GODFREY KAHN S.C. HNTB GTiMA MANDLI COMMUNICATIONS

August 2019

All ACES

Article Author

Robert Fischer
GTiMA
rfischer@usgtima.org

Group Members

Steve Caya
Mandli Communications
scaya@roadview.com

Steve Cyra
HNTB
scyra@hntb.com

Art Harrington
Godfrey & Kahn, S.C.
ajharrin@gklaw.com

Ned Witte
Godfrey & Kahn, S.C.
nwitte@gklaw.com

Amir Zaman
Mandli Communications
azaman@mandli.com

The information in this article is based on a summary of legal principles. It is not to be construed as legal advice. Individuals should consult with legal counsel before taking any action based on these principles to ensure their applicability in a given situation.

Blockchains, Smart Contracts, and the Future of Transportation Security

Tomorrow's vehicles will be computers on wheels, connected to each other, the infrastructure, and the internet.

While officials across the country tout the potential benefits of this increased connectivity, it is also the source of considerable anxiety. Protecting these vehicles from hackers is turning out to be a hard nut to crack, but some experts at the U.S. DOT believe blockchain could be the magic bullet.

"Cybersecurity is a major concern," remarked U.S. Transportation Secretary Elaine Chao while addressing a packed room at the Autonomous Vehicle Symposium last year. "The hacking of AV software could result in privacy violations, theft, or even the acquisition of a vehicle by terrorists," she continued.

If you think Secretary Chao's warnings are speculative, think again: there have been 1.4 million vehicles impacted by the first, and only, cybersecurity-related recall, which occurred in 2015 when Fiat Chrysler recalled vehicles after researchers used a wireless connection to turn off a Jeep Cherokee's engine as it drove.

But what Secretary Chao failed to mention was a recent report by the U.S. DOT John A. Volpe National Transportation Systems Center, which examines various blockchain applications in transportation – including blockchain's potential for preventing cyber-attacks on automated vehicles.

With vehicles continuously connected to their surroundings, the report notes, "the attack surface for hackers is broad, touching most in-vehicle systems via a wide range of external networks such as Wi-Fi, cellular networks, service garages, toll roads, fuel stations, traffic lights, and aftermarket devices."

The report's conclusion: blockchain's inherent value proposition of immutable transactions, and decentralized consensus through transparent nodes, may have a role to play in certain aspects of securing automobiles form cyberattacks.

For instance, vehicles are produced with more and more electronic control units – from 30 to 100 in automated vehicles – and each unit's operating system will likely be updated over the air. When receiving these updates from potentially unsafe Wi-Fi networks at fuel stations, homes, dealers, etc., blockchain can validate the authenticity of these critical peer-to-peer software updates, instead of relying on the central server of an automotive components manufacturer.

Another aspect of AV security resides in the supply chain, where original equipment manufacturers typically integrate hundreds of components they receive from multiple suppliers around the world, often unaware of security flaws in these components. Blockchain could serve as a trusted ledger of maintenance activities performed on these components throughout their lifetime.

While blockchain is not particularly new technology, its application to the world of transport is relatively nascent.

A blockchain is a digital, openly shared, immutable, and a decentralized log of transactions. The concept was introduced in the late 2000s as a virtual scaffolding for transactions using the digital currency bitcoin.

The idea behind bitcoin was to remove banks from financial transactions by allowing non-trusting members to interact over a network in a verified way without a trusted intermediary.

Every bitcoin transaction is stored on a blockchain that is continuously updated across a network of thousands of computers. Consequently, if you want to sell a piece of art to your neighbor, for example, you can verify that your neighbor indeed possesses the requisite amount of bitcoin, and execute the transaction, all without the involvement of a bank.

Though blockchains were made for finance, smart contracts make blockchains applicable beyond finance, to industries like transportation.

Smart contracts, according to another Volpe Center report, are software, not actual contracts. But like a contract, they set parameters that parties to a transaction agree upon. Terms of the agreement are written directly into lines of code, and smart contracts refer to blockchains as a source of truth.

It is precisely these smart contracts that enable blockchain to, for instance, validate the authenticity of peer-to-peer software updates, or act as a trusted ledger of maintenance activities performed on vehicle components. The parameters for each of these transactions – or over the air software updates – can be baked directly into the code, and confirmed for their validity.

The technology does have it's limitations, however, which is why the Volpe report is careful to note that blockchain's effectiveness in securing automobiles is limited to certain situations. "The time required for participating mining nodes to come into consensuses of transaction blocks is several minutes," according to the report. For critical updates that need to happen in mere seconds, blockchain might not be suitable. On the other hand, "use of blockchain for overnight updates would be appropriate," the report concluded.

Regardless of whether or not blockchain is the silver bullet against vehicle cyber-threats, one thing is for sure: traditional enterprise security strategies, which have focused on cutting off outside access, are not optimal for automated vehicles, where secure systems within the vehicle must interact with many other secure systems.

Building a walled garden, figuratively speaking, is no longer an option. But a chained-linked fence – like blockchain – just might be the solution.

Robert Fischer is President of GTiMA and a Technology and Policy Advisor to Mandli Communications. Both GTiMA and Mandli work with national, international and regional authorities to advance smart city standards, policies, and best practices - especially as they relate to the future of mobility. Robert is also an Associate Editor of the SAE International Journal of Connected and Autonomous Vehicles.