



Reverse Traceability Framework for Identifying Liability of Crashes for Self-Driving Vehicles Using Blockchains

Samar Gupta, Indian Institute of Foreign Trade, New Delhi, India

 <https://orcid.org/0000-0002-8048-9031>

Jitendra Kumar Verma, Indian Institute of Foreign Trade, Kakinada, India*

 <https://orcid.org/0000-0003-4103-4218>

ABSTRACT

Modern vehicles are increasingly having a higher level of technology and automation. Humans are increasingly becoming dependent on these modern technologies to take decisions related to their lives and safety. Such an increasing dependence on automation raises an important question. If an autonomous vehicle (AV) meets an accident, who will be responsible? It is not the human driver, but technology that makes those crucial decisions on the road. This question is attracting considerable attention in the insurance industry because traditional vehicle insurance is based on the liability of human drivers, but in the future, vehicle technology will replace human drivers. Therefore, the vehicle manufacturer or one of its suppliers may be held responsible for the accident. This paper presents a crash liability identification framework that can identify who is liable if there is a crash or an accident of an autonomous self-driving vehicle. The use cases demonstrate that the proposed framework can be used by regulators to efficiently identify the liable party when an AV crashes.

KEYWORDS

Automotive Sectors, Autonomous Vehicles, Liability Framework, Reverse Traceability, Self-Driving Vehicles, Supply Chain Management

INTRODUCTION

Self-driving autonomous cars may change the way people travel. The study predicts that by 2025 8 million autonomous self-driving or semi-autonomous vehicles will be on the road¹. More than 80 companies are testing around 1,400 autonomous self-driving vehicles, meanwhile, 55% of Americans believe that most cars will drive themselves by 2029. This change will have far-reaching economic and social consequences. Modern vehicles already have advanced automation capabilities, such as

DOI: 10.4018/JGIM.329961

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

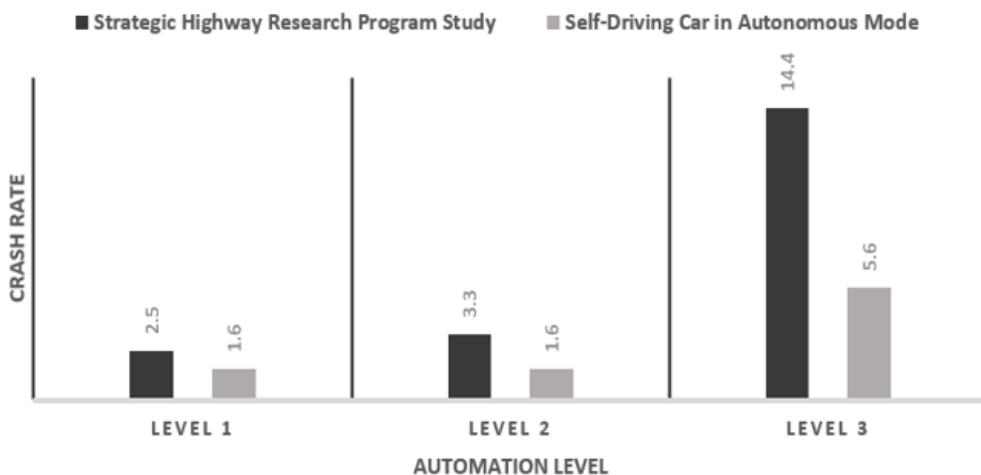
adaptive cruise control and lane-keeping assistance. If self-driving technology controls the steering wheel and pedals, then technology will also take critical decisions instead of human drivers. It is needless to mention that society accepts that humans are not perfect but expects self-driving vehicles to be flawless and must save lives through appropriate decision-making (Anderson et al., 2018). Its impact further widens as the traditional insurance industry is based on driver's liability, but self-driving vehicles no longer have a driver. So, who will be held responsible in the event of a crash? Self-driving vehicles are becoming a reality of the future; hence, these self-driving vehicles may expose automotive vehicle manufacturers and suppliers to significant liabilities in the event of a road accident or crash.

In addition, automotive manufacturers often end up recalling many parts if they do not identify with trust and transparency whether the issue is with a specific part, a specific supplier, or with all parts. Identification of any of the participants of the automotive industry incorrectly may cause major setbacks in terms of revenue earning. Thus, there is a critical need for backtracking in the automotive industry so that it can be identified who manufactured the defective/failed part and why it failed. Such backtracking will not only safeguard the many parties involved in the automotive manufacturing process, but also improve the overall quality of the manufactured part because allegations of manufacturing/supplying defective parts may be proven by available data, thus significantly preventing crashes in the future caused by similar reasons.

Each year, 1.35 million people lose their life in road accidents globally caused by human-driven vehicles² due to the relatively higher reaction time of human drivers. However, self-driving autonomous cars can theoretically react much faster. Also, self-driving autonomous cars are free from human distractions like texting while driving, looking at hoardings, sleepiness, and drunken driving. Figure 1 shows self-driving car accident statistics³ for the United States for the period of 2018-2022. Level 1 represents vehicles that are controlled by a human driver with some assisting technologies; Level 2 represents vehicles that have partial automation for acceleration and steering but the human driver also remains engaged; and Level 3 represent vehicles that have conditional automation where the human driver is not required to monitor the environment but should take control on notice. It is clearly visible from the data in Figure 1 that crash rates for autonomous cars are lower in all levels of vehicles.

In future cars, technology will make decisions for human life and safety, which will cause a paradigm shift in the responsibility of liability from the human driver to the vehicle manufacturer. To keep continuing hassle-free business, vehicle manufacturers or Original Equipment Manufacturers (OEMs) need to protect themselves from wrong/false claims of liability by some irrefutable data that

Figure 1. Crash rate per million miles



can meet the law of the land and upcoming regulatory compliances. However, existing information systems lack the production of such irrefutable data across the supply chain. Hence, OEM will find it difficult to fix the liability in the event of an AV crash. Traditionally, the flow of information in the automotive supply chain for human-driven vehicles is decided by requirements from vehicle manufacturers who focus only on the forward flow of information (Uzair, 2021). As implied by Figure 2, AV manufacturers need end-to-end reverse traceability to protect themselves from any wrong/false liability.

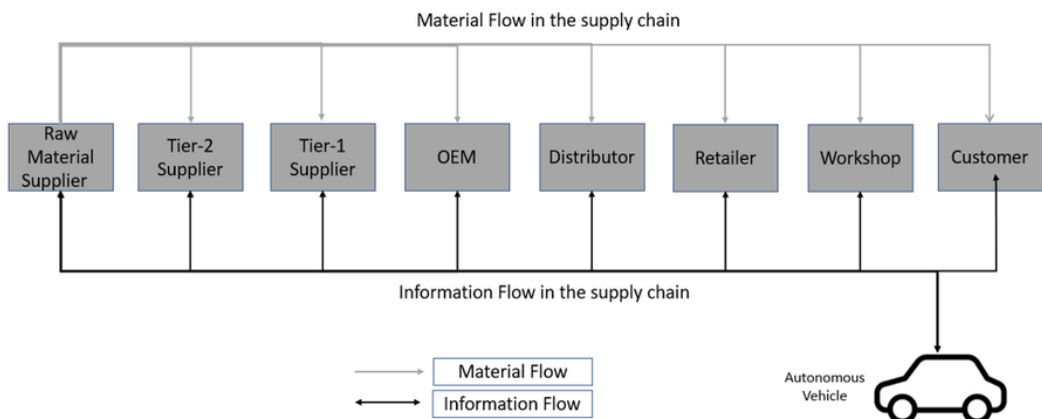
The above problem can be resolved by introducing blockchain-based reverse traceability in the information system for fixing the liability of car crashes. Reverse traceability using blockchain technology is a promising development in improving the trustworthiness, traceability, and transparency of products being delivered to customers (Lohmer & Lasch, 2020) as blockchain uses an immutable ledger of transactions in a distributed database (Nofer et al., n.d.) Thus, once a blockchain transaction is written by a party, it cannot be reversed or refuted. Centobelli et al. (2022) mentions how trust, traceability, and transparency are critical factors in designing blockchain solutions for circular supply. Based on the above background, we formulate and attempt to answer the following research question (RQ).

RQ. *“In case of a Semi-Autonomous or Autonomous Self-Driving Vehicle crash, how can blockchain technology be used to identify liability with trust, traceability, and transparency?”*

This paper presents a blockchain framework for identifying the liability in case of a crash of an automotive vehicle. We address the limitations of existing blockchain framework and present a 4-layer blockchain framework for automotive manufacturing supply chain. This framework can also be applied to semi-autonomous vehicles that have a high degree of automation. The proposed framework considers the inherent trust, traceability, and transparency of blockchain and offer agility by the cloud computing environment that is secure and can quickly scale to meet the needs of the industry. We testify real-world scenarios where an automotive vehicle crash occurs, and the airbags did not open. Data captured from the entire supply chain and vehicle is used to identify whether the customer is liable or whether any of the suppliers are liable. We present how the proposed framework may help in the identification of the liable party.

Blockchains use decentralized, distributed real-time ledger to record the transactions between the nodes. Hence, data retrieval via blockchains is a slow process which is a major limitation of blockchains. A modified blockchain storage and retrieval algorithm has been introduced in this

Figure 2. Automotive supply chain



paper to overcome the issue of slow information retrieval, thereby allowing for faster data queries. A cloud-based storage framework is suggested to make the deployment agile and subscription-based.

The main contribution in this work are the following:

- 1) We introduce modified storage and retrieval method for blockchains to support fast data query and information retrieval.
- 2) We propose a blockchain-based framework promoting trust, traceability, and transparency for reverse product traceability in self-driving vehicles.
- 3) We identify the data that are needed to be captured in the proposed blockchain framework.
- 4) We assess the proposed framework for fixing the liability for a car crash using two use cases of autonomous self-driving vehicles.

The remainder of the paper is organized as follows. Section 2 presents the review of the literature with theoretical background, Section 3 provides the proposed work, Section 4 presents experimental study and discussion based on use cases. Finally, Section 5 concludes the paper.

LITERATURE REVIEW

Safety-critical products need quality control and transparency during the manufacturing process (Chuan et al., 2005). This safety criticality is linked to the fact that society accepts that humans are not perfect but they expect self-driving vehicles to be 100% flawless so that human lives will be free from life-threatening dangers (Anderson et al., 2018). Reverse traceability using blockchain technology will be a promising development to overcome such life-threatening dangers by improving trustworthiness, traceability, and transparency in the automotive supply chain. These three factors help in determining the liability in case of an AV crash (Lohmer & Lasch, 2020). Traceability is described by quality standards such as International Organization for Standardization (ISO) 26262 and therefore it is mandatory for automotive companies that develop safety-critical systems (Maro et al., 2017). Compared to traditional contracts, smart contract-based agreements may be able to autonomously monitor and evaluate regulatory conditions and policies to ensure their sustainability (Fahimnia et al., 2015). There is a need to map reverse traceability-based liability, compliance, and control in the automotive industry with the three primary drivers of blockchain technologies which are trust, traceability, and transparency (Centobelli et al., 2022). Apart from this, it is essential to understand critical blockchain features that can help in implementing the liability framework for autonomous cars as well as the potential challenges against its adoption.

Impact of AVs on Current Liability Frameworks. In the event of an accident involving an AV, determining liability can be a complex and challenging task. Liability may depend on a variety of factors, including the cause of the accident, the actions of the vehicle's operator, and the behavior of other drivers and pedestrians involved in the incidents. As indicated in Figure 2, the complexity of the manufacturing supply chain is dependent on the large number of entities involved. In the event of a crash of an automotive vehicle, we must clearly identify which entity is liable. Most of the time, material flow is unidirectional, but information flow must be in both directions for transparency. Vehicle liability frameworks refer to the legal systems and regulations that determine who is responsible for damages or injuries caused by a vehicle. At present, vehicle liability frameworks are not based on data, and information systems are based on the supply chain. Instead of this, the liability framework is based on the traditional regulatory judicial framework and type of vehicle.

Negligence-based liability is the most common framework in which the person who causes an accident is held responsible for any damages or injuries resulting from the accident (Ilková & Ilka, 2017). To recover damages, the injured party must prove that the other driver was negligent or did not exercise reasonable care while driving. Strict liability framework holds the manufacturer or seller

of a vehicle responsible for any defects or malfunctions that cause an accident regardless of the other vehicle's driver being negligent (Alawadhi et al., 2020). Strict liability can also be applied to vehicle owners who allow unlicensed or unfit drivers to use their vehicles. Each party may be held responsible for their own damages and injuries under a strict liability framework regardless of who caused the accident. This framework was designed to simplify the claims process and reduce litigation, but it can limit the ability of injured parties to recover damages. It must be noted that liability frameworks can also vary depending on the type of vehicle involved in a crash, such as cars, trucks, buses, or motorcycles, as well as the use of the vehicle, such as personal use, commercial use, or government use. In general, the vehicle liability framework aims to ensure that those responsible for causing accidents are held accountable and that injured parties receive compensation for their damages and injuries. Thus, the current liability framework makes the driver or owner accountable for any damage or crash. The drivers buy the insurance for their vehicle and to protect themselves from third party liability resulting from a crash. The liability of vehicle manufacturers or OEM is generally limited to the warranty of the vehicle and replacement of the defective part.

AVs can be classified into five types based on the degree of automation (Rödel et al., 2014). These five types are as follows: (i) Level 1 vehicles which are controlled by a driver with some driving assist; (ii) Level 2 vehicles have partial automation and the driver is expected to continuously monitor and take over in case of a fault; (iii) Level 3 vehicles have conditional automation, which monitors the environment, and the driver is not required to monitor the environment but should take control on notice; (iv) Level 4 vehicles are highly automated but fully automated only for specific use cases; and (v) Level 5 vehicles have full automation where the driver needs to set the destination and the vehicle will make all decisions. The increased adoption of new technologies for AVs will impose a shift in responsibility for driving. Traditional drivers will make fewer decisions and critical decisions might be made by technology. Thus, liability in case of crash will shift from human drivers to OEM. This opens a new area of research on regulatory policies to determine who is liable if an AV causes damage to life and property. This also needs to be adequately supported by irrefutable data that is trusted and transparent.

Evolving Legal Requirements for AVs. There are many regulatory requirements globally that mandate reverse traceability. A blockchain-based system can accurately identify that only a specific part of a batch has a safety defect, or all the parts have a defect. Such information can help the vehicle manufacturer save themselves from legal liability and ensure compliance with the law. Manufacturers can save millions of dollars as they can use such information to identify a specific batch of vehicle that has a faulty part and thus do not have to recall thousands of vehicles.

Today, vehicles have much greater use for electrical/electronic components that detect and prevent collisions, lane detection, and departure monitoring, thus the quality of such components is critical. ISO 26262 covers the entire life cycle of such electrical and electronic components, from the definition of requirements, design development, raw material, manufacturing, operation, support, and disposal (Kafka, 2012). Safety must be managed throughout the supply chain; therefore, this ISO standard has a close relationship with traceability. USC Chapter 301 – Motor Vehicle Safety (U.S.) is an obligation for recall mechanism that started in the United States (Lee, 2017). Under this Act, when a vehicle or any of its equipment/parts is found to have safety defects or when a new vehicle fails to meet the safety standards, the manufacturers should notify administrative authorities and users of such a defective vehicle. The vehicle manufacturer also has an obligation to recall or repair the relevant vehicle free of charge. General safety regulations 2021 mandates that all new cars sold in the EU from 2022 must have advanced safety features (Seidl et al., 2021), including an event data recorder (EDR) or “black box” to record information in the event of an accident. China Automotive Industry Development Policy includes provisions to improve vehicle quality and safety, which requires all new vehicles to have a traceability system for tracking vehicle production and distribution including the source of the materials used (Black et al., 2020).

Critical Blockchain Features for Liability Framework. It is essential to identify critical features of blockchains to map with liability framework. Sunny et al. (2022) provides a high-level overview of blockchains, outlines their key features, and highlights their potential applications in multiple areas such as security and privacy in the financial sector as well as in the Internet of Things (IoT). They analyzed 750 papers published between 2015 and 2021 that discuss various applications of blockchain technology. This study was based on broader applications of blockchain in various industries, however, we went in-depth to identify the features relevant to our proposed framework in this paper.

The automotive supply chain has many participants including suppliers, OEMs, dealers, customers, and many more. It is important that participants can trace back the data with trust and transparency, which are available with blockchains as its inherent features. Blockchain has a distributed database in which each transaction is added after consensus between participants, thus blockchain provides a trusted immutable ledger of transactions (Nofer et al., n.d.). Decentralized and distributed ledgers make it easier for automotive supply chain participants to trust each other by recording and storing all relevant data and transactions even in the absence of a single authoritative figure. This is critical for tracking back the liability with trust in case of an AV crash (Centobelli et al., 2022). Traceability is the ability to trace products (such as authenticity, components, and locations) throughout the automotive manufacturing and distribution processes (Abeyratne & Monfared, 2016). Ali et al. (2021) examined that blockchains allow users to verify, maintain, and synchronize the contents of data that is copied by numerous users. Kuhn et al. (2021) propose a blockchain-based traceability architecture to achieve transparency in automotive. Security and transparency may additionally be enhanced using direct data inputs from IoT solutions, i.e., without dependence on input data coming from human intervention. Meanwhile, their work lacks the identification of critical data that needs to be captured. On the contrary, we identify the data to be captured in the proposed framework. Identification of the right set of data is critical to ensure that the volume of data remains low so that the overall cost of the solution can be reduced and the scalability of the solution can be increased.

In a typical linear supply chain, material or product flow from suppliers to manufacturers, manufacturers to distributors, distributors to retailers, and finally to customers. On the other hand, circular supply chain has a reverse flow from the customer to the supplier. This encourages manufacturers to retake, or reuse discarded or failed products and remake them into finished products. However, supply chain networks may be limited by visibility. It is evident that the reverse flow of the product and related information is also critical to customer feedback and identification of quality issues in the product. This reverse flow of information becomes even more critical in the case of self-driving cars due to the high dependency that human life has on them. In the event of a vehicle accident and associated liability, it is critical to have a solution that carries data from all participants to the supply chain in a trustworthy and transparent way so that source of failure can be traced quickly and efficiently.

Blockchain enables one to track and trace all past locations of raw materials and finished goods, history of custody, and which party added what value addition. All parties can use this information to transparently monitor and make decisions for optimizing operations in supply chain. Auto manufacturers can lose billions of dollars in costly recalls or counterfeit parts in the market. If a vehicle crash is attributed to a specific part, then automakers must accurately identify whether a specific batch of failed parts needs to be recalled or a larger set (Raj Kumar Reddy et al., 2021). An automotive supply chain may be very complex with each vehicle manufacturer having hundreds of Tier-1 suppliers and similarly large numbers of Tier-2 suppliers (Kuhn et al., 2021). The blockchain accurately records the value addition by all parties, and the auto maker has complete visibility on the entire network. In this way, automakers can identify the specific vehicles that have defective parts installed and issue recalls only for specific vehicles. Additionally, parts are tracked by Quick Response (QR) codes using the temper-proof blockchain ledger. Thus, the customer can quickly scan and identify whether a part is genuine.

Challenges to Blockchain Adoption for Liability Identification. Kouhizadeh et al. (2021) and Xing et al. (2021) carried out an exploratory study to investigate the obstacles that stand in the way of the acceptance and implementation of blockchain technology in the realm of supply chain management. They examined blockchain from an information systems and management point of view, performed a literature analysis, and identified key themes to investigate in greater depth. Their literature analysis reveals that there are not too many blockchain technologies ready for widespread adoption despite the technology offers promising possibilities for a wide range of uses across several different sectors.

Blockchain is an ideal solution for the storage of data in a transparent and decentralized way. Data is stored in blocks with a timestamp and each block is hashed. Additionally, each block is linked to the previous block. Thus, the blockchain cannot be altered. The blockchain implementation for manufacturing supply chain is different than cryptocurrencies as a huge amount of stored data needs to be retrieved from the blockchain unlike traditional databases, namely SQL, Oracle, etc. Traditional databases are designed for storing large amounts of data that can be efficiently retrieved using a query.

Blockchain has few challenges when it comes to querying the stored data as a blockchain instead of as a database. Query efficiency will decrease as the number of blocks grows. Querying data from blockchain can run into various performance and bandwidth issues and existing blockchain solutions have weak performance in data management (Xing et al., 2021). Faster query processing may be achieved by the method suggested by Xing et. al. (2021) where big blockchains are divided into sub-chains and various sub-chains relate to hash pointers to reduce the query time. Multiple transactions from the same source are merged and thereby reduce the cost of overhead and index construction.

The blockchain has built-in security, as discussed above. It is critical that the data on the blockchain is fed automatically by various IoT sensors or machines. This avoids human errors and builds greater trust in the system. The deployment of IoT for various blockchain solutions results in an expanded attack surface that requires end-to-end security mitigation (Minoli & Occhiogrosso, 2018). IoT sensors range from mission critical sensors in self-driving cars to business applications. The proposed framework will leverage trusted network devices or sensors located at participating entities. These devices create a chain of transaction blocks that contain the data. The information travels through the encrypted network to its destination in the cloud. The storage also has the integrity protection of blockchain. Thus, data are protected end-to-end, while in rest or while in motion. These devices also have a dual authentication mechanism to authenticate with the blockchain. Dual authentication ensures the integrity of the data. Blockchain helps IoT nodes in storing data records which can be used publicly and securely. In heterogeneous environments, IoT nodes need this method to communicate securely (Alam, 2019).

Meanwhile, traditional blockchain solutions require upfront investment and high computing power. This reason poses challenges for effective rollout in small and large scale, hence the automotive industry needs elasticity in solution when adding new participants. Such quick elasticity for entire blockchain infrastructure and data storage may be offered by cloud computing environment to leverage the benefits of scalability, agility, and security (Xue & Wang, 2022). The adoption of clouds is critical as most participants will not have sufficient resources to keep the blockchain infrastructure secured. It is critical that the infrastructure is secured in a uniform, consistent way. Additionally, blockchain participants might be added or changed over a period of time, therefore the need to store data can also vary dynamically, depending on the legal needs and the use cases. Henceforth, the cloud platforms provide a scalable and flexible model to increase or decrease the storage based on the need and resource demand, and thus proposed framework do not get locked-in with a high upfront investment. This also offers an operational expenditure (Opex) model to participants. Thus, the upfront cost will be lower, and participants will pay monthly/annually until they are part of the solution.

PROPOSED WORK

Proposed Fast Data Storage and Data Retrieval Method

To overcome the challenges of blockchain adoption in the automotive industry, we propose the modified blockchain storage and retrieval process that will be hosted in the cloud platform to achieve scalability, agility, and secure access. Figure 3 represents a simplified blockchain architecture for automotive supply chain which include the most critical blockchain components, i.e., data, the hash of the previous block, the hash of current block, the index, and the timestamp.

Optimized Data Storage Algorithm for Liability Framework. As the raw material or products go through various parties or entities involved in the process, data corresponding to specific entity or participant is generated. We define all entities involved in process as E , and obtain following equation:

$$E = E_1, E_2, E_3, \dots, E_n \tag{1}$$

Where E_1 represents one of the entities involved. Let us assume that E_1 represents ‘Customer’, E_2 represents ‘Vehicle’, E_3 represents ‘Workshop,’ and so on. Refer to Table 1 for the name of all possible entities.

Figure 3. Simplified blockchain architecture

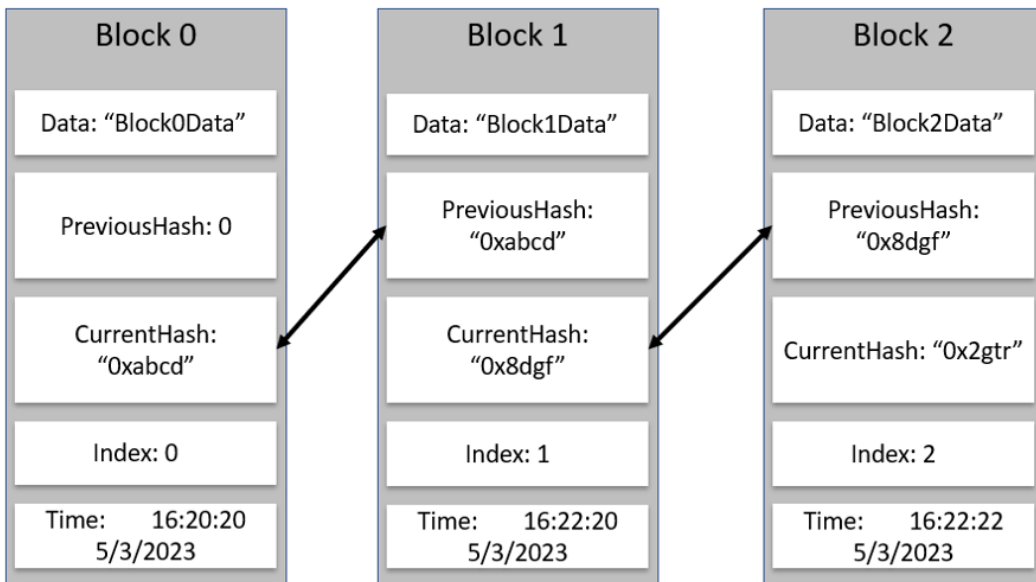


Table 1. Data to be captured in blockchain

Customer	Vehicle	Workshop	Retailer / Distributor	OEM (Vehicle Manufacturer)	Suppliers	Regulator
Repair and upkeep information	Speed, direction, navigation, response to obstructions, external environment	Service history, corrective actions recommended to customer	Test information	Which unit got which part	Location, batch, raw material mix, Quality test information, OE information	Approvals, roles-based access control, cyber security

Each entity or participant will have multiple production processes, and data will be captured for each process. We define all the processes involved as P and obtain the following equation:

$$P = \{P_1, P_2, P_3, \dots, P_n\} \quad (2)$$

Where P_1 represents one of the processes of a specific entity. Each entity has different processes, and the same process will differ between entities. For instance, the assembly process at E_1 might be very different than E_2 . Multiple data points will be generated for each process. These data may be generated by various sensors, controllers, smart machines, ERP, etc. We define all data generated in a specific process as D_1 and obtain the following equation.

$$D = \{D_1, D_2, D_3, \dots, D_n\} \text{ ledger of transactions in a distributed da} \quad (3)$$

Therefore, entity E_1 below will define complete process data. We define this as transaction $T(E_1)$:

$$T(E_1) = P_1 \{D_1, D_2, \dots, D_n\}, P_2 \{D_1, D_2, \dots, D_n\}, \dots, P_n \{D_1, D_2, \dots, D_n\} \quad (4)$$

Where $T(E_1)$ is the first transaction from entity E_1 .

For efficient data retrieval on the blockchain, we propose transactions from each entity to be stored on a separate sub-chain. This ensures that blockchain do not grow too big, which avoids linear runtime probing in hashing while searching as each entity will have a separate small sized sub-chain for enabling faster data retrieval. A blockchain is then formed by connecting the hash values of all sub-chains. This will ensure data integrity in the entire blockchain. Algorithm 1 shows how block is generated for each transaction in Entity E_1 and then how blocks are combined to form a $SubChainE_1$ for entity E_1 . Hash of $SubChainE_1$ is then combined with hash of pre-existing sub-chain called $SubChainE_2$ and $SubChainE_3$ to form a complete blockchain.

Figure 4 shows how IoT sensor transactions are used to create separate sub-chains for each participant and then combine them into a single blockchain. This methodology will help in efficient querying and retrieval of data from the blockchain.

Optimized Data Retrieval Algorithm for Liability Framework. We define three roles in the reverse traceability process for blockchain. These roles may be assigned to any of the blockchain participants or to a third-party. Figure 5 shows the three roles (Xue & Wang, 2022).

DR is the data requestor. DR will raise the reverse traceability request for a specific purpose. For example, if there is a crash due to a vehicle failure, the DR can be a regulator that wants to know which supplier is responsible for the failure.

1) DA is the data approval agency. DA will verify whether the purpose of DR is genuine and will provide the proof to DR . It will also be authorized to retrieve data from the blockchain. It will receive the proof with raw data from the blockchain. It will use the raw data to verify the proof. The raw data will not be passed on to DR .

2)

Algorithm 1. Procedure of Generating Sub-Chain for an Entity

```

Input:  $DataE_1$ ,  $PreviousBlock.Hash$ ,  $CurrentIndex$ ,  $CurrentTime$ ,  $SubChainE_2$ ,
 $SubChainE_3$ 
Output:  $BlockChain$ 
begin
var  $Block0E1 = Generate0Block(T1(E_1))$  {
/*  $Block0$  is called Genesis block*/
var  $PreviousBlock = 0$ ;
var  $CurrentIndex = 0$ ;
/* Index increases by 1 as compared to previous block*/
var  $CurrentTime = getDate\Time()$ ;
var  $CurrentHash = CalculateHash(T1(E_1), 0, CurrentIndex, CurrentTime)$ ;
return  $Block(Data, 0, CurrentHash, CurrentIndex, CurrentTime)$ ;
};
var  $SubChainE_1 = 0$ 
for each  $T$  do
var  $BlockE1 = Generate1Block(T)$  {
/*  $Block0$  is called Genesis block*/
var  $PreviousBlock = getLastBlock()$ ;
var  $CurrentIndex = PreviousBlock.Index + 1$ ;
/* Index increases by 1 as compared to previous block*/
var  $CurrentTime = getDate\Time()$ ;
var  $CurrentHash = CalculateHash(T, PreviousBlock.Hash, CurrentIndex,$ 
 $CurrentTime)$ ;
return  $New\ Block(T, PreviousBlock.Hash, CurrentHash, CurrentIndex,$ 
 $CurrentTime)$ ;
};
 $SubChainE_1 = SubChainE_1 + BlockE1$ 
for each  $E$  do
var  $BlockChain = CombineHash(SubChainE_1, SubChainE_2, SubChainE_3)$  {
var  $CurrentIndex = PreviousBlock.Index + 1$ ;
var  $CurrentTime = getDate\Time()$ ;
return  $New\ Block(SubChainE_1, SubChainE_2, SubChainE_3, CurrentIndex,$ 
 $CurrentTime)$ ;
};
};

```

- 3) DO is the owner of the blockchain data. DO is tasked with keeping the blockchain secure and ensuring that only trusted entities can add transactions in a transparent manner. It also ensures that only authorized DA can access the data.

DA uses the GET function to retrieve the data from DO . It can send data retrieval requests to its own node or to any other node with a public API. N_1 is the node from where data is retrieved, TE_n^P is the transaction containing defined purpose from an entity, and t_n is the time.

The pre-requisite to GET function is authentication between DA and DO . DA and DO , each have a set of public keys and private keys. Only DA has access to its private key. Any data it encrypts may only be decrypted using its public key. The same holds true for keys of DO . DA will sign the query using its private key and DO its public key.

Figure 4. Flow chart for adding data into blockchain

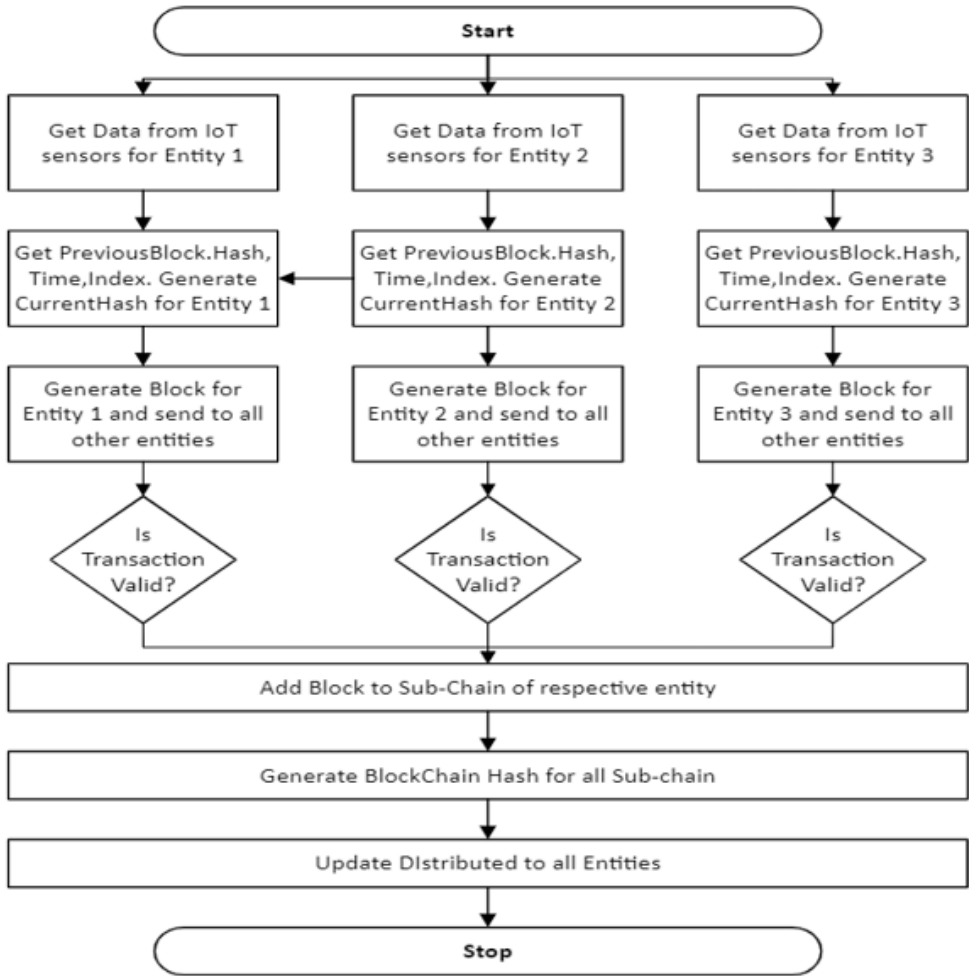
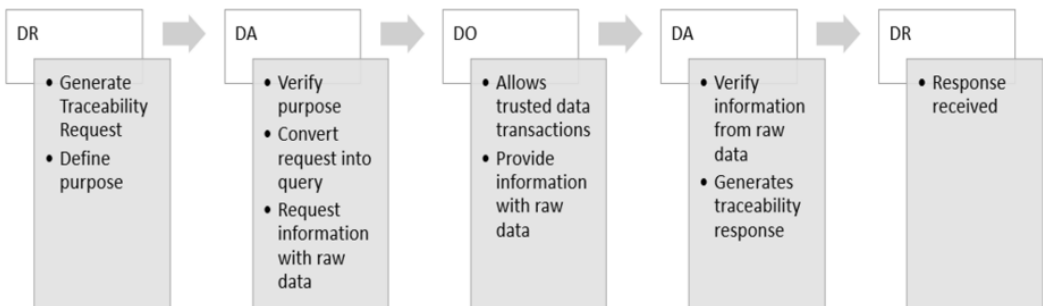


Figure 5. Roles in reverse traceability process



Furthermore, the query is passed to *DO* following which *DO* establishes authentication to allow trusted data transactions using its own private key and *DA*'s public key. Once the query is

executed on N_1 , it can generate a large set of non-related data. This data is used by DO to construct the proof. Proof, along with raw data is transferred back from DO to DA . Proof, along with raw data is signed and transferred back from DO to DA as *Traceability Response*.

Algorithm 2 shows how the raw data and proof are returned by DO as a traceability response based on a query received from DA . First, DO authenticates the received query from DA and then decrypts it. It then generates the data dump and proof from the blockchain technology layer. These are encrypted and sent back to DA .

The traceability response is decrypted by DA and it verifies the proof again. The verified proof is passed on from DA to DR . DR does not get the raw data.

Proposed Blockchain Framework for Crash Liability Identification in AVs

Autonomous Supply Chain and Relevant Data. A crash of a fully autonomous self-driving vehicle can occur either due to failure of parts or negligence by the customer, such as not doing maintenance service on time, etc. It is important to capture the information from various sensors in AVs as this can provide valuable data to identify the liability (Jain et al., 2021). AVs have many sensors that can provide data for adaptive cruise control, collision avoidance, object detection and classification, light or shade detection, parking assistance, navigation, and detection of road signs, traffic signals, or lanes.

In the event of an AV crash, identifying who owns the liability is not simple because of the huge number of parties involved in manufacturing process (suppliers, OEMs, dealers, customers, and many more) (Raj Kumar Reddy et al., 2021). Identifying the right set of data from the right party and the required interval is critical. Too much data can slow down the blockchain response, and it may become impractical to manage a large set of data. Additionally, capturing the right set of data is important so that liability ownership can be identified in the event of a crash. A blockchain framework

Algorithm 2. Procedure of Generating Proof by DO and Returning It to DA

```

Input: SignedQueryDA
Output: TraceabilityResponse
Begin
var QueryDA = DecryptQuery( SignedQueryDA ) {
/* Authenticated query by DA signed using private key of DA and public Key of DO */
var PrivateKeyDO = getPrivateDO();
var PublicKeyDA = getPublicDA();
return Decrypt(Decrypt( SignedQueryDA , PrivateKeyDO ), PublicKeyDA )
};
var DataDump = GetData( QueryDA ) {
for each n in TEnP {
var Data = getData( QueryDA ) /* Get data from N1 for the query*/
DataDump = DataDump + Data
};
};
var DataProof = verify( DataDump , EnP , tn )
/* Data Dump is used by DO to construct the proof for specified purpose*/
var TraceabilityResponseDO = Tresponse( DataDump , DataProof ) {
/* Authenticated query by DA signed using private key of DA and public Key of DO */
var PrivateKeyDO = getPrivateDO();
var PublicKeyDA = getPublicDA();
return Sign( Sign( DataDump , DataProof , PrivateKeyDO ), PublicKeyDA )
};

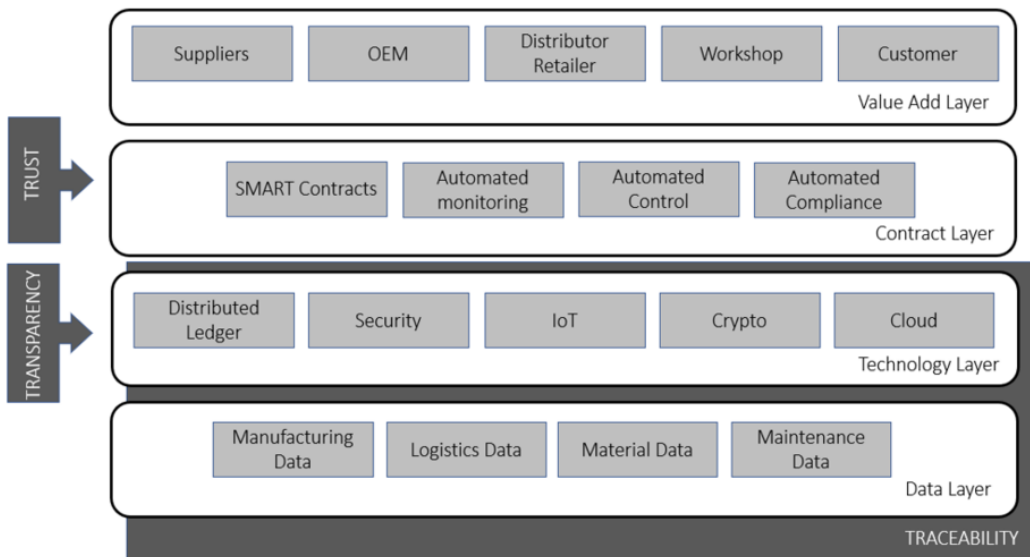
```

for the reverse traceability of parts of self-driving vehicles will capture the data indicated in Figure 6. Transactions between participants are automatically recorded in a blockchain implemented for supply chain network. Smart contracts are automatically executed using monitoring, control, and compliance data. As a result, it brings openness, which boosts partnerships (Aung & Chang, 2014). Each participant in the distribution chain will have faith in the integrity of the others and act accordingly because of this mutual trust. The supply chain response to changes in the network is enhanced by this level of confidence (Handfield & Bechtel, 2002).

Conceptual Framework. The full solution can be constructed using the following proposed framework:

1. **Value-Add Layer:** This layer includes parties such as raw material suppliers, vehicle manufacturers, distributors, retailers, workshops, customers, and AV. These parties will have access rights to add data to the blockchain but limited rights to retrieve the data back.
2. **Contract Layer:** This layer defines the purpose of traceability and brings TRUST to the overall framework. The layer maintains the authentication and provides a verification interface for proof. The contract layer requires support from the technology layer to execute SMART Contracts, for automated monitoring, control, and compliance. This layer directly interacts with the *DO* and the owners of production data.
3. **Technology Layer:** This layer includes technologies such as cloud, Crypto, digital ledger, etc. that help in execution of the contract layer. This layer is mainly responsible for generating the proof of traceability. It also performs the core function of privacy prevention. It has a data extraction and privacy protection engine. Data will be added to the blockchain while maintaining trust, traceability, and transparency.
4. **Data Layer:** This layer contains the raw data generated by each entity or participant. This raw data includes actual production, maintenance, and sales data. The raw data is also generated by IoT sensors, controllers, self-driving vehicles, and modern machines. Data input for this layer may also come from ERP systems, HRMS, and financial systems, which may vary between organizations.

Figure 6. Proposed blockchain framework for self-driving vehicles



Capturing the right data set as per the above framework is critical for identifying the party that is liable

EXPERIMENTAL STUDY AND DISCUSSION

We use the proposed framework to analyze how blockchain technology will help in identifying who is liable in case of a self-driving vehicle crash. We captured data from all the participants of the supply chain viz. Raw Material Supplier, Tier-2 Supplier, Tier-1 Supplier, OEM, Distributor, Retailer, Workshop, Customer, and Vehicles (table 2). The retrieved data can help in identifying the liable party for the two use cases mentioned below.

Figure 7 shows a supply chain operation along with the movement of automotive parts, and information in a blockchain solution. It also shows the information captured and how regulators can identify which party is liable in the event of an automotive crash. After implementing blockchain, all participants in the supply chain can freely exchange data. Each data entry is recorded in the blockchain digital ledger by IoT sensors in machines or cars. Each transaction recorded on a blockchain is handled by a smart contract. For agility and scalability, the solution is hosted over cloud platform to leverage the inherent benefits. The data captured by each participant may change depending on the regulatory policies. In the event of a crash, the regulator will be interested in knowing which part failed and who manufactured it. A vehicle manufacturer or supplier will be interested in knowing the root cause of the failure, so appropriate quality control measures may be taken into consideration during the manufacturing process. They will also be interested in knowing which customers have similar defective parts, as it will enable them to do a limited recall and save themselves from costly recalls of large sets of vehicles.

Use Case 1: Identifying Cause of AV Crash

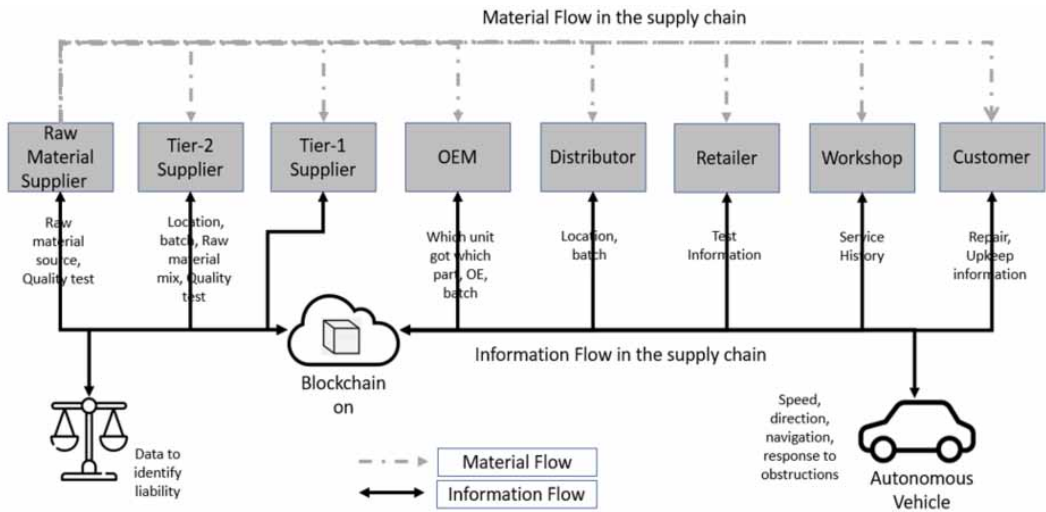
We consider a scenario use case where an AV crash occurred. A normal vehicle can crash due to large number of factors: (i) human behavior of over speeding, drunken driving, distractions for driver, influence of drugs, not following traffic rules, improper lane changes, not wearing seat belts, or not getting car serviced on time; (ii) technical issues like design defects and tire bursts; or due to (iii) environment conditions like weather or deadly curves on road⁴. These factors change dramatically in the case of AVs as technology is replacing drivers. The owner of a vehicle still carries the responsibility of getting the vehicle serviced on time and ensuring that passengers are using safety gadgets like seat belts.

Proposed blockchain framework can identify the cause for the following reasons of an AV Crash:

Table 2. Questions that will be answered from captured data

Customer	Vehicle	Workshop	Retailer / Distributor	OEM (Vehicle Manufacturer)	Suppliers	Regulator
Was maintenance done on time? How was the driving pattern during manual control?	Did the vehicle respond appropriately to speed, direction, navigation, obstructions, and environment? Did the vehicle raise an alert to customer?	Was the maintenance done by the customer on schedule? Any anomaly detected and reported to customer? What was customer response?	Was AV retested before delivery to customer?	Which supplier manufactured the failed/defective part? What was the data and time stamp, batch number and name of the supplier?	What was the mix of raw materials? What was the data and time stamp, batch number, name of operational engineer, and which machine used?	Do all parties regularly audit the controls as per law? Are they compliant as per law?

Figure 7. Flow of information in the circular supply chain



- 1) **Car driving pattern:** The technology layer in the proposed framework uses IoT to capture data and store it on a secure distributed ledger situated on cloud. IoT sensors in vehicles record speed, direction, and navigation. The contract layer may be used to identify whether technology was doing rash driving. It can also identify whether the car was following the traffic rules. Thus, regulators may identify whether a crash occurred due to the way the car was being driven.
- 2) **Technical issues:** The technology layer in the vehicle records the data related to all onboard electronic and electrical equipment. This will be used to determine whether the system worked as expected or had an unexpected failure of electrical/electronic equipment. Here, the contract layer will identify the failed component and its supplier. The supplier can use quality tests, batches, and raw material information to further identify the root cause and take corrective steps.
- 3) **Not using safety gadgets:** Life can be at risk if passengers do not wear seat belts or if they switch off other safety gadgets for collision avoidance. This information will be captured by the technology layer in the vehicle. Therefore, the contract layer will deliver automated warning to the passenger and inform the workshop.
- 4) **Vehicle not being maintained:** The service history and maintenance record from the workshop or service center will also be captured in the data layer that will help in identifying whether the customer maintained the vehicle as per the manufacturer's recommendation. The contract layer will deliver automated warnings to the passenger and can execute SMART contracts for terminating warranty of the vehicle.
- 5) **Environmental issues:** The technology layer will record the nature of roads, weather conditions, etc. Accordingly, the contract layer will send appropriate system-generated warnings to the customer. The workshop or service center will also use the contract layer for suggesting remediation measures to the customers.

Use Case 2: Identifying Cause of Airbag Failure in AV

We consider a scenario use case where an AV crash occurs and air bags did not open. Air bags can fail for several reasons, including the nature of the collision, defective airbag sensors, defective electrical equipment, not wearing seat belts, vehicle not being maintained through timely services, previous airbag deployment, previous water damage to the vehicle, etc. Proposed blockchain framework can identify the cause for the following reasons of Airbag Failure in AV:

- 1) **The nature of collision:** The technology layer in the proposed framework uses IoT to capture data and store it on a secure distributed ledger on the cloud. IoT sensors in vehicles record speed, direction, and navigation. The data layer may be used to identify if the driver was rash or aggressive. Thus, regulators may identify whether a crash occurred due to a driver's mistake.
- 2) **Defective airbag sensors or defective electrical equipment:** The technology layer in the vehicle records the data related to airbag sensors and electrical equipment. This data will be used to determine whether the system attempted to deploy the airbag and which module of electrical equipment failed. The contract layer will identify the failed component and its associated supplier. The supplier can use quality tests, batches, and raw material information to further identify the root cause and take corrective steps.
- 3) **Not wearing seat belts:** Airbags might not be deployed if passengers are not wearing seat belts. This information will also be captured by the technology layer in the vehicle. The contract layer will deliver an automated warning to the passenger.
- 4) **Vehicle not being maintained:** Vehicle maintenance is the customer/owner's responsibility. The service history and maintenance record from the workshop or service center will be captured in the data layer and will help identify if the customer maintained the vehicle as per the manufacturer's recommendation. The contract layer will deliver automated warnings to the passenger and inform the workshop.
- 5) **Previous airbag deployment or previous water damage to the vehicle:** The technology layer will record previous airbag deployments and if water came inside the vehicle in past. This contract layer will send appropriate system-generated warnings to the customer and workshop. The workshop or service center will use the contract layer for suggesting remediation measures to customers.

The transactions captured as per the proposed framework can identify the reason for a failure. Thus, these can be used to identify the party liable in case of an AV accident. Once the reason is identified, the data would be used to improve quality checks and processes.

Testing of Proposed Framework

Test cases contain a set of conditions that are checked for expected results from an input. We primarily focus on functional and performance testing. Meanwhile, additional testing may also be performed exhaustively such as security testing (for providing assurance that various entities can only modify or access the data as per our proposed design), unit testing (for testing the individual parts), UI testing (for ensuring UI is easy to use), integration testing (for ensuring all components work seamlessly together), and finally the user acceptance testing. Performance test cases enable us to identify the load that the system can take and plan accordingly. Table 3 lists the critical performance test cases for liability framework and Table 4 lists the critical functional test cases for liability framework. The identified test cases ensure that a production system built using the conceptual framework proposed above meets the functional and performance requirements.

CONCLUSION

This paper highlighted the changing scenario in the automotive industry and the way automotive manufacturers can protect themselves from potentially heavy financial losses due to liability claims. Automotive supply chains are complex with many suppliers, distributors, dealers, and workshops. Thus, it is critical that the cause of failure and associated liability is correctly identified. We proposed a crash liability identification framework based on blockchain. It can identify who is liable in the case of a crash of autonomous self-driving vehicles. Selectively captured data and SMART contracts also helps manufacturers to maintain the quality of the products. The proposed framework unites

Table 3. Performance test cases

Test ID	Condition	Steps	Input	Expected Result
1	Check number of transactions per second with 20 entities/participants	1. Define test transaction size 2. Use load testing tool to generate transactions 3. Number of transactions per second to continuously go up in increment of 10 4. Measure system load	Test load transactions with 20 participants	1000+ transactions per second with less than 80% system load
2	Check number of transactions per second with 50 entities/participants	1. Define test transaction size 2. Use load testing tool to generate transactions 3. Number of transactions per second to continuously go up in increment of 10 4. Measure system load	Test load transactions with 50 participants	1000+ transactions per second with less than 80% system load
3	Check number of queries per second with 20 entities/participants	1. Define test query size 2. Use load testing tool to generate queries 3. Number of queries per second to continuously go up in increment of 10 4. Measure system load	Test load queries with 20 participants	100+ queries per second with less than 80% system load
4	Check number of queries per second with 50 entities/participants	1. Define test query size 2. Use load testing tool to generate queries 3. Number of queries per second to continuously go up in increment of 10 4. Measure system load	Test load queries with 50 participants	100+ queries per second with less than 80% system load

Table 4. Functional test cases

Test ID	Condition	Steps	Input	Expected Result
1	Check that blockchain can add data from an entity	1. Data generated by apps or IoT sensors 2. Data transferred to blockchain cloud 3. Data stored in entity Sub-chain 4. Blockchain updated	Data from sensors or apps	Updated sub-chain and blockchain
2	Check that SMART contracts get executed when there is water damage to airbag	1. IoT sensor in car generates data for water damage to airbag 2. Data transferred over air to blockchain cloud 3. Contract layer generates automated alert 4. Alert delivered to owner by warning on car screen and SMS	Water damage to airbag	Owner receives a warning
3	Check that SMART contracts get executed when seat belts malfunction	1. IoT sensor for seat belt generates data 2. Data transferred over air to blockchain cloud 3. Blockchain generates SMART contract for workshop to recall car and fix the seat belt	Seat belt malfunction	Car recall by workshop for fixing of seat belt
4	Verify that DO can generate proof (traceability response) from raw data	1. Reverse traceability request received from DA 2. DO runs the query to extract raw data 3. DO generates proof from raw data	Reverse traceability request from DA	Proof and raw data for DA

the three main factors affecting circular blockchains (i.e., trust, traceability, transparency) with the futuristic reverse traceability needs of the automotive sector. Blockchain technology is critical to a liability identification framework for the automotive industry. The technology has certain data transfer speed limitations that can be mitigated using the modified storage and retrieval algorithm presented above. Trusted IoT devices will directly enter data into the blockchain ledger for maintaining trust and transparency in the overall system. Meanwhile, cloud will help in cutting down initial investment,

providing scalability, and a pay-per-usage linked subscription-based model for the participants. We have demonstrated that the proposed framework efficiently identifies a party liable for two scenario use cases: (i) Cause of AV crashes and (ii) Cause of airbag failure. Also, we presented a modified blockchain storage and retrieval algorithm that can speed up data retrieval while maintaining security.

This paper provides numerous contributions, but it has a few limitations as well. Firstly, the proposed work has been tested in two use cases only with limited testing methods. Hence, proposed framework may be adopted for multiple use cases to verify the applicability and robustness in different scenarios by applying other testing methods too. Secondly, Proof of Concept (POC) of the proposed framework for optimized blockchain storage and cloud-based agility may also be carried out as a future direction of work.

ACKNOWLEDGMENT

We would like to express our profound gratitude to Prof. O. P. Wali, the Head of the Research Division at Indian Institute of Foreign Trade, New Delhi, for his invaluable guidance, support, and encouragement throughout this research project. His insights and expertise have been instrumental to the success of this work.

COMPETING INTERESTS

The authors of this publication declare there are no competing interests.

FUNDING AGENCY

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), 1–10. doi:10.15623/ijret.2016.0509001
- Alam, T. (2019). Blockchain and its role in the Internet of Things (IoT). *SSRN Electronic Journal*, 5(1). <https://doi.org/10.2139/SSRN.3639000>
- Alawadhi, M., Almazrouie, J., Kamil, M., & Khalil, K. A. (2020). Review and analysis of the importance of autonomous vehicles liability: A systematic literature review. *International Journal of System Assurance Engineering and Management*, 11(6), 1227–1249. doi:10.1007/s13198-020-00978-9
- Ali, O., Jaradat, A., Kulakli, A., & Abuhlimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access : Practical Innovations, Open Solutions*, 9, 12730–12749. doi:10.1109/ACCESS.2021.3050241
- Anderson, J. M., Kalra, N., Stanley, K. D., & Morikawa, J. (2018). *Rethinking insurance and liability in the transformative age of autonomous vehicles*. RAND. doi:10.7249/CF383
- Aung, M. M., & Chang, Y. S. (2014). Traceability in a food supply chain: Safety and quality perspectives. *Food Control*, 39, 172–184. doi:10.1016/j.foodcont.2013.11.007
- Black, A., Roy, P., El-Haddad, A., & Yilmaz, K. (2020). *The political economy of automotive industry development policy in middle income countries: A comparative analysis of Egypt*.
- Centobelli, P., Cerchione, R., Vecchio, P. D., Oropallo, E., & Secundo, G. (2022). Blockchain technology for bridging trust, traceability and transparency in circular supply chain. *Information & Management*, 59(7), 103508. doi:10.1016/j.im.2021.103508
- Chuan, W. Y., Lim, J. C. H., Pasupuleti, A. N., & Liga, A. (2005). Safety critical components traceability. *IEEE Symposium on Product Safety Engineering*, 92–94. doi:10.1109/PSES.2005.1529528
- Fahimnia, B., Sarkis, J., & Davarzani, H. (2015). Green supply chain management: A review and bibliometric analysis. *International Journal of Production Economics*, 162, 101–114. doi:10.1016/j.ijpe.2015.01.003
- Handfield, R. B., & Bechtel, C. (2002). The role of trust and relationship structure in improving supply chain responsiveness. *Industrial Marketing Management*, 31(4), 367–382. doi:10.1016/S0019-8501(01)00169-9
- Ilková, V., & Ilka, A. (2017). Legal aspects of autonomous vehicles—an overview. *2017 21st International Conference on Process Control*, 428–433. doi:10.1109/PC.2017.7976252
- Jain, S., Ahuja, N. J., Srikanth, P., Bhadane, K. V., Nagaiah, B., Kumar, A., & Konstantinou, C. (2021). Blockchain and autonomous vehicles: Recent advances and future directions. *IEEE Access : Practical Innovations, Open Solutions*, 9, 130264–130328. doi:10.1109/ACCESS.2021.3113649
- Kafka, P. (2012). The automotive standard ISO 26262, the innovative driver for enhanced safety assessment & technology for motor cars. *Procedia Engineering*, 45, 2–10. doi:10.1016/j.proeng.2012.08.112
- Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics*, 231, 107831. doi:10.1016/j.ijpe.2020.107831
- Kuhn, M., Funk, F., & Franke, J. (2021). Blockchain architecture for automotive traceability. *Procedia CIRP*, 97, 390–395. doi:10.1016/j.procir.2020.05.256
- Lee, C. (2017). Grabbing the wheel early: Moving forward on cybersecurity and privacy protections for driverless cars. *Federal Communications Law Journal*, 69. <https://heinonline.org/HOL/Page?handle=hein.journals/fedcom69/&id=35&div=6&collection=journals>
- Lohmer, J., & Lasch, R. (2020). Blockchain in operations management and manufacturing: Potential and barriers. *Computers & Industrial Engineering*, 149, 106789. doi:10.1016/j.cie.2020.106789
- Maro, S., Staron, M., & Steghöfer, J.-P. (2017). Challenges of establishing traceability in the automotive domain. In *Software Quality. Complexity and Challenges of Software Engineering in Emerging Technologies: 9th International Conference, SWQD, 2017* (pp. 153–172). Springer International Publishing. doi:10.1007/978-3-319-49421-0_11

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things (Netherlands), 1*, 1–13. doi:10.1016/j.iot.2018.05.002

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (n.d.). *Blockchain*. 10.1007/s12599-017-0467-3

Raj Kumar Reddy, K., Gunasekaran, A., Kalpana, P., Raja Sreedharan, V., & Arvind Kumar, S. (2021). Developing a blockchain framework for the automotive supply chain: A systematic review. *Computers & Industrial Engineering, 157*, 107334. doi:10.1016/j.cie.2021.107334

Rödel, C., Stadler, S., Meschtscherjakov, A., & Tscheligi, M. (2014). Towards autonomous cars: The effect of autonomy levels on acceptance and user experience. *Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, 1–8. doi:10.1145/2667317.2667330

Seidl, M., Edwards, M., Hynd, D., McCarthy, M., Livadeas, A., Carroll, J., Martin, P., Edwards, A., Huysamen, K., Radcliffe, J., Pistak, K., & Appleby, J. (2021). *General Safety Regulation: Technical Study to Assess and Develop Performance Requirements and Test Protocols for Various Measures Implementing the New General Safety Regulation, for Accident Avoidance and Vehicle Occupant, Pedestrian and Cyclist Protection in Case of Collisions*. <https://trid.trb.org/view/1869691>

Sunny, F. A., Hajek, P., Munk, M., Abedin, M. Z., Satu, M. S., Efat, M. I. A., & Islam, M. J. (2022). A systematic review of blockchain applications. *IEEE Access : Practical Innovations, Open Solutions, 10*, 59155–59177. doi:10.1109/ACCESS.2022.3179690

Uzair, M. (2021). Who is liable when a driverless car crashes? *World Electric Vehicle Journal, 12*(2), 62. doi:10.3390/wevj12020062

Xing, X., Chen, Y., Li, T., Xin, Y., & Sun, H. (2021). A blockchain index structure based on subchain query. *Journal of Cloud Computing (Heidelberg, Germany), 10*(1), 52. doi:10.1186/s13677-021-00268-0

Xue, Y., & Wang, J. (2022). Design of a blockchain-based traceability system with a privacy-preserving scheme of zero-knowledge proof. *Security and Communication Networks, 2022*, 1–12. doi:10.1155/2022/3572404

ENDNOTES

¹ *The 6 Levels of Vehicle Autonomy Explained* | Synopsys Automotive. <https://www.synopsys.com/automotive/autonomous-driving-levels.html>

² Road Traffic Injuries and Deaths—A Global Problem
<https://www.cdc.gov/injury/features/global-road-safety/index.html>

³ 2022 Self-Driving Car Accident Statistics
<https://1800injured.care/self-driving-car-accident-statistics/>

⁴ Preventing Emergency Vehicle Crashes: Status and Challenges of Human Factors Issues <https://journals.sagepub.com/doi/epub/10.1177/0018720818786132>

Samar Gupta is a PhD scholar at the Indian Institute of Foreign Trade in Delhi, India. He is Vice President and Head-Group IT for Anand Automotive Group and SUJAN hospitality at New Delhi. He is Ex-Microsoft, Ex-Wipro, Ex-Stryker and Ex-Flex. He holds an MBA from Management Development Institute, India and attended a Harvard leadership program, an MS in Engineering from Oklahoma State University (USA), and a BE in Electronics and Telecommunications from Nagpur University (India). He is responsible for managing Digital Transformation and Information Technology across the Anand Group. The Group is comprised of 23 companies with \$2 Billion annual revenue and is currently the largest Tier-1 automotive parts manufacturer in India. His research interests are on how Information Systems can improve the overall circular supply chain and traceability in the automotive sector.

*Jitendra Kumar Verma is an Assistant Professor of IT & Knowledge Management Discipline at Indian Institute of Foreign Trade (Kakinada Campus) of Andhra Pradesh State of India. He received his M.Tech and PhD in Computer Science from Jawaharlal Nehru University, New Delhi, in 2013 and 2017, respectively. He obtained his degree of B.Tech in Computer Science & Engineering from Kamla Nehru Institute of Technology (KNIT), Sultanpur, in 2008. Over his short career, he has published numerous papers in peer-reviewed international journals and books with renowned publishers, conference proceedings papers, and book chapters. He has organized several international conferences, seminars, and workshops. He delivered numerous invited talks and seminars at various platforms of national and international repute. He authored one book, *Green Cloud Computing* (Lambert Academic Publishing, 2016), and edited five books, *Applications of Machine Learning* (Springer Verlag, 2020), *Computational Intelligence and Its Applications in Healthcare* (Elsevier Academic Press, 2020), *IoT and Cloud Computing for Societal Good* (Springer International Publisher, 2021), and *Advances in Augmented Reality and Virtual Reality* (Springer Verlag, 2022), *Cloud IoT: Concepts, Paradigms and Applications* (Chapman and Hall/CRC — Taylor & Francis Group). He is an awardee of the prestigious DAAD "A New Passage to India" Fellowship (2015–2016) funded by the Federal Ministry of Education and Research – BMBF, Germany, and German Academic Exchange Service. He worked at Julius-Maximilian University of Würzburg, Germany as a visiting research scholar during 2015-16. He has organized several international conferences, seminars, and workshops and delivered several invited talks. He is associate editor and guest editor of several international journals. He is also a member of several national and international societies/professional bodies, including ACM (USA), IEEE Industrial Applications Society (USA), IEEE Young Professional (USA), IEEE (USA), Institut De Diplomatie Publique (United Kingdom), Hyderabad Deccan ACM Chapter, Computer Society of India (New Delhi), and Soft Computing Research Society (New Delhi). Recently, He is elected as Senior Member of IEEE (USA) by high panel of academicians worldwide. He serves as a reviewer for various high-impact international journals, conferences, and workshops. His core research interests include Software engineering, Cloud Computing, Edge Computing, Blockchains, Internet of Things, Social computing, Image Processing, Artificial Intelligence & Machine Learning, and Soft Computing Techniques.*