Blockchain-enabled Supply Chain Security for Autonomous Vehicle Components

By Dr. Paulo Leitão

Professor of Informatics, University of Minho, Portugal

1. Introduction

With the burgeoning potential of autonomous vehicles, the automotive industry is rapidly being transformed from a human-driven car industry to a driverless one. Though many enabling technologies such as lidar, artificial intelligence, and machine learning contribute to the fast development of autonomous vehicles, security of their components is of utmost significance from technical, social, ethical, and legal perspectives. Security here not only deals with the physical security against unauthorized access, malicious modification, and counterfeit parts, but also assures the data integrity throughout the vehicle life cycle. Data integrity is critical when autonomous vehicles are communicating with other vehicles, passengers, or pedestrians and when they are interacting with the cloud and the backend system. Blockchain technology has been proven, due to its characteristics of decentralization, tamper-resistant, transparency, and cryptographic protection, to be a viable solution for ensuring the physical security and the data integrity of autonomous vehicle components. Moreover, since autonomous vehicles, as the nodes in the Internet of Things, need to exchange data among themselves, their components, and the backend systems, a lightweight, low-latency blockchain is needed, particularly for certain computing devices of autonomous vehicles.

1.1. Background and Significance

The centralized process is certainly verifiable, but it is expensive and cumbersome for all the parties involved. There have been instances in the past where untrusted agencies have been successful in obtaining certification for a component, especially when the certification agency's expertise is limited in the subject area. The agent could either be overwhelmed by the product design complexity or is simply untrustworthy. In both cases, the autonomous vehicle manufacturers would need extra insurance to protect themselves from potential liability. In this paper, the authors introduce operating a Blockchain-controlled Network of Trusted Autonomous Component Inspection and Application (B-COTACIA). There are several Blockchain protocols for handling supply chain information management and many for safety/quality certification and certain secure collaboration verification. In most cases, the motivations for many of the implementations in this space are cost, speed, and trust. This paper focuses solely on the issues of trust and security. We apply the Bitcoin consensus model to our supply chain information process.

In order to address these security challenges, this paper introduces the concept of Blockchain-Enabled Supply Chain Security for Autonomous Vehicle Components. The goal is to deploy a distributed and secure consensus of autonomous vehicle component information. The resulting autonomous vehicle's functionalities and performance are dependent not only on the software applications that govern the driver's actions but also on the quality and performance of component hardware. The impacts of software malfunction or hacking can be less dramatic if hardware components can only perform limited/authorized functionalities. However, if additional capabilities have been built into the hardware by design or accident, the potential damage to the system is much higher. There are methods that the autonomous vehicle manufacturer can use to verify this information. First, they can perform the component verification. This can be an expensive process, so it is typical to select an acceptable probability of correctness across multiple components of the same type. However, multiple unacceptable components can significantly diminish the overall system security and safety. Second, the tier-1 and -2 components may have been tested by a trusted testing agency. In this process, the performance and functionality can be verified through independent yet trusted testing methods.

Blockchain technology introduces the capability of distributed, secure, and transparent data transactions among multiple parties without central control. Over the past several years, the auto industry has been embracing autonomous vehicle technology. Companies such as Tesla, Uber, Lyft, Waymo, and General Motors are developing and testing autonomous vehicles. Autonomous vehicle manufacturers leverage additional software applications, hardware functionalities, and other supplied components on top of conventional automobile parts. The functionality and performance of those additional components are critical to the safety and security of drivers, passengers, and pedestrians. However, there are many cybersecurity and quality concerns that pose a risk to the secure and safe deployment of autonomous vehicles.

Cybersecurity and supply chain security have continued to be major concerns, primarily because of the complex interaction of hardware and software.

1.2. Research Objectives

The research addresses the question of how secure supply chains for autonomous vehicle components could be enabled and maintained. To do this, we examine the following related questions: Which state-of-the-art solutions apply to the security of the AD components supply chain? Does the automotive model represent a departure from state-of-the-art solutions? What are relevant differences? What security problems exist in the automotive supply chain? What is an overall security model, including the unique setting and participants that should be considered?

- Develop a framework for supply chain security in developing autonomous vehicle components. - Identify the actor roles and relationships in the supply chain and external interfaces. - Clarify the challenges of supply chain security within the development context. - Conduct a security and threat assessment of state-of-the-art standards and protocols. - Consider the intelligent system's design and components, the requirements of hybrids, intelligent transportation systems, and other applicable standards. - Identify potential vulnerabilities of the supply chain. - Consider the current solutions and limitations to state-of-the-art. - The unique challenges, the impact of the dynamic nature of the overall system, including the business model, do deployed measures, including incentive structures, encourage or deter misbehavior to achieve the objectives? - Design a blockchain-enabled, advanced persistence security solution based on an existing open-source framework. - Validate the performance and evaluate the solution using Use Case Evaluation, Threat Simulation, and Identify Key Performance Indicator metrics.

With the overview of the industry setting, the research objectives are developed. The key research objectives are as follows:

2. Autonomous Vehicles and Supply Chain Security

Ensuring the safe operation of the autonomous vehicle requires having equipment in place for fraud protection and anti-counterfeiting operations. Thus, there is a need not just to create a secure and dependable AV, but also to build vehicle accessories that are similarly secure and dependable. Take for instance a vulnerability in an internet-connected feature of the infotainment system in the Jeep Cherokee, which exposed the control area network (CAN) bus that can allow for a direct compromise of the engine, steering, brakes, or transmission. If these components are industrial-grade, the supply chain is likely to be a well-defined vendor source, and the vehicle manufacturer is likely to undergo security compliance for the vendor products. This poses a unique challenge in building an AV. The dynamic and diverse operational capabilities of this vehicle's systems necessitate that these vendor supply sources be dynamic and diverse, which offers several points of entry for attackers to compromise the vehicle. Vendors may adopt cyber supply chain practices or simply be negligent, presenting a significant vector for adversarial exploits. The challenge is multi-headed. The organization should regularly evaluate and monitor the vendors, seek third-party validations, check for certificate revocations, and maintain a robust list of verified vendors with integrity-proven products.

The hype behind autonomous vehicles (AVs) is real. AVs are expected to save lives, increase convenience for travelers, decrease costs for transport service providers, reduce time spent on transport, and increase economic efficiency. AV technology is not a clear path. Although self-driving cars have become a reality, safely deploying an autonomous vehicle that is capable of performing all driving functions in all relevant driving situations without human assistance is an intricate pursuit. As a growing and complex mesh of technologies and systems solve engineering problems and ease public concerns, we ought to remember that AVs demand a complex intersection of many technologies and technical advancements. That is, creating a safe autonomous vehicle is but a single aspect of a system of systems problem that must be overcome. For instance, the vehicle has to be capable of detecting any technological malfunction, and the community has to be equipped to rescue both the vehicle and its passengers.

2.1. Overview of Autonomous Vehicles

Autonomous vehicles, or self-driving cars, are built with embedded technology and software for monitoring, navigating, controlling, and driving vehicles without human intervention. Autonomous vehicles use various sensor technologies, e.g., LiDAR, radar, ultrasonic sensors, and cameras to capture the surrounding information and make driving decisions. Each sensor type has strengths and weaknesses. For instance, cameras identify reflectivity, shapes, and colors but cannot function properly in foggy, wet, and low-light conditions. LiDAR is robust in different lighting conditions but has a problem when a smudge or reflection is detected by the sensor. Radar is not affected by direct sunlight or lighting conditions, but may perform poorly in metal obstacles or concurrent traffic. The collection of sensor data enables the vehicle to make informed, flexible decisions and ultimately enables safe, efficient autonomous movement.

2.2. Challenges in Supply Chain Security

Larger-scale testing of complex electronic systems is unavoidably time-consuming, expensive, and still often the slowest part of the development and release process. Who pays for security testing, and when? How is the cost distributed? These testing-related upstream security dilemmas are particularly compelling in high-liability applications, such as automotive systems and medical device platforms, and in environments where multiple parties must collectively assure the behaviors of large complex systems that are formed by the integration of software and hardware from numerous sources. Complex products such as personal transportation systems for future cities and age- and disability-friendly transportation systems present further issues and concerns. High-liability concerns in aerospace and defense industries have long encouraged cross-industry security investment in the form of performance and safety standards, with the exact nature, rigor, and required regulatory status of such standards subject to complex national and international governmental debate. In automotive industries, issues such as uniqueness and customization of components and the importance of environmental and legal aspects cannot be understated. High-liability "intersourcing" concerns are also present in other domains, which further hampers security testing that may need to be repeated when laws or liabilities change. Miscellaneous additional security barriers with economic, engineering, social, and cultural sources also often hinder existing supply chain and provenance efforts. Overall, systematic frameworks for balancing risk, regulation, and third-party security validation have not kept pace with advances in cyber-physical system engineering.

As shown so far, various sources of evidence clearly underscore that practices for addressing supply chain security issues across firms, industries, and sectors must be subject to significant improvement. Conventional approaches to supply chain security often include varied kinds of organizational measures to prevent and control tampering with items in the supply chain, overriding existing security controls, and client-side attacks. Key measures typically include access controls, separation of duties, trusted business processes, trusted data processing, security integrity measures, and client-side attack controls. It has long been recognized that aspects of the supply chain security problem intersect with, yet are logically distinct from, facets of provenance, traceability, and chain-of-custody issues that have been the focus of seminal work in areas such as digital rights management, software and hardware trusted computing, and anti-counterfeiting technologies.

3. Blockchain Technology in Supply Chain Security

Supply chain security is one of the areas most likely to see significant impact from the adoption of the blockchain infrastructure, with industrial companies currently conducting several experiments. Over a third of companies surveyed in a joint UPS/Deloitte study were considering integrating blockchain technology into their supply chain. Today, the complexity and the interconnections of the supply chains, often come in global scale and unshared software applications, make data sharing and data consistency particularly challenging. Typically, supply chain business processes span across multiple organizations, and even between different portions of the same organization, there is no common system of record that spans the whole process. Between organizations, the lack of a common system of record leads to a situation where documentation relating to a process being completed by an organization is only available to them, preventing other involved parties from knowing whether that process occurred. For these reasons, a lack of true visibility into a supply chain can be among the largest challenges that it faces. Blockchain data shared across a specifically permissioned network is potentially a novel way of handling these information sharing issues. By redefining how various supply chain attributes are captured, managed, and validated, the technology has the potential to offer both an audit trail of immutable trust and enable an open way to reach informed decision-making based on common, agreed-upon data held by actors who are generally wary of sharing such data. Shaik, Mahammad, et al. (2018) explore granular access control in the expanding IoT landscape.

Blockchain technology, originally devised for cryptocurrency, is an enabling technology for many applications. It has the potential to redefine the way of recording, sharing, and processing data within and between enterprises. In general, blockchain technology offers a public digital ledger system that can store transactional records called blocks, taking the form of a database at multiple sites. Every block contains the digital fingerprint of the previous block, a timestamp, and the list of transactions. Blockchain technology offers the benefits of decentralization, securing the lifetime of data and making records visible to all members of a network. These unique features make blockchain a highly tamper-evident, verifiable, accessible, and transparent technology platform that is critical for many applications, such as supply chain security and identity verification, in addition to recording monetary transactions directly between participants.

3.1. Fundamentals of Blockchain

In most blockchain systems, all transactions in one block are encrypted to guarantee their confidentiality and integrity. Blocks are chained together through cryptographic hashing. A hash of a block is created by encrypting the contents of the block using a cryptographic algorithm in a manner that the output of the algorithm is fixed in size regardless of the contents. Therefore, this hash serves as a unique digital signature of the block. In this way, each block is entirely linked to a specific previous block as all blocks contain the hash value of the previous block. When properly integrated, this chaining mechanism has the following crucial effect: Any modification of the content of a given block results in the misalignment of the hash chains in all subsequent blocks.

Before we describe how blockchain technology can be applied to enhance the supply chain security, we first present the basic building blocks of blockchain systems. A blockchain is a particularly useful type of distributed ledger that enables untrusted parties to agree on a set of jointly managed records. It is secure and operates without a central authority that owns or has the ability to control the entire system. A crucial matter that such a system is aiming at is to prevent unauthorized changes to those records. A reasonable solution to this security issue is the sequential chaining of groups of records so that it is computationally impractical to modify entries once they have been created and associated with one another. Therefore, a blockchain conceptually consists of a sequence of blocks where each block contains a group of transactions or records and a reference to the previous block.

3.2. Benefits and Limitations in Supply Chain Security

Benefit: Where Chipscope and the DFI tools are integrated with the HDL development toolchain, and if binary difference debugging support is needed for upcoming FPGA or ASIC in-market chips, the somewhat specialized skillsets are likely to evolve within those organizations for the cloud-based storage and translation of the HFI toggle switch settings to DFIR SQL FIELDS of the on-chip modules. This could also couple the unique device identifier with the specific execution counter and other runtime logging metadata. Such a development could essentially give autonomous vehicle chip developers a warm fuzzy knowing their chips are a combination of the right-off and encrypted SWaP-C floorplan for proprietary performance throughput; runtime-access programmability with plausible deniability; a background of complete executable protection; unique SWaP-C cryptographic safe-steering control that exceeds the expected chip fabrication; and an insurance policy through offsite prototypical continuous security incident response.

Benefit: The processes encapsulating each system module or component with a physical blockchain QR-tag or using the proposed backend integration are significantly deterministic and thus secure. The overall security score of any SWaP-C is just shy of 100%. In other words, a hacker would need access to the complete relevant blockchain modules, the complete binary and assembly content of the encrypted modules, the encryption keys, and the exact placement of the modules within the physical SWaP-C using non-trivially side-channel access free technological and design obfuscation. This is a major impact because modern supply chain attacks against autonomous vehicles, such as the Fiat Cripto's 500 demo of drive-by vehicle hacking, could be detected even retroactively through Sidebandapi.io and obfuscated SWaP-C security score decrease within BlockchainDP. Such a physiological security score for SWaP-C is not brute forceable in human scale time.

This cryptography-based technological approach for supply chain security of SWaP-C components has a number of implications. The major contributions and some of the limitations of the technology are briefly discussed below.

4. Case Studies and Best Practices

Organizations that participate in the automotive sector must walk a fine line in developing and sustaining secure procurement networks. As automotive manufacturers demand tighter inspection and quality data flows, they run the risk of stifling innovation, driving unrealistic investment requirements or fewer players, and/or driving the selected participants out of business. Meanwhile, the participants involved in these supply chains face more and more kinds of tests, tracking, and inevitable interaction points with the supply chain security and its inspection requirements. This chapter discusses how they can shift to more secure, yet practical, procurement systems for the major, but even more so, for the complex and specialized components which are necessary to engineering success, and which possess complex reliability and security attributes that are not present in alternatives. These data show the promise of vouching for the supply chain and its merchandise through concrete and relevant parts and procurement supply chain security protocols.

Today's supply chain systems pose numerous challenges for companies, manufacturers, technology vendors, and others in the automotive industry. As it stands, our industry sells complex, interconnected systems, which are constructed from thousands of individual parts and subsystems, riding on global supply and distribution networks. In effect, we need to figure out how to bridge the gap between our current supply chain security practice and what the modern world needs. In particular, we need to find a solution that is effective, but practical to use.

4.1. Real-world Examples of Blockchain Implementation

A number of pilot projects or real-world applications have tried to use blockchain to build up transparency in supply chain scenarios. While these systems have demonstrated promising initial results and public acknowledgement, some are still isolated within a specific country or business group; others are directly contributed to by specific companies or supply chains. Such openness problems may restrict the scalability of the systems. To our knowledge, there is no public blockchain platform for an autonomous vehicle industry supply chain at present. It is an industry that has an urgent need for such a platform. We profile the following projects and analyze their weaknesses to be leveraged by a secure autonomous vehicle supply chain based on blockchain.

Blockchain has received significant attention in recent years in academia, as well as in industry, government, and the public domain. In the real world, its implementation is still very much in its infancy. To ensure the scalability of blockchain, the design of data access interfaces, consensus algorithms, and distributed databases requires innovation. Early blockchain systems only handled transactions involving assets and lacked support for further collaboration. Permission-based blockchain pioneered some valuable applications, like wholesaling of products, shipping cities, and others. However, these systems only supported partial transparency, and they are mostly targeted to general business scenarios. Permissionless ledgers can enable true transparency and are now actively used in real-world applications. Smart contract platforms, such as Ethereum, have the potential to support full automation and can enable crowdsourcing or oracle support for specific tasks. At times, however, privacy and security concerns limit the design of related smart contracts and their execution.

4.2. Best Practices for Integrating Blockchain in Supply Chains

The challenge in using blockchain in industrial sectors such as automotive to address unique security risks is to develop a model capable of incorporating these needs. As a result, we find few carefully-established practices and general consensus on those. This is especially critical as blockchain becomes more popular and organizations with nuanced supply chains begin integrating blockchain. Integrating the motivations behind blockchain and the functional capabilities alone are not sufficient to mitigate security risks in an OEM's supply chain. This challenge can be addressed by taking the lessons from blockchain use in other industrial sectors, which means determining an effective method of collaborating to outline the critical features to be considering in establishing best practices for blockchain supply chain development.

To effectively implement blockchain in an automotive supply chain, we now look to best practices and frameworks used in the industry today, such as those defined in ISO/TS 22163 Railway Applications – Quality Management System and ISO 44002:2019 – Collaborative Business Relationship Management Systems, as well as those used to promote these principles in other industries. Subsequently, we present four key best practice areas we believe are critical to harness blockchain's full potential in order to reach the desired goals. Collaboration will ensure that companies remain agile and relevant so that the right stakeholders and enabling technology are able to cultivate an environment of innovation, while sharing data. Additionally, we look for frameworks which empower the capabilities of blockchain technology and address topics of inter-organizational management, and early beginnings of blockchain integration. The aggregation of these best practices will promote a successful decentralized integration of highly complex functions.

5. Future Directions and Research Opportunities

As the proliferation of autonomous vehicles in various forms is inevitable given the potential safety, security, and environmental efficiency benefits, the development and deployment of blockchain-enabled security systems for auto-components holds great promise for the overall cyberphysical infrastructure reliability. However, the topic is vast, complex, and highly active. The research community is only in the mood for a harvest, but the complexities demand the careful design of education programs, the alignment of theoretical concepts with reality, and the continuous mentoring with industrial applications.

This article has made a case for the application of blockchain technology in providing security for auto-components and hence, autonomous vehicle supply chains. We proposed and developed systems that linked different auto-components to their digital twins through the use of Radio Frequency Identification (RFID) tags with blockchain to detect counterfeit in cellular chains. We demonstrated a case study for passenger vehicle tires and discussed mechanisms for building trust, fostering group decision, and integrating with Artificial Intelligence. However, the use of blockchain technology in this space is fairly new, and there are many compelling areas to work on. This section will enumerate some of these areas with implications to better access the technology for practical security in both vehicle components and beyond.

5.1. Emerging Technologies in Supply Chain Security

Autonomous supply chain security composes a Blockchain-IoT integration through which credibility and transparency can be increased. Especially in the context of the strategic position to integrate factory, car, and component suppliers in a supply chain, the emerging blockchain technology has the potential to integrate supply chain data created by different supply chain owners. In security and traceability in the supply chain, increased transparency ensures broader production quality monitoring and maintenance in the autonomous vehicle. Data from different supply chain owners become immutable and transparent on the blockchain. In addition, using a customized service, BPs could trust each other to trace the authenticity of the original Equipment Manufacturer (OEM). Use cases of BP memberships will be shown.

In the context of emerging technologies in supply chain security, the relevant areas include the Internet of Things (IoT), smart contracts, and blockchain technology frameworks. IoT, by its integration with the supply chain infrastructure, can provide tracking and monitoring of items sent through the supply chain, and smart contracts can assist in automation to facilitate contract implementation that is both credible and transparent. However, IoT and smart contracts' data transparency and credibility in supply chain security are not implemented in a way that is inherent in blockchain, and lack of clarity entails higher third-party risks.

5.2. Potential Research Areas in Blockchain and Autonomous Vehicles

Automotive Supply Chain Integrity Autonomous vehicles are complex, interconnected, and integrated subsystems with hundreds of small, medium, and large vendors having contracts with the system and the system integrator to deliver components tested and qualified to function as designed in the system. There are many blockchain solutions available for supply chain linkages between producers, distributors, and customers. However, one solution linked with a manufacturer leads to recurring business procurement of components utilizing the blockchain solution enabled security and validation proofs. This blockchain link connects the OEM periodic customer inspection, security assessment tools, and proof of theft, loss, or damage of the component. Multiple technology vendors specialize in security products associated with communication, access controls, monitoring, and analytics of data streams for Bentley's enterprise-scale industrial management and social responsibility requirements as part of the supply, design, and production activity. In turn, tracker component security in the enterprise with Tamr. However, consolidating into a single blockchain the need to mix track, proved security, and continuous authorization leads to a significantly different technical aspect than chaining public supportable transactions relative to the recipient's blockchain-linked license and security proof.

The various inherent characteristics of the blockchain, such as immutability, distribution, decentralization, anonymity, and transparency, are suitable for various use cases, particularly those involving entities with little or no trust associated with them interacting with extremely sensitive and private information. In the context of autonomous vehicles, a lot of research has been pursued in the technical enablers and societal/policy aspects involving private ownership and public use of autonomous vehicles. However, enterprise-level AVLs require somewhat different research motivations and usage models. Enterprises have specifically designed business models aiming to simplify and streamline a variety of applications, mainly for production, supply chain, and transportation of goods. With a plethora of components and sub-assemblies constituting the AVL, it is key to extend an existing remedy of blockchain and examine potential use cases.

6. Conclusion and Recommendations

There are several limitations that may reduce the effectiveness of the proposed approach. As mentioned before, this modification spends almost 30% more on gas, regardless of the difference in the cost between smart contract transactions and normal transactions, influencing the implementing effect. Moreover, the security and encryption method should be studied further in the part information proof phase to well protect the information. Unlicensed maintenance and improvements in the secure communication channel are also required between OSD and the maintenance center. More secure and role model designs could increase the robustness of the protocol. Precautions needed to be taken during the triggering top-scoring candidates, as observed in the system performance.

The scope and cost of counterfeit automotive parts have encouraged automobile manufacturers to explore new technologies that will improve the security of supply chain operations, ensuring that only legitimate parts are used in the production and maintenance of vehicles. This paper introduces a new approach in using blockchain technology to address the fake auto parts problem. The proposed approach may offer various benefits, including security and transparency of the supply chain. Security advances include protecting part information stored on the blockchain. Luckycoin, introduced to the car maintenance center, is engineered to improve the security of car part transaction units, so there is an immediate perceived benefit to auto manufacturers and car owners. Until the buyer and receiver get their products, the multi-signature smart contract will still keep the deposit.

6.1. Summary of Findings

This research affirms that, as distributed secure ledgers, blockchains can serve as excellent platforms for sharing verifiable attributes related to TACE component provenance. Pedagogical models of supply chain relationships and component identification methods were then developed and presented in a number of vehicle-centric scenarios. Use cases were presented and evaluated that demonstrate how blockchain features can support these foundational models relative to niche considerations in the TACE ecosystem. Upon evaluation and formal risk analysis, we were able to assert that the use of blockchain technology could introduce additional security protections which enable greater confidence in the authenticity of provenance and supply chain relationships of TACE components than are currently provided. This greater level of confidence would stem from structured proofs in the form of consensus-driven data transactions. This new technique of probing the provenance of an imported component, enabled through direct use of a distributed secure ledger, we claim is beneficial and long overdue. Moreover, implementing this extra level of verification should have minimal impact on system performance.

The research questions that drove this study sought to understand how blockchain technology, an emerging cryptographic innovation that can be used to establish and maintain immutable records of verified events in supply chain provenance, could be leveraged as a foundational layer in creating new security design elements for TACE components. First, the relevant literature was reviewed in order to define the main constructs regarding supply chain security. A further review of essential concepts related to blockchain technology was carried out to establish key understanding of pertinent technical requirements and constraints.

6.2. Recommendations for Industry and Policy Makers

6.2.1. Overcoming Technical Challenge The discussions in this chapter have shown that industry needs more technical solutions that operate on diverse and specialized autonomous components. This implies that libraries that offer these solutions, or common practices that are based on these solutions, have to make clear the suboptimal consequences of not using a comprehensive blockchain-enabled holistic approach.

6.2.2. Supply Chain Security Certification In recent times, there are a number of bodies looking at providing security certification for products, including ones that generate certificates that can be leveraged as attributes on blockchain devices. Certification bodies like IEC, NIST, EUROCAE and relevant national bodies should, in collaboration with standard setting organizations, ensure cybersecurity principles in those certification are based on sound cryptographic practices. With the increase in importance and complexity of digital components in industry devices, certification programs that perform third-party adherence verification and attestations for those principles should be created.

With the increasing level of connectivity and autonomy in autonomous vehicles today, there is a commensurate increase in the complexity and importance of hardware security. This chapter has discussed how blockchain-enabled provenance has been leveraged to provide trust in component integrity, the need for such verification in integrated autonomous components, and the deployment challenges and potential workaround. Based on the discussions, we make the following recommendations for industry and policy makers.

7. References

1. J. Wang, L. Peng, J. Wang and J. Wang, "A blockchain-based framework for reliable and cost-effective information sharing in a supply chain," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3680-3688, June 2019, doi: 10.1109/TII.2019.2902859.

2. L. Xu, X. Chen, and L. S. Wang, "A blockchain based approach to secure GPS data in intelligent transportation systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 9, pp. 3480-3490, Sept. 2019, doi: 10.1109/TITS.2018.2876329.

3. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in IEEE PerCom Workshops, Athens, Greece, 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917639.

4. R. Umar, S. A. Samad, S. S. Siddiqui, and F. U. Khan, "Blockchain for secure and efficient data sharing in V2X communication: A survey," in IEEE Access, vol. 8, pp. 156496-156516, 2020, doi: 10.1109/ACCESS.2020.3019036.

5. S. Khan, A. U. Rehman, and B. R. Ghani, "A blockchain-based framework for secure data sharing in vehicular ad-hoc networks," in IEEE Access, vol. 8, pp. 12341-12356, 2020, doi: 10.1109/ACCESS.2020.2964296.

6. S. Tanwar, A. Javaid, M. U. A. Khan, and K. Alam, "A blockchain future for internet of things security: A survey," in IEEE Access, vol. 6, pp. 32979-33001, 2018, doi: 10.1109/ACCESS.2018.2842684.

7. Tatineni, Sumanth. "Ethical Considerations in AI and Data Science: Bias, Fairness, and Accountability." *International Journal of Information Technology and Management Information Systems (IJITMIS)* 10.1 (2019): 11-21.

8. Vemoori, V. "Towards Secure and Trustworthy Autonomous Vehicles: Leveraging Distributed Ledger Technology for Secure Communication and Exploring Explainable Artificial Intelligence for Robust Decision-Making and Comprehensive Testing". *Journal of Science & Technology*, vol. 1, no. 1, Nov. 2020, pp. 130-7, https://thesciencebrigade.com/jst/article/view/224.

9. Shaik, Mahammad, et al. "Granular Access Control for the Perpetually Expanding Internet of Things: A Deep Dive into Implementing Role-Based Access Control (RBAC) for Enhanced Device Security and Privacy." *British Journal of Multidisciplinary and Advanced Studies* 2.2 (2018): 136-160.

10. Vemori, Vamsi. "Human-in-the-Loop Moral Decision-Making Frameworks for Situationally Aware Multi-Modal Autonomous Vehicle Networks: An Accessibility-Focused Approach." *Journal of Computational Intelligence and Robotics* 2.1 (2022): 54-87.

11. M. Alphand, N. Aitsaadi, and R. Langar, "Blockchain-based secure firmware update for the Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 1, pp. 380-390, Jan. 2021, doi: 10.1109/TITS.2020.2966879.

12. H. Zheng, W. Dong, H. N. D. Nguyen, Y. Li, and Z. Han, "Blockchain-enabled data marketplace with privacy-preserving and truth discovery," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1809-1822, 2020, doi: 10.1109/TIFS.2019.2936310.

13. S. S. Kanhere, A. Dorri, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2018 IEEE International Conference on Pervasive Computing and Communications (PerCom), Athens, Greece, 2018, pp. 618-623, doi: 10.1109/PERCOMW.2018.8482298.

14. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016, pp. 254-269, doi: 10.1145/2976749.2978309.

15. T. Hardjono, A. Lipton, and A. Pentland, "Towards a design philosophy for interoperable blockchain systems," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 617-624, doi: 10.1109/Cybermatics_2018.2018.00110.

16. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in IoT: Challenges and solutions," in 2017 IEEE International Conference on Pervasive Computing and Communications

Workshops (PerCom Workshops), Kona, HI, USA, 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917639.

17. Z. Yang, J. Hu, W. N. Gansterer, and R. T. Böhme, "Blockchain-based decentralized trust management in vehicular networks," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 1976-1983, doi: 10.1109/ICDCS.2017.265.
18. H. Zhu and Z. Wang, "A blockchain based new secure multi-layer transportation system architecture for future ITS," in 2019 IEEE Intelligent Transportation Systems Conference (ITSC), Auckland, New Zealand, 2019, pp. 465-470, doi: 10.1109/ITSC.2019.8917322.
19. X. Li, J. Li, H. Su, S. Zhao, and J. Zeng, "Design and implementation of secure data access control scheme based on blockchain in intelligent transportation system," in 2019 IEEE International Conference on Smart Internet of Things (SmartIoT), Tianjin, China, 2019, pp. 244-249, doi: 10.1109/SmartIoT.2019.00056.
20. M. Zheng, D. Yao, Y. Liu, and W. Liu, "Blockchain-based data sharing in intelligent transportation systems," in 2019