the mobile phone would send a query consisting of the VIN number to the blockchain (or intermediate server) to determine if the vehicles state is valid. The blockchain state for the specific VIN would then be returned to the mobile phone as a response. The state of the vehicle is stored as a value under the VIN key and consists of the open recall status and parts provenance. This information would be returned to the customer through the mobile application.

c) Recall Awareness: Once the customer has purchased the vehicle, the mobile application will periodically notify the driver of any important changes made to the blockchain that concern the vehicle. If, for example, a recall is made for a set of vehicles that have breaks installed from a given supplier and batch, and if the drivers vehicle falls within the affected vehicles, then the OEM can easily notify the customer through the mobile application. In this event, the driver will be notified in real-time, without having to wait for lengthy snail-mail nor disturbing phone calls. This personalized notification system will make the customer more aware, and less prone to overlooking the recall notification.

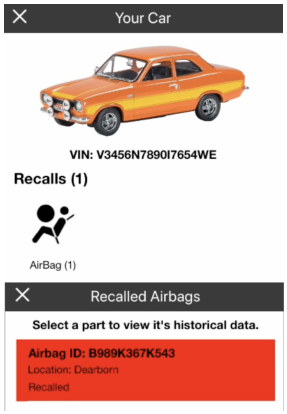

Fig. 4: Snapshots of the mobile application.

B. Feedback and Analysis

The mobile app was presented at an internal tech expo of a major OEM, attended by evaluators from a variety of organizations such as product development, manufacturing, mobility, purchasing, marketing, design, etc. 91% of these attendants believed the app is relevant to their respective sub-domains. While the revenue generation potential was not deemed to be high for this technology, its ability to enhance safety has the potential to greatly protect customers, enhance customer confidence and improve brand image. As one can deduce, this technology was perceived to be valuable for more than just airbag counterfeit detection, but also for other safety critical components and for other use-cases such as increased recall awareness and precision recalls. National Highway Traffic Safety Administration (NHTSA) issued recalls have the highest percentage of customers coming in for the part replacements (over 70%) as they are safety-critical. The scope of these recalls is not very precise as OEMs have limited control and real-time visibility of the supply chain, making this the most expensive type of recalls. The mobile app and its underpinning Blockchain platform proposed in this paper has the potential to provide precision recalls, by bringing together all the supply chain players to track and monitor safety-critical automotive components through its life-cycle, from initial assembly to aftermarket servicing. Lack of real-time visibility of the supply chain is a known issue in the automotive industry. Our solution can help enable real-time access to part traceability data, and can have smart contracts to automate data exchange in 'specific situations' such as counterfeiting and recalls, reducing cost and delays. The privacy preservation feature of our solution could help incentivize suppliers to join and share their sub-tiers data on the Blockchain network, which is otherwise difficult because of concerns about losing competitive advantage and cost margin. To that end, we expect

the privacy preservation feature to be a game changing agent in transforming automotive supply chains.

V. Challenges

Several challenges are inherent to the interaction between blockchain and supply chain. In the following we describe these challenges, some of which are from the nature of supply chain itself while others arise from the implementation subtleties of Hyperledger Fabric.

A. Privacy

Achieving strong privacy guarantees entails several challenges regarding data leaks, handling of meta-data and the communication patterns themselves. Overcoming these challenges is not trivial. [22]–[25] Using off-the-shelf techniques can assist to build stronger privacy protection at the cost of higher system complexity and reducing its efficiency. So a careful analysis and design is required to build upon the appropriate building blocks to maintain the balance between privacy and usability.

a) Privacy Issues Regarding Blockchain Data: The blockchain maintains a shared ledger that records plenty of information about the transactions such as the timestamp, chaincode name or the identity of the transaction's creator itself. This information is considered sensitive in many scenarios including supply chain, where the different participants wish to hide their business from competitors.

In this state of affairs, our proposed system provides a data confidentiality mechanism built upon symmetric-key encryption operations to protect privacy of the data in the blockchain (see Section III). One of its key advantages is its flexibility as it allows to define different privacy levels so that only appropriate information is encrypted, establishing thereby a required trade-off between privacy and usability.

For instance, in its simplest form, only the transaction's parameters field containing the invoked function and arguments can be encrypted. However, a transaction contains more information that should be appropriately addressed depending on the use case. For instance, the endorser signatures are a critical part within a block, since they indicate which peers checked and endorsed particular transactions. As an illustrative example, assume that only the OEM can mount components into a car and thus only OEM can endorse the relevant transactions. In such scenario, whenever an adversary observes that a transaction is endorsed by the OEM, the adversary will know that this transaction is calling "MountComponent" function with a high probability. Similar problems can also appear in relation to the "chaincode name" field in a transaction.

Staring from Hyperledger 1.2, there is a new feature called *private data collection*, which is designed to achieve similar confidentiality goals as the one described in this work. Private data collection provides a way to keep some data confidential among a subset of endorsing peers. Compared with our solutions, it requires communication among the subset of endorsing peers in order to share a secret key among them. This however might not be feasible in practice where different peers are run by untrusted parties within the supply chain. Moreover, the private data collection technique only provides restricted confidentiality (i.e., covering only partial transaction information) while our solution provides a flexible confidentiality mechanism.

b) Privacy Issues Regarding Communications: Sensitive data included in the transactions is not only at risk at the chaincode level, but also in the communication between clients and endorsing peers. If the client transmits the transaction in plane to the peer, transaction data is trivially leaked to eavesdroppers who can inspect all the traffic. This can be avoided with *authenticated* and *confidential* TLS channels that hides sensitive transaction data from prying eyes of adversaries inspecting the communication between users and endorsing peers.

However, although TLS is used, adversary can still detect the fact that sender and receiver are communicating with each other and this fact itself may reveal information. For example, assume that the adversary notes that a supplier is communicating with the OEM. Although the adversary has no knowledge of the transaction data itself, he can easily deduce that the supplier is transferring components to OEM with high probability. In this state of affairs, anonymous messaging system like Stadium [26] or mixing networks like Atom [27] may help to break the linkability between clients and the recipients of the messages they send.

c) Privacy Issues Regarding Ordering Service: By design, ordering nodes should not check the content of transactions, they should only order transactions and send them back to peers. But if an ordering node is curious, he can always try to explore the content of the transaction. Moreover, an ordering node can trivially link the content of a transaction and the identity of the client who sent such transaction. This linkability is considered an important privacy breach. In order to overcome this linkability issue, we propose to add two layers of protection against curious ordering nodes. First, encryption should be used to protect the content of transactions. Second, anonymous messaging systems and mixing networks can be applied here to break linkability between the transactions and their senders.

B. Multiple chaincode invocation

Hyperledger Fabric has strict restrictions regarding the invocation from a chaincode to another, which come mainly in the form of endorsement policies. The principle is that both the endorsement policy of the invoker chaincode and the endorsement policy of the invoked chaincode must be satisfied. All endorsement policies can be written as a combination of AND and OR clauses, and we study several chaincode invocation cases, summarize the general rules for endorsement policies and identify the challenges to realize them.

a) General rules for AND policy: Let chaincode $CC1$ be the chaincode being invoked with endorsement policy $\mathcal{E}_{cc_1}$: $\{P_1 \wedge P_2 \wedge \cdots P_i\}$ and CC be the invoking chaincode with endorsement policy $\mathcal{E}_{cc}$: $\{P'_1 \wedge P'_2 \wedge \cdots P'_i\}$. Then for the transaction proposal to be successful, the following conditions

must be satisfied: (i)$\mathcal{E}_{cc_1} \subset \mathcal{E}_{cc}$; (ii) $CC1$ *and* CC need to be installed in peer set $\mathcal{E}_{cc}$; and (iii) the transaction needs to be sent to all peers in $\mathcal{E}_{cc}$.

b) General rules for OR policy: Let chaincode $CC2$ be the chaincode being invoked with endorsement policy $\mathcal{E}_{cc_2}$: $\{P_1 \vee P_2 \vee \cdots P_i\}$ and CC be the invoking chaincode with endorsement policy $\mathcal{E}_{cc}$: $\{P'_1 \vee P'_2 \vee \cdots P'_i\}$. Then for the transaction proposal to be successful, the following conditions must be satisfied: (i) both $CC2$ *and* CC need to be installed in peers $\mathcal{S} := \mathcal{E}_{cc_2} \cap \mathcal{E}_{cc}$ or at least in any of the proper subsets of $\mathcal{S}$ and the transaction needs to be sent to all peers in $\mathcal{S}$ or its proper subsets; and (ii) the transaction needs to be sent to all peers in $\mathcal{S}$ or its proper subsets.

Intuitively, it is possible to expand this endorsement policy language with arbitrary combinations of AND and OR policies. We leave the research into this possibility as well as corresponding challenges as an interesting future work.

VI. Concluding Remarks and Future Work

To conclude, in this work we study the benefits and challenges of using blockchain to prevent counterfeiting in the presence of malicious supply chain parties. In particular, we show that the provision of a distributed and append-only ledger jointly governed by supply-chain parties themselves, by means of a distributed consensus algorithm, makes permissioned blockchains such as Hyperledger Fabric a promising approach towards mitigating counterfeiting. With the combination of blockchain and supply chain and "self-aware" cars, the life cycle traceability of components can be built up even in aftermarket. Authentication, accountability and different level of privacy protection can be also achieved. We also summarized the lessons we learned which can be applied to other supply chain cases and we study the privacy issues in Hyperledger Fabric. Besides, we provide a solution to support access control in Hyperledger Fabric by using multiple chaincodes with multiple endorsement policies. For this we study the current limitation of multiple chaincode invocation in Hyperledger Fabric.

In the near future, we plan to study involved cases regarding multiple chaincode invocation and give a general solution on how to design chaincodes with different endorsement policies so that endorsement rules are enforced meanwhile necessary communication among chaincodes are allowed. As we discuss data privacy should be treated as a significant property in supply-chain blockchains, and we also plan to try to provide feasible solutions maintaining the balance of efficiency and privacy. We will also dig more into supply chain scenario like multi-tier suppliers, multiple manufactures trying to find some common ideas applicable to all supply chain use cases.

References

[1] A. News, "Counterfeit parts flood china's aftermarket," Jan 2011. [Online]. Available: http://www.autonewschina.com/en/article.asp?id=6512

[2] OECD, "Trade in counterfeit and pirated goods," April 2016. [Online]. Available: http://www.oecd.org/governance/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, June 2007, pp. 9–14.

[4] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in *Service Systems and Service Management (ICSSSM)*, 2016, pp. 1–6.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf," 2008.

[6] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *EuroSys*, 2018, pp. 30:1–30:15.

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[8] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," *R3 CEV, August*, 2016.

[9] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy (SP)*, pp. 459–474.

[10] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, no. 11, pp. 15–17, 2016.

[11] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*, 2015, pp. 180–184.

[12] M. Pilkington, "11 blockchain technology: principles and applications," *Research handbook on digital transformations*, p. 225, 2016.

[13] D. Galvin, "IBM and Walmart: Blockchain for Food Safety," 2017.

[14] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[15] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, 2017, pp. 618–623.

[17] C. Mena, A. Humphries, and T. Y. Choi, "Toward a theory of multi-tier supply chain management," *Journal of Supply Chain Management*, vol. 49, no. 2, pp. 58–77, 2013.

[18] N. Delener, "International counterfeit marketing: Success without risk," *Review of Business*, vol. 21, no. 1/2, p. 16, 2000.

[19] D. Dob, "Permissioned vs permissionless blockchains: Understanding the differences," July 2018. [Online]. Available: https://blockonomi.com/permissioned-vs-permissionless-blockchains/

[20] I. B. Labs, "What are consortium blockchains?" Jan 2018. [Online]. Available: https://www.blockchainlabs.asia/news/what-are-consortium-blockchains/

[21] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract)," in *ACM STOC*, 1988, pp. 1–10.

[22] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2017, pp. 468–477.

[23] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 43–60.

[24] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2016, pp. 1392–1393.

[25] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *arXiv preprint arXiv:1506.03471*, 2015.

[26] N. Tyagi, Y. Gilad, D. Leung, M. Zaharia, and N. Zeldovich, "Stadium: A distributed metadata-private messaging system," in *Symposium on Operating Systems Principles*, 2017, pp. 423–440.

[27] A. Kwon, H. Corrigan-Gibbs, S. Devadas, and B. Ford, "Atom: Horizontally scaling strong anonymity," in *Proceedings of the 26th Symposium on Operating Systems Principles*, 2017, pp. 406–422.