Azerbaijan Journal of High Performance Computing, Vol 6, Issue 1, 2023, pp. 77-90
https://doi.org/10.32010/26166127.2023.6.1.77.90

Smart Contract Implementation Using Blockchain IoV for Vehicle Accident Investigation

Gulfam Ahmad, Mariam Fareed

Ghazi University, Dera Ghazi Khan, Pakistan, hahmd@gudgk.edu.pk, mariamfareedit22@gmail.com

*Correspondence: Gulfam Ahmad, Ghazi University, Dera Ghazi Khan, Pakistan, hahmd@gudgk.edu.pk,

Abstract

Recent advancements in digital accident forensics, a conceptual evidence management paradigm developed using smart contracts and interplanetary file system in iov. This paper comprehensively summarizes the Smart contract implementation blockchain framework for vehicle accident investigation in IoV. We investigate comparing some review papers to find the classification of the smart contract. Using blockchain, evidence management provides an immutable and auditable method for investigating and resolving accident cases. Precisely we first investigate the security and privacy threats; therefore, Smart contracts provide effective access control for proof data and reports. On both the public and private Ethereum blockchains, the cost of setting up and executing transactions using smart contracts is assessed. However, we utilized the Inter Planetary File System most efficiently while minimizing memory and execution costs. Finally, we draw open research directions for building future digital-proof management.

Keyword: Blockchain, Smart Contracts Interplanetary File System, Internet of Vehicles, Accident Forensics, Digital Evidence, Access Control.

1. Introduction

Vehicle accident investigation and settlement are still difficult. Many cases reaming unresolved because there is not enough information about the accident. Investigation reports' validity is doubtful and accessible to manipulation (World Health Organization, 2018; European Commission, 2010). There are five stages to a mishap inquiry: reporting, on-site investigation, technological planning, expert recreation, and root-cause analysis. Then, the basics of traffic accident investigations, including the relevant laws and regulations and the national standards for accident categorization, are discussed. Information gathered from and about people is then described in depth, including the presence of proof, the identification and description of proof or victim interviews, injuries, the condition of drivers or pedestrians immediately before an accident, and the driving process and strategy (European Union, 2017). You must state the type of accident—such as a collision, head-on collision, car crash, or pileup.- as well as the occasion, setting, and motivation when describing an accident. Adjectives like fatal, severe, frightful, terrible, tragic, sad, dreadful, and horrible can describe how bad the accident was. Drivers: excessive speeding, reckless driving, breaking traffic laws, failing to read traffic signs, being tired, and drinking. Pedestrian: Ignorance, road crossing, moving on the carriageway, jaywalkers, and carelessness.

Analyzing every occurrence, even those with little bearing, is crucial for two reasons (World Health Organization, 2009). First, examining even little incidents can teach investigators vital lessons that can help them prevent worse incidents in the future. Second, conducting thorough investigations into every occurrence shows staff members and outside regulators that the business is serious about and persistent in pursuing its commitment to safety (Chauhanl, A., & Sharma, N., 2015). The investigator's job is to compile and arrange data to ascertain the incident's cause. The investigator should have sufficient expertise and competency to carry out the procedure with management's complete confidence and cooperation because facts are not always clearly defined, and proof can provide vastly different perspectives of the same occurrence. The investigator starts an At-scene investigation for the technical preparation of data and collects data from different sources to professionally reconstruct the authorized report, as shown in Figure 1.

The Internet of Automobiles (IoV) offers a variety of technical solutions to increase road safety. These solutions use a variety of sensors, including magnetic, radar, inductive loop, and RSU for collision avoidance as well as video and image-capturing devices. Effective Internet of Automobiles (IoV) solutions for road safety are made possible by the combination of sensor data with communication systems for efficient vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connections (Abdi, A. I., et al., 2020). The Internet of Automobiles (IoV) enables each vehicle to gather and distribute ITS-related information, such as data for navigation, logistics, and road safety, and to take in various information offered by other automobiles and devices online. IoV offers users considerable conveniences in this way (Ahmed, Z., Naz, S., & Ahmed, J., 2020). Adequate solutions for road safety are made possible by combining sensors and communication systems for effective communication between cars (Vehicle-to-Vehicle, or V2V communication) and between automobiles and infrastructure (Petroni, B. C. A., et al., 2020). IOV provides V2X; onboard sensors gather driving information from drivers, such as speed and location, and then send that data to surrounding automobiles. These automobiles' computers then evaluate the data to warn the drivers of potential dangers. However, it would not be restricted to inter-vehicle communication: Cars might also receive information from stop lights, effectively getting a countdown to when the light turn red. Smartphones or watches could also gather information from adjacent automobiles and broadcast it to notify pedestrians and cyclists who have chosen to join the V2X network. The term "vehicle-to-everything technology" describes the sensors, cameras, and wireless connectivity that enable cars to communicate in real time with their drivers, other cars, pedestrians, and roadside infrastructure like traffic signals (Athanere, S., & Thakur, R., 2022).

To execute data association, integration analysis, and privacy mining, enemies can exploit the information. IoV must offer effective and scalable techniques for message and vehicle authentication, user privacy protection, and secure message delivery (Benaissa, K., Bitam, S., & Mellouk, A., 2020). Unfortunately, the data collected could reveal highly personal details, such as the car's position, which could quickly raise privacy concerns among the users and discourage data sharing in IoV. Because of the abundance of data being transferred, duplicate communication and network traffic gridlock are possible. Given these constraints, collecting IoV data via a centralized computer is impractical, which suggests that traditional machine-learning approaches may not be suited to dispersed IoV with local features (Berdik, D., et al., 2021).

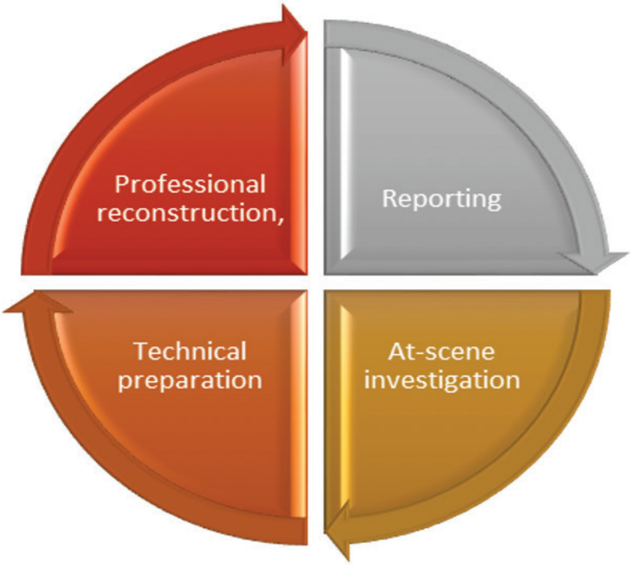

Fig. 1: Report creation steps diagram

1.1. Security Threats

Any situation or occurrence may negatively affect an organization's operations, assets, users, other organizations, or the country through a system, whether through illegal access, information deletion, disclosure, modification, or denial of service, for maintaining critical security updates to regulate the legitimacy and timeliness of the vehicle identity. The method for isolating and punishing unreliable or out-of-control vehicle nodes has yet to be developed. Vehicle systems can offer remote WIFI hotspots based on cellular mobile communication networks, which raises the possibility of an attack portal. Data and sound are transferred between car gadgets via microphones via the cellular mobile communication system. The automobile system becomes abnormal once an attacker bypasses the cellular mobile communication system. Devices can access the car's internal network via WiFi, allowing attackers to access the internal data of automobiles (Bhatti, F., Shah, M. A., Maple, C., & Islam, S. U., 2019). Since an authentication method is necessary for the Internet of Automobiles, it should also protect the privacy of the automobiles that provide and use the information. Vehicle owners, police, the transportation department, the legislation, insurance, vehicle manufacturers, and maintenance facilities. Are some of the various players involved? The names and functions of participants and authorities may change depending on the nation. In Iov, four crucial security fundamentals must be followed.

User Authenticity: A communication's origin could either be a trustworthy node or a malicious one. Determining if the node is trustworthy or malicious is the first step in enhancing the security of the IoV system. The system must be able to recognize malicious nodes from authorized ones and take action against the latter.

User Anonymity: It is best to remove any information that might identify the sender of a communication. Alternatively, the message's content should not make the sender's physical identity obvious. The IoV system must protect the identity of the message sender.

User Integrity: The information users send to one another should always be the same. It should be possible for the system to verify that the transmission was not interfered with in transit.

Low Overhead: Most IoV communications require quick responses. They are only useful if they reach the intended recipient in a certain amount of time. Because of this, the IoV system must prioritize security while ensuring overhead does not rise to the point that broadcasting takes longer and the system is no longer functional by the time it reaches its target.

1.2. Main Characteristics of the Blockchain

Decentralization, transparency, and tamper-proofs are all features of blockchain technology that could be advantageous. These features can improve many IoT applications, such as smart cars, intelligent towns, and healthcare systems, by facilitating secure data exchange without third-party participation and providing accountability and openness (Bosch EDR diagnostics, 2022; Cebe, M., Erdin, E., Akkaya, K., Aksu, H., & Uluagac, S., 2018; Chan, F. H., Chen, Y. T., Xiang, Y., & Sun, M., 2017).

All participants in a blockchain network can take part in verifying transactions, unlike in a centralized system where only the network leader can perform these actions.

- Traceability: Because every participant in the blockchain has a copy of the transactions in the ledger, an audit is simple to conduct. As a result, the participants in the blockchain network can confirm a particular blockchain address' data exchange (transaction). A timestamp is assigned to each record kept in a blockchain, ensuring transaction traceability. The blockchain protects user privacy and provides a semblance of pseudo-anonymity.

- Tamper-proof: All nodes in a P2P network agree on and validate new entries being added to the blockchain in a decentralized manner. To alter any entry in the blockchain would require the consent of the overwhelming majority of the network's users, making the blockchain unchangeable.
- Transparency: Since all participants in public blockchain systems, such as those used by Bitcoin and Ethereum, have equal user access, they can all take part in validating and adding new transactions to the blockchain. As a result, all participants in the blockchain network would be able to see the data recorded in the ledger.
- Secure: The blocks in a blockchain are each stored separately. Encryption is used throughout the blockchain network to ensure the safety of all communications. Since there is no centralized authority, one cannot simply add, change, or delete information about the group. In the blockchain, each record is cryptographically encoded to ensure that it is uniquely associated with the company. Separate from the code of the previous block, each new block also has its unique hash (Chang, W. J., Chen, L. B., & Su, K. Y., 2019). This brand ensures the encryption integrity of the interblock connections. Refreshing the data would necessitate altering each hash Number, which is impossible (Deflorio, F., & Carboni, A., 2022).
- Building on the ideas of its precursor, a decentralized payment system, Ethereum has created a worldwide computer network that links users to a community of decentralized apps (dApps), providing unparalleled speed, security, and user control. Ethereum builds upon Bitcoin's decentralized network and money, which were both significant first steps in the industry (Due to its cutting-edge combination of features, including smart contracts, Ethereum is used for various cutting-edge uses in fields as diverse as banking, online browsing, gambling, advertising, character the board, and production network directors. Ethereum's permissionless network, which allows the creation of applications without intervention from a central authority, creates a place for innovation. Thousands of decentralized applications (dApps) have been built on Ethereum, with millions signing up and billions of money being generated. We will look at some of the most prominent use cases on Ethereum (Dima, D. S., & Covaciu, D., 2017, October).

1.3. Smart Contract

Only blockchain technology makes it feasible for innovations like smart contracts. A smart contract is digital, kept within a blockchain, and enforces all aspects of the agreement using cryptographic code, as opposed to a regular, garden-variety contract, which defines the parameters of an agreement between parties and is frequently enforceable by law. In other words, smart contracts are just software programs that operate as their designers intended, just like all other software programs. Smart contracts may negotiate the terms of an agreement, automatically verify completion, and even execute the agreed terms without the need for a central body to certify if a party fulfilled their half of the bargain, as in Figure 2. This is all done through elegant math. Intermediaries like notaries, agents, and attorneys are useless in the age of smart-contract (Ethereum Gas Tracker, 2022). Smart contracts are short, immutable codes executed when specific criteria are met. Simple if/then statements are used to design smart contracts with functions and data saved at a specific blockchain address. Functions can be used to implement various functionality. The functions can be invoked using their addresses, as shown in Figure 2, To read and store data across the blockchain.

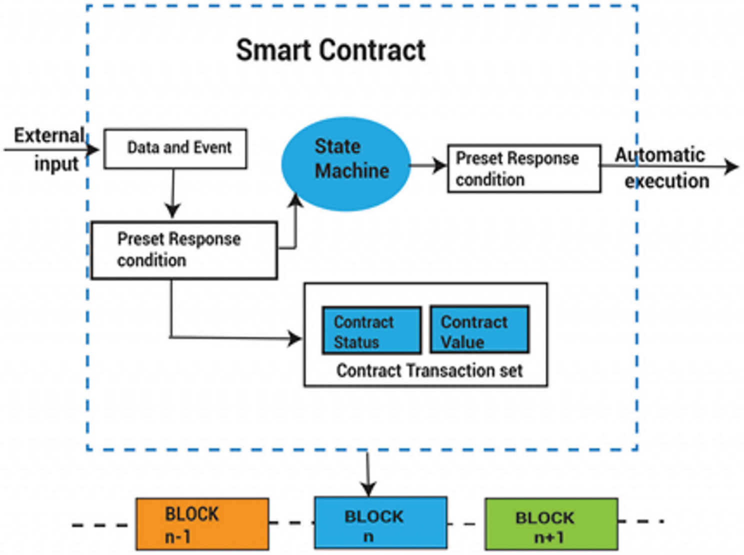

Fig. 2: Schematic diagram of the smart contract

When predefined circumstances are satisfied and validated, a network of computers does the necessary activities. After being created and made, the agreement rationale is sent onto the Ethereum blockchain. A record should carefully endorse each Ethereum exchange to be legitimate. Wallets manage accounts using key pairs, each consisting of a private key used to verify transactions and a public key used as a public identifier. Two types of Ethereum accounts are Remotely Claimed Records (EOA) and Smart Agreement Records (Ethereum Upgrade, 2022). A key combination limits the addresses of EOA accounts, which are determined by a checksum of the public key. Shrewd Pact Documents locations are chosen on the spot. Brilliant agreements and related capabilities can be gotten to and called utilizing the addresses. Every element and partner in the structure application is connected to an EOA and goes through exchanges utilizing calls to brilliant agreement addresses. Each capability can be carried out in a smart contract, and shrewd agreements can be reached by calling a particular function (Gerrits, L., Kromes, R., & Verdier, F., 2020, August).

1.4. Interplanetary Files System (IPFS)

IPFS stands for the Interplanetary Files System and is a decentralized, peer-to-peer file-sharing protocol that operates independently of the blockchain. You can use IPFS to store the media files for massive amounts of content, such as video and image files; blockchain is impractical and expensive. In the application being considered, accident proof includes videos and pictures gathered from compact cars, other cars, CCTV footage, and pedestrians who proofed the occurrence and recorded media. Additional evidence includes a large quantity of instrument data that coincides with the time and place of the event (Guo, H., Meamari, E., & Shen, C. C., 2019, March). IPFS, a distributed file-sharing network, provides an autonomous content capacity approach for off-chain data storage. This is contingent upon content disclosure, association, and content relating criteria. IPFS can store the media files and provide a unique substance location ID hash (CID) for the uploaded content to the blockchain. This cipher verifies the authenticity of the data and serves as a hub for retrieval. Each server in an IPFS network receives 256 kilobytes of data at a time. The hash of a file is a unique fingerprint that ensures the integrity of the data and facilitates its retrieval and transmission. To organize the content's connections, Merkle DAGs are used, while distributed hash tables (DHTs) are employed for content found (Guo, H., Meamari, E., & Shen, C. C., 2018, August).

IPFS allows for the safe and efficient transfer of data between blockchains. Compared to online storage, IPFS is a better option for storing information and helping fix issues related to centralized data centers. Pinning IPFS data prevents it from being deleted in the future. To keep data from being deleted by an IPFS node during routine maintenance, the data must be "pinned," or marked as essential, before the node saves it. The information on the needles may be wiped clean once the corresponding investigations have concluded. Intended-Participant File System (IPFS) is a blockchain-based secure and efficient file exchange solution. If you are having trouble with centralized storage, consider IPFS as an alternative to online storage for your material. IPFS data needs to be saved to prevent it from being deleted. To keep data from being deleted by an IPFS node during routine maintenance, the data must be "pinned," or marked as essential, before the node saves it. The information on the needles may be wiped clean once the corresponding investigations have concluded. There are paid services like Pinata for data maintenance and saving (Hamrouni, A., Ghazzai, H., Frikha, M., & Massoud, Y., 2020).

2. Background

Academic publications suggest putting vehicle data on the blockchain and analyzing how blockchain might be used in the Internet of Automobiles. One critical technology enabling the Internet of Automobiles to realize the Transport System's goal is blockchain. The Internet of Automobiles must have a safe, transparent, and unchangeable information exchange and storage infrastructure. Blockchain technology can record a vehicle's lifetime information, including registration, certification, insurance, and moving offenses (Holt, T., & Dolliver, D. S., 2021). The idea of putting away information related to an accident on a blockchain for post-mishap legal sciences and mishap remaking was initially brought up in Block4Forensic, perhaps of the earliest work to do as such. A scientific daemon that could recover information from EDR, BSMs, and onboard IOT sensors through CAN transport was wanted to be introduced in the OBU. The framework divided the data into maintenance, diagnosis, and event-related data. A fragmented ledger was suggested by the architecture to hold relevant data. Vehicular Public Key Infrastructure was used to ensure the confidentiality and authenticity of the communications (IPFS Pinning Service, 2022). An autonomous vehicle liability attribution framework built on a permissioned blockchain is being researched. Auto builders, proofs, service makers, warranty companies, government transferring authorities, and appropriate authorities were among the entities interacting inside the system. The blockchain was divided into two parts: a valuable component and an opinion part, used to establish entity responsibilities (Kaiwartya, O., et al., 2016).

The transactions were divided into four categories: event safety, primary proof, notification proof, and request proof. Event safety transactions determined event verification of a self-ruling automobile's behavior, direct proof transactions, proof report transactions, and request proof transactions were used to gain proof to provide a beneficial award (Khaliq, K. A., et al., 2019). After an accident, automobiles straightforwardly associated and adjoining automobiles check and save occasion information with the assistance of a progressively framed league of automobiles inside a similar vehicular organization. Upon the event of a collision, the elaborate automobiles broadcast a solicitation to frame a league of automobiles inside the organization. A subset of automobiles goes about as verifier automobiles to frame a league. The verifying vehicles were selected using a notoriety score calculated from the drivers' and detailers' histories with the vehicles in question. Due to a decentralized pioneer political decision computation, the verifier car with the highest standing score was designated as the lead validator and given the task of generating a new block of the incident. As soon as a new block is generated by the lead validator car, it is transmitted and recorded permanently (Khodaei, M., & Papadimitratos, P., 2015). In (Khoukhi, L., Xiong, H., Kumari, S., & Puech, N., 2021), a framework for episode location and permanent information stockpiling coordinated blockchain and AI advancements. RSUs were prepared to identify issues inside automobiles and to give area explicit driving-related alerts utilizing AI. Blockchain-based ciphertext strategy property-based admittance control (CP-ABE) was utilized to force access command over the occurrence information (Kim, S., & Kim, B. J., 2020). A system for incident detection and immutable data storage that integrated blockchain and machine learning technologies. RSUs were trained to detect issues within automobiles and to provide location-specific driving-related warnings using machine learning. Access control over the event data was implemented using ciphertext policy attribute-based access control (CP-ABE), which was implemented using the blockchain. The enforcement of access control over the proof data in these works depends on additional cryptographic techniques. Any of the frameworks do not cover the situation of a hit-and-run pedestrian. The works must detail the storage and execution costs of running and maintaining the apps. It is necessary to look at the design and implementation of intelligent contracts specifically geared toward acquiring and managing proof after incidents (Leal, F., Chis, A. E., & González–Vélez, H., 2020). The suggested approach investigates the most straightforward and effective method of obtaining and managing proof using the underlying IoV and Blockchain architecture without adding any further complexity. More articles are studied and described in Table 1.

Table1: Review

References	Authors	Smart Contract	Blockchain	IoV
Liu, M., Wu, K., & Xu, J. J. (2019)	Rodrigo Franco GonclavesW.	✓	✓	✗
Abdi, A. I., et al. (2020)	Adam Ibrahim Abdi	✓	✗	✗
Athanere, S., & Thakur, R. (2022)	Smitha Athanere	✗	✓	✗
Berdik, D., et al. (2021)	David Berdik	✗	✓	✗
Gerrits, L., Kromes, R., & Verdier, F. (2020, August)	Luc Gerrits	✗	✓	✓
Mihelj, J., Zhang, Y., Kos, A., & Sedlar, U. (2019)	Jernej Mihelj	✓	✗	✗
Oham, C., Kanhere, S. S., Jurdak, R., & Jha, S. (2018)	Zeli Wang	✓	✗	✗
Philip, A. O., & Saravanaguru, R. A. K. (2018)	Chao Wang	✗	✓	✓
Philip, A. O., Saravanaguru, R. K., & Abhay, P. A. (2022)	Abin Oommen Philip	✓	✓	✗
Cebe, M., Erdin, E., Akkaya, K., Aksu, H., & Uluagac, S. (2018)	Mumin Cebe	✗	✓	✓

3. Contribution to Study

In this paper, we present a comprehensive survey 0n the existence of a V2X-connected environment and the interoperability of cars, infrastructure (RSUs, CCTV), and pedestrian mobile phones. Data gathered and analyzed at the vehicle OBU; the cars can recognize and initiate an incident, such as accident and near accident scenarios. Through BSM communications, automobiles convey their states to nearby automobiles and RSU. The transmissions are believed to be encrypted and authenticated using a vehicle's public critical infrastructure (VPKI). When n incident has been started by the vehicle or one of the occupants, The driver can be responsive in documenting the occurrence for future guarantee payout hope in the event of casual accidents. The mobile phones of pedestrians are likewise presumptively skillful in being activated and sending proof data to RSU upon being struck by a car. The RSU is expected to be safe for collecting and storing proof data and then sending that data to the blockchain utilizing function calls to smart contracts. After an event in the V2X environment is detected, the included automobiles notify the RSU and communicate with RSU.After receiving an event notice, the RSU contacts nearby cars, other road users, and area CCTV to seek the transmission of more proof. The RSU compiles all relevant incident-related proof. The sensitive data collected as proof are sent to IPFS via RSU, and the CID for the file is then retrieved. The CID acts as the media file's associated content hash in the blockchain. The RSU uses specific intelligent contract function calls to write the proof to the blockchain. The occurrence is given a unique incident id, and the vehicle is of any automobile included summarized to that event. Using the RSU id, the event's location is found.

Placed on the automobile ID and RSU ID, participants can control who can access information about the incident. Identification of the vehicle aids in defining access controls for the owner, manufacturer, and insurance company engaged. The RSU id aids in identifying the relevant jurisdiction for the incident. All participants are

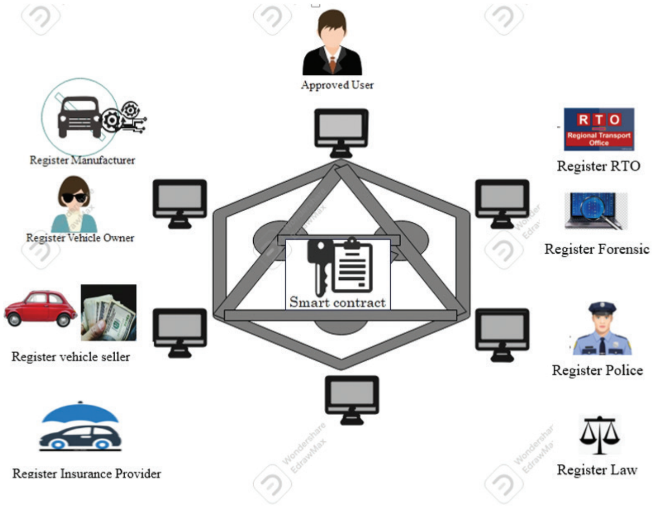

Fig. 3: Participant's registration in the smart contract

registered, verified, and allowed to use specific smart contracts. Through specific intelligent contract calls, the participants communicate with the blockchain and have access to the proof. Data related to proof access is restricted using utilizing related smart contracts for subsequent processing and settlements, as shown in figure3.

4. Open Issues

On the Ethereum network, the computational power required to complete transactions is measured in gas units. The number of Gas units needed to complete a transaction is preset and stays constant regardless of the tasks. We contrast how the application is implemented on the public and private Ethereum blockchains. For both options, the intelligent contract sense is the same. Further cryptographic measures are needed to secure the approach control because all proceedings on the public blockchain are transparent. Each transaction conducted on the open Ethereum network has a cost that must be paid in ether.

Conclusion

This work covered the potential for proof management and collection after an accident in a V2X context. Participants' roles, responsibilities, and access controls regarding the incident data were discussed. Many approaches to using smart contract functions to transfer vital and supplementary alternate data gathered by RSUs to the blockchain were investigated. For participant registration and each function carried out by the participants, the intelligent contracts' execution costs and transaction sizes were built and assessed. Implemented and compared were separate smart contracts since using chain storage on IPFS. The most effective method was found to be storing all incident-related data. Similar benefits were seen for storing additional proof from compact automobiles, security cameras, and other road users. It was determined that it was cost-effective to prefer off-chain storage of some data on IPFS. Other cryptographic mechanisms are needed, To establish access control on proof data. As automobiles become connected in the future as a component of the intelligent transportation vision through technologies.

References

Abdi, A. I., et al. (2020). Blockchain platforms and access control classification for IoT systems. *Symmetry, 12*(10), 1663.

Ahmed, Z., Naz, S., & Ahmed, J. (2020). Minimizing transmission delays in vehicular ad hoc networks by optimized placement of road-side unit. *Wireless Networks, 26,* 2905-2914.

Athanere, S., & Thakur, R. (2022). Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing*. Journal of King Saud University-Computer and Information Sciences, 34*(4), 1523-1534.

Benaissa, K., Bitam, S., & Mellouk, A. (2020). BSM-data reuse model based on in-vehicular computing. *Applied Sciences, 10*(16), 5452.

Berdik, D., et al. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management, 58*(1), 102397.

Bhatti, F., Shah, M. A., Maple, C., & Islam, S. U. (2019). A novel internet of things-enabled accident detection and reporting system for smart city environments. *sensors, 19*(9), 2071.

Bosch EDR diagnostics (2022). Bosch EDR diagnostics. https:// cdr. boschdiagnostics.com/cdr/.

Cebe, M., Erdin, E., Akkaya, K., Aksu, H., & Uluagac, S. (2018). Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE communications magazine, 56*(10), 50-57.

Chan, F. H., Chen, Y. T., Xiang, Y., & Sun, M. (2017). Anticipating accidents in dashcam videos. In *Computer Vision–ACCV 2016: 13th Asian Conference on Computer Vision, Taipei, Taiwan, November 20-24, 2016, Revised Selected Papers, Part IV 13* (pp. 136-153). Springer International Publishing.

Chang, W. J., Chen, L. B., & Su, K. Y. (2019). DeepCrash: A deep learning-based Internet of vehicles system for head-on and single-vehicle accident detection with emergency notification*. IEEE Access, 7,* 148163-148175.

Chauhanl, A., & Sharma, N. (2015). Vehicle-to-vehicle communication: traffic safety over RF communication. *Int. J. Sci. Res. Manag, 3,* 2769-2772.

Deflorio, F., & Carboni, A. (2022). Safety systems and vehicle generations: Analysis of accident and travel data collected using event data recorders. *Journal of Transportation Safety & Security, 14*(8), 1307-1332.

Dima, D. S., & Covaciu, D. (2017, October). Solutions for acceleration measurement in vehicle crash tests. In *IOP Conference Series: Materials Science and Engineering* (Vol. 252, No. 1, p. 012007). IOP Publishing.

Dima, D. S., & Covaciu, D. (2017, October). Solutions for acceleration measurement in vehicle crash tests. In *IOP Conference Series: Materials Science and Engineering* (Vol. 252, No. 1, p. 012007). IOP Publishing.

Ethereum Gas Tracker (2022). Ethereum Gas Tracker. https:// etherscan.io/ gastracker.

Ethereum Upgrade, (2022). Ethereum Upgrade. https://ethereum. org/en/upgrades/

European Commission (2010). Towards a European Road Safety Area: Policy Orientations on Road Safety 2011–2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0389

European Union (2017). The Council of Europe: Valletta Declaration on Road Safety; Available online: https://eumos.eu/wp-content/uploads/2017/07/Valletta_Declaration_on_Improving_Road_Safety.pdf (accessed on November 2022).

Gerrits, L., Kromes, R., & Verdier, F. (2020, August). A true decentralized implementation based on iot and blockchain: a vehicle accident use case. In *2020 International Conference on Omni-layer Intelligent Systems (COINS)* (pp. 1-6). IEEE.

Guo, H., Meamari, E., & Shen, C. C. (2018, August). Blockchain-inspired event recording system for autonomous vehicles. In *2018 1st IEEE international conference on hot information-centric networking (HotICN)* (pp. 218-222). IEEE.

Guo, H., Meamari, E., & Shen, C. C. (2019, March). Multi-authority attribute-based access control with smart contract. In *Proceedings of the 2019 international conference on blockchain technology* (pp. 6-11).

Hamrouni, A., Ghazzai, H., Frikha, M., & Massoud, Y. (2020). A spatial mobile crowdsourcing framework for event reporting. *IEEE transactions on computational social systems, 7*(2), 477-491.

Holt, T., & Dolliver, D. S. (2021). Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. *Forensic Science International: Digital Investigation, 37,* 301167.

IPFS Pinning Service, (2022). IPFS Pinning Service. https://docs. ipfs.io/how-to/work-with-pinning-services/#use-an-existing-pinning-service.

Kaiwartya, O., et al. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects*. IEEE access, 4,* 5356-5373*.*

Khaliq, K. A., et al. (2019). Road accidents detection, data collection and data analysis using V2X communication and edge/cloud computing. *Electronics, 8*(8), 896.

Khodaei, M., & Papadimitratos, P. (2015). The key to intelligent transportation: Identity and credential management in vehicular communication systems. *IEEE Vehicular Technology Magazine, 10*(4), 63-69.

Khoukhi, L., Xiong, H., Kumari, S., & Puech, N. (2021). The Internet of vehicles and smart cities. *Annals of Telecommunications,* 1-2. https://doi.org/10.1007/s12243-021-00891-

Kim, S., & Kim, B. J. (2020). Crash risk-based prioritization of basic safety message in DSRC. *IEEE Access, 8,* 211961-211972.

Leal, F., Chis, A. E., & González–Vélez, H. (2020). Performance evaluation of private ethereum networks. *SN Computer Science, 1,* 1-17.

Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in auditing, 13*(2), A19-A29.

Melo, C., Dantas, J., Pereira, P., & Maciel, P. (2021). Distributed application provisioning over Ethereum-based private and permissioned blockchain: availability modeling, capacity, and costs planning. *The Journal of Supercomputing,* 1-27.

Miao, L., Virtusio, J. J., & Hua, K. L. (2021). PC5-based cellular-V2X evolution and deployment. *Sensors, 21*(3), 843.

Mihelj, J., Zhang, Y., Kos, A., & Sedlar, U. (2019). Crowdsourced traffic event detection and source reputation assessment using smart contracts*. Sensors, 19*(15), 3267.

Miloud Dahmane, W., Ouchani, S., & Bouarfa, H. (2022). Guaranteeing information integrity and access control in smart cities through blockchain. *Journal of Ambient*

Intelligence and Humanized Computing, 1-10.

Mollah, M. B., et al. (2020). Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet of Things Journal, 8*(6), 4157-4185.

Oham, C., Kanhere, S. S., Jurdak, R., & Jha, S. (2018). A blockchain based liability attribution framework for autonomous vehicles. *arXiv preprint arXiv:1802.05050.*

Petrescu, L., & Petrescu, A. (2017, October). Vehicle-pedestrian collisions–Aspects regarding pedestrian kinematics, dynamics and biomechanics. In *IOP Conference Series: Materials Science and Engineering* (Vol. 252, No. 1, p. 012001). IOP Publishing.

Petroni, B. C. A., et al. (2020). Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain. *Forensic Science International: Digital Investigation, 34,* 300985.

Philip, A. O., & Saravanaguru, R. A. K. (2018). A vision of connected and intelligent transportation systems*. International Journal of Civil Engineering and Technology, 9*(2), 873-882.

Philip, A. O., Saravanaguru, R. K., & Abhay, P. A. (2022). Traffic event reporting framework using mobile crowdsourcing and blockchain. In *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021* (pp. 909-930). Singapore: Springer Nature Singapore.

World Health Organization (2009). European status report on road safety: towards safer roads and healthier transport choices.

World Health Organization. (2018). World Health Organization Road Traffic Injuries. *https://www. who. int/news-room/fact-sheets/detail/road-traffic-injuries (Accessed: 14.07. 2019).*

Submitted: 15.03.2023
Accepted: 19.05.2023