2021 NDIA Ground Vehicle Systems Engineering and Technology Symposium
VEA/Cyber Technical Session
August 10-12, 2021 – Novi, Michigan

BLOCKCHAIN VEHICLE APPLICATIONS AND CYBERSECURITY: AN APPROPRIATE USE OR USE APPROPRIATELY?

Charles Parker, II

Stephenson Technology Corporation

ABSTRACT

Bitcoin and other digital currencies utilize blockchain. Blockchain, in summary, is a collection of blocks. Within each block is a collection of transactions. Each computer (node) has the same list of blocks and transactions, which they can see as the blocks are filled with the transactions. While this is the traditional application experienced, there are other applications relevant to cybersecurity. As part of the blockchain technology, the nodes are responsible for decision-making. The blockchain technology may be used for this function in these systems. In adjusting the data flow, this is an option to increase the cybersecurity for a complete system. This addition to the cybersecurity system provides a clear benefit.

Citation: Parker, C., "Blockchain Vehicle Applications and Cybersecurity: An Appropriate Use or Use Appropriately?", In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, August 10, 2021.

1. Introduction

There are many who have entwined blockchain and Bitcoin into one application, as this is the most noted implementation. Since Bitcoin recently topped $60k/Bitcoin, this connection may be further amplified with the marketing and media buzz and increased number of news articles. This is a natural extension since the predominant blockchain use case has historically been coupled with Bitcoin. This may be the believed firm grasp of what Bitcoin is, while leaving the blockchain application in a fog.

Bitcoin and other cryptocurrencies require while blockchain, blockchain does not require Bitcoin to exist. Blockchain is a peer-to-peer (P2P) network used to authenticate transactions and record these in a ledger, much like a bookkeeper or with a database. This has been the use case in a majority of the cases. The blockchain maintains the processes and ledger, which holds the transactions. This method is also called a trust network or distributed trust network, as the nodes or members of the network trust each other as they approve the transactions. These transactions are stored in blocks that are chained together (hence blockchain). The chaining occurs when the has value for the transaction of the prior block is stored on the next block. The members of the blockchain all have the same copy of the ledger. Once the data is recorded in the blockchain, this is permanently stored. With all the members/nodes having the same copy of the blockchain ledger, modifying or changing this is difficult from the perspective of the number of resources and costs required to execute an attack. There are two attacks which may alter these when successful. One of these is the 51% attack, which will be addressed later. While the Bitcoin application is well-known, there are many other applications, which are completely viable, and in use today.

2. Similarities with the vehicle digital infrastructure

Over the last approximately 15 years, the vehicle has transformed itself from the mass of metal to computer on wheels. The prior platforms were controlled more through mechanical means. With the paradigm, there are electronic modules, throughout the vehicle monitoring the entirety of the operations and controlling movement.

While blockchain is an entirely different technology than the current state of automobiles, there are similarities [1]. There is the decentralized architecture to consider. With the blockchain, there is no central authority. Each node has its input and there is not a central node making all the decisions. The decentralized architecture also allows for scaling. Adding nodes is not an excessively difficult task. Vehicles, dependent on the manufacturer model, and options have a varying number and variety of modules. The higher end vehicle may be expected to have more based on increased functions and options. Adding functional nodes/modules does involve more time and effort but is likewise a scalable objective.

Availability is likewise similar. With blockchain there is no single point of failure (SPoF). Each node operates on its own. With the vehicle infrastructure, the form is much the same. If the pressure monitoring system becomes inoperable the driver receives a message of the issue. While this is a problem, the vehicle does keep operating. This is noted though with a caveat, in that there are critical systems in a vehicle which do no need to be working for the vehicle to operate.

Within the vehicle infrastructure, one aspect is highly encouraged. The vehicle has many different commands and actions to take in a split second. In watching the messages flow on the CANBus, these bombard the screen as the vast number of these messages continuously filter through the screen. The speed of these does not allow human real-time review in any measure of the term. These messages/frames are automatically processed by the appropriate module. Blockchain has the same functional aspect among the available options, smart contracts. When implemented, and the conditions met, the smart contracts tasks are executed.

3. Vehicle & embedded systems

The nodes/modules in a vehicle have programmed functions, operating in the vehicle as the user drives it. The modules running these tasks may be engineered to allow other functions in memory [1]. One significant issue with vehicle embedded systems has been cybersecurity. For each system there are the known attacks and variants being created through the research process. As technology advances, there are additional attacks which will be used on these. As each attack becomes known, as applied to its target, a defense is created. This circular attack-defense scenario continues until the defense in depth makes this impractical for the attackers. Implementing blockchain technology in ground vehicle systems provides the defense in depth need to secure the ground vehicle system. The blockchain application may take advantage of this hardware opportunity to establish a trust network. Each vehicle model is unique. A full-size pick-up truck with a touring package is unique from a medium-sized sedan. Comparably between each platform there would be overlap with the modules and functions, however, there is sufficient differentiation. Within each vehicle there are also different communication protocols (e.g. Wi Fi, cellular, Bluetooth, CAN, and ethernet). These likewise may be used to support blockchain in the vehicle.

a. Applied in other industries

There are already many applications in use across the globe and industries. Blockchain is used in Thai judicial system to for record-keeping [2], charitable payments [3], part of the voting platform with the Michigan Democratic Party State Nomination Convention [4], and identification in South Korea [5]. For the vehicle infrastructure, this function should be applied to data integrity and assurance, among other tasks. The additional benefit is derived from the blockchain being decentralized. This removes the usual attack vectors and increases the effort and resources required for the attack. There would not be not a central attack point, for example, with over-the-air updates. In prior models, the authentication protocol was managed in one area. With the blockchain application, this is managed by the nodes in the vehicle, not just one node.

4. Smart contracts

The vehicle software and firmware will require updates. The vehicle owner does not drive the vehicle into the dealership for every firmware and software update. This is handled wirelessly over the air. With the over-the-air (OTA) updates, the vehicle would not automatically apply these. There is an authentication process with a single point processing the requests. These may, in theory, originate from an untrusted or malicious source, and contain malware or other malicious content. To mitigate this issue, smart contracts may be applied to the vehicle system. In other

forms these are already used with other industries, such as with smart billing [6]. These are simply code with instructions to execute upon previously agreed on tasks being completed once the set of conditions are met, the smart contract is executed without human interaction. This process is much more efficient than others as the system is less complex than the alternatives which translates into quick processing.

Lee and Lee [7] researched this for IoT devices. While this is not precisely the same with vehicles, the same principles apply. With their model, there is a verification node. If the firmware were to be outdated on a node, this would be placed in a list with the other nodes requiring updates. Once the firmware update is loaded, the updates are distributed to the nodes requiring the updates.

Rathee, Sharma, Iqbal, Aloqaily, Jaglan, et al. [8] had a different view of this. For connected and autonomous vehicles (CAN) the blockchain would assist in keeping track of the transactions. The method used multiple vehicles, all connected to IoT devices as the nodes. This was used to monitor the vehicles on the road. The individual vehicle would be dependent on the other vehicles within the subject vehicle Wi Fi range. On a map, the vehicles with the diameter of a subject vehicle appear as a cluster. While beneficial, this may also be viewed as a potential vulnerability, based on the cybersecurity (not or partially) applied to the other vehicles. If the applied cybersecurity was not to at least the baseline acceptable level, there could be an issue with the insecure vehicle and others within the range of trusted vehicles. As these are assimilated temporarily into the blockchain while within the inter-connected range, each vehicle may have open vulnerabilities or individual compromised systems. This generally would be unknown to the subject car.

5. Proposed implementation

In comparison to the others, the proposed methodology is intra-vehicle, versus inter-vehicles, in its structure. This would be utilized when the vehicle would need firmware or software OTA updates, and other operations and tasks requiring security. The vehicle's systems not considered as critical, yet still required, certainly would be viable candidates to use this.

Implementing blockchain in this alternative method is a nuance. As noted, the prior implementation traditionally have been focused on cryptocurrency. This is a natural on-going usage as cryptocurrency was the first usage. This application applies blockchain as a security feature only. Ground vehicles require security just as any other vehicle embedded system would. The new method requires a different view of its application. In the new method, instead of nodes being present throughout the globe, the nodes would be in the vehicle's network structure. One other proposed method would have used other ground vehicles as the nodes. One issue with this are the other ground vehicles are clearly not in the scope of control for any other vehicles. Each vehicle operates independently of the others and there is no active assurance of security being fully applied. For this to work, ground vehicle A would assume all of the vehicles proximate to vehicle A were sufficiently protected and secured, the firmware for all the modules would be current, and no vulnerabilities would be present. This is by far too much to depend on for other vehicles, especially when troops lives may be in danger in the case of malware being introduced into the

system. The addition of blockchain to the process would add a layer to the defense in depth for the ground vehicle, modules, and troops.

The specific work and data flow would differ per each vehicle platform. In general, the process would start with the authentication process. This simple task may be managed in different methods per the federal and DoD standards and requirements. The authentication process. For this step, the process may use certificate, key, or other predetermined process to authenticate the sending node (A). As the communication uses TLS 1.2 or 1.3, dependent on the environment. This would be sent through the secure gateway. The secure gateway itself should be secured and not simply present. This should have security in mind during the architecture process for both the hardware and software. Once the authentication is successful, the gateway would communicate this in return, and wait for the remainder of the handshake. The sending node, A, sends the encrypted message/payload. Once received, as an optional additional step, the sender is verified as being a trusted source using a different method from the authentication. Granted, this is an additional step and will take a few milliseconds. This however does provide for a greater level of security as an additional tool with defense in depth. The payload would then be decrypted with the symmetric key, if this method would be used. At this point the payload with update has not been provided to the modules/nodes requiring firmware or software updates.

The blockchain would be configured as a private blockchain. Each approved node in the private blockchain is detailed and logged with the end-of-line (EOL) processing at the factory. As not all the modules are manufactured by one entity, this sub-process has to be done at the EOL. The modules could be produced by dozens of manufacturers. The manufacturer knows the suppliers and modules for each vehicle and may use these as nodes. The specific software and hardware within each may also be documented with an SBOM (software bill of materials) and HBM (hardware bill of materials).

At this point each node is permissioned. Optionally, 5%-10% of the nodes may not be fully permissioned, acting as decoys for anyone attacking the system. This may be viewed as a quasi-honeypot on the system, allowing any attacker the opportunity to waste their time and resources attacking a pseudo-node in the blockchain. As the requests arrive at the vehicle after assembly, when the ground vehicle is placed into service, the nodes would process the requests for updates only after 51% of the modules/nodes validate the packet based on predetermined security attributes (e.g., hash values). The number of nodes in the vehicles range from 80-150 based on the OEM and model. The greater the number of modules/nodes in the vehicles permissioned with in the blockchain, the effort and resources required for any attack increases. Instead of requiring one or two compromised modules to execute an attack, as with the standard attack, there would need to be at least 41 successful attacks based on an 80 module/node system. If this attack were to occur, the attack process would create a substantial amount of noise within the vehicle's modules and CAN. With a properly configured system, this should be noted and red flagged.

Directly this provides a substantial set of hurdles to cross for the attacker. Compromising one module may not be a significant amount of time for a team. Compromising more than 4 nodes to maliciously adjust the firmware updates for one vehicle or a fleet becomes a rather large undertaking most teams would prefer to avoid. Indirectly, this provides an additional layer for the defense in depth.

If this proposed version were to create an unacceptable amount of overhead (e.g., processing time, additional memory, or other factors), the alternative would be to implement smart contracts. As with the true blockchain implementation, applying smart contracts would be a nuance . Smart contracts have been used to automatically process information or complete a set of tasks only when a predetermined set of items or checklist have been fully executed. The smart contract would not act on anything until these would be done. The smart contract implementation would add the additional layer of security. The usage would not provide the vast security expanse as the blockchain would, however, this is still a consideration. This would provide for a less expansive implementation, while still adding the additional layer of security to the module/node, system, and vehicle.

This is a vastly simplified version of the implementation, abridged for the venue. Each ground vehicle network and meta-system is different and unique. Each uses a distinct architecture, modules, suppliers, and hardware/software combinations throughout. Addressing each present form and implantation would be problematic. While there are similarities to be leveraged, the differences potentially are voluminous. The full implementation, including data flow, workflow, and DFMEA are available.

6. Attacks & Mitigations

These blockchain systems are not un-hackable. These are not perfect, and do have vulnerabilities present. In practice the predominant attack is the 51% attack. There have been several successful attacks within the last 2.5 years against cryptocurrency, and by extension the blockchain technology. For example in January 2019 the cryptocurrency Ethereum Classic on the Coinbase exchange platform, where people are able to buy and sell the cryptocurrency, was successfully attacked [9]. In this case, the ledger or history of the transactions was being attacked. The attack was focused on taking control of over half of the nodes. This allowed the attacker to rewrite the ledger, which holds the transactions. This is not the only attack in recent history. There have been over 200 attacks documented [10] based on the vulnerabilities [11]. There are several forms of attacks against the blockchain. The include API exposure (the API when improperly exposed may be targeted), block mining race attack (much like the Finney attack), block mining timejack attack (the attacker may isolate the node's time signal), block reordering attack (when the cryptographic operations are implemented incorrectly the blocks within the ledger holding the information may be re-ordered), no or insufficient hashing capacity (when the blockchain network does not have the capacity to properly hash, the attackers would be able to rent hashing capacity to execute the 51% attack), blockchain peer flooding attack (the attackers creates a large number of false nodes on the blockchain network, force the real nodes to slow down or not being able to respond; appears much like the DDoS

attack), blockchain reorganization attack (aka alternative history attack), consensus 51% attack (gain control of over half of the nodes), and consensus delay attack (by slowing down the blockchain operations, other attacks may be organized and executed).

While the list is extensive, the attack used primarily is the 51% attack. This works best with small blockchains. The vehicle network system is not huge or moderately large, thus seemingly this would appear to be a viable target. There are many defenses available to defend the blockchain from these attacks. The security architecture team may increase the number of nodes for the consensus [12]. The vehicle system may deny access of attacking IP address or node. This may be short-sighted in that the shifting the IP address for the attacker is not a significant task. The security team may also recommend using the MESS (Modified Exponential Subject Scoring) system [13]. This decreases the potential for a successful 51% attack. This works to increase the resources required for this attack by 31%.

7. Justification

The enterprise has been fortifying the defenses for much longer than embedded systems. This significantly only began to receive the necessary attention approximately a decade ago. As the embedded systems have not had the opportunity yet to mature the applied cybersecurity or include this throughout the development process and SDLC, these systems are viable targets for attacks.

Further complicating the issue and adding strain to the cybersecurity architects is the criticality of these systems. This article focused on the vehicle systems. These transport our families on errands and people to work, among other tasks. These provide a method for people to arrive at their workplace. Commercially, these deliver food, and goods required for our society. Embedded systems are used in other industries as a mission critical hardware system. These systems are used in maritime shipping, aircraft, farm equipment, and other machinery. Also, in the case of a breach, these assets could be used maliciously. The uses rate this as being critical to society, creating a larger target on the embedded systems. This requires more security to be applied to the embedded system to mitigate the increased level of risk.

8. Discussion

The application works as an additional layer for the vehicle's cybersecurity to be added into the defense in depth. This in concept, would be used with the other security tools in place. When properly implemented, this tool removes the single point of failure (SPoF) relating to malicious updates and other attacks. This also would be easily used to ensure the integrity of the firmware and software in a vehicle or any other embedded system. If an attack on a vehicle were to be planned, at a minimum above compromising the engineered systems, 51% of the modules/nodes would have to be successfully attacked. Each of these modules are manufactured by several Tier 1 suppliers and present a unique target with its own functionality and specific attack vectors. There may be an overlap in attack methods, however, it is not likely to be significant. The other aspect is this creates a significant amount of noise in a vehicle which should be detected by an IDS or secure gateway as the unusual traffic increases. If the system has no method or tool to detect unusual traffic, this may be more of a systemic issue.

With this proposed system in place, defeating the vehicle's cybersecurity measures requires much more time and resources than the standard attack. This aspect generally is enough to deter an attacker as they focus on simpler systems as targets. With this system, the low hanging fruit of an easy or easier attack is not present.

While this is a clear benefit, this will require time to design into a system and implement. With at least a three- or four-year model year lag, here is time for further analysis and source for any additional hardware.

The additional engineering effort to further secure the vehicle is justified. As the attacks increase in number and complexity, there will be additional and improved security measures required. Simply resting on our past success from years past and hoping security by obscurity works is not an option. There is too much at risk to assume. Any calculation will show this viable and deployable solution is workable and feasible.

1. References

[1] Mendiboure, L., Chalouf, M.A., & Krief, F. (2020). Survey on blockchain-based application in vehicles. *Computers & Electrical Engineering*, 84. https://doi.org/10.10/16/j.compeleceng.2020.106646

[2] Nelson, D. (2020, August 20). Thailand is prepping to move judicial system records to a blockchain. https://www.coindesk.com/Thailand-blockchain-court-of-justice

[3] Delong, J. (2020, September 12). A malaysian company is developing a blockchain-based app for charities. https://www.reporter.am/a-malaysian-company-is-developing-a-blockchain-based-app-for-charities/

[4] Wright, T. (2020, September 2). Blockchain voting hailed a success at Michigan democratic convention. https://cointelegraph.com/news/blockchain-voting-hailed-a-success-at-michigan-democrat-convention

[5] Faridi, O. (2020, September 6). Mobile banking app offered by south korea's shinhan bank now uses blockchain based decentralized ID authentication. https://www.crowdfundinsider.com/2020/09/166348-mobile-banking-app-offered-by-south-koreas-shinhan-bank-now-uses-blockchain-based-decentralized-id-authentication/

[6] Zhang, H., Deng, E., Zhu, H., & Cao, Z. (2019). Smart contract for secure billing in ride-hailing services via blockchain. *Peer-to-Peer Networking and Applications, 12*(5), 1346-1357. https://doi.org/10.1007/s12083-018-0694-5

[7] Lee, B., & Lee, J. (2016). Blockchain-based secure firmware update for embedded devices in an internet of things environment. *The Journal of Supercomputing, 73*, 1152-1167.

[8] Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. *Sensors, 19*(14). https://www.doi.org/10.3390/s19143165

[9] Orcutt, M. (2019, February 19). Once hailed as unhackable, blockchains are now getting hacked. https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/amp/

[10] Seifreid, K. (2020, October 26). Over 200 documented blockchain attacks, vulnerabilities and weaknesses. https://cloudsecurityalliance.org/blog/2020/10/26/blockchain-attack-vulnerabilities-and-weaknesses/

[11] Amiet, N. (2021). Blockchain vulnerabilities in practice. Digit Threat: Res. Pract., 2(2), Article 8. Doi:https://doi.org/10.1145/3407230 & https://dl.acm.org/doi/fullHtm/10.1145/3407230

[12] Quentson, A. (2014, June 8). 4 lines of defense against a 51% attack. https://cch.com/4-lines-defence-51-attack/

[13] Thompson, P. (2020, October 13). Ethereum classic implements 51% attack defense. https://coingeek.com/ethereum-classic-implements-51-attack-defense/