Negative: OTA Blockchain

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan requires “Blockchain” technology to be used to manage Over The Air (OTA) software updates being broadcast in the future to self-driving cars. There’s always a risk that hackers could take control of cars by hacking these updates, and Blockchain is supposed to prevent it. But the status quo is already implementing security, and Blockchain is far from the perfectly secure system AFF thinks it is.

Negative: OTA Blockchain 3

OPENING QUOTES / NEG PHILOSOPHY 3

Affirmative Burden 3

TOPICALITY 3

1. Not AI 3

Existing non-AI cars already use OTA. Examples: Ford, GM and Tesla 3

Violation: OTA isn’t AI 3

Impact: Negative ballot 3

INHERENCY 3

1. “Uptane” solves in Status Quo 3

Uptane already exists in Status Quo and provides security against attacks using a distributed system 3

Definition of Uptane 4

2. OTA already in use (it’s not a “new” problem that has to be solved to make AI cars work) 4

Existing (non-autonomous) cars are already using OTA updates 4

Existing OTA already has methods to patch security flaws well enough to outweigh security concerns 4

[Not something we need to solve before AI cars are deployed] OTA is already deployed - $35 billion expected in 2022 4

3. More study needed (and already underway) 5

Status Quo standards being set right now: ISO committee is defining standards for automotive OTA security 5

HARMS / SIGNIFICANCE 5

1. Hacking risk is low 5

Risk of OTA hacking on cars is low and impacts easily avoided 5

SOLVENCY 6

1. More study needed 6

Blockchain is still in its infancy and is full of scams and hype 6

Years of further analysis and study needed. You can’t just implement it quickly 6

2. Blockchain isn’t secure 6

If you think Blockchain is unhackable, you’re “dead wrong” 6

Hackers have stolen $2 billion from blockchain cryptocurrencies so far 6

Blockchain can be hacked too – it’s already happened 7

Coinbase blockchain was hacked in 2019 7

Largest Bitcoin exchange in the world was hacked… twice (2011 and 2014)! And went bankrupt when most of their money was stolen 7

3. High Data Volume 7

Blockchain not workable in high-volume data environments 7

Failure: Car OTA systems are high data volume environments 8

Example: Solana blockchain crashed in Sept 2021 during high data volume incident and took hours to get restarted 8

DISADVANTAGES 9

1. Less security 9

Blockchain doesn’t solve, and false confidence in it makes security weaker 9

Non-Blockchain solutions would have been better 9

A/T “But we’re not using “public” blockchain” – Then you’re not really using blockchain. “Private” blockchain is no different from status quo systems we’ve had for 60 years now 9

Works Cited 10

Negative: OTA Blockchain

OPENING QUOTES / NEG PHILOSOPHY

 Affirmative Burden

Affirmative cannot win this debate by simply proving that Blockchain is secure. They have to prove that status quo OTA systems are not as good as Blockchain and that the difference between Status Quo systems and Blockchain provides a significant advantage.

TOPICALITY

1. Not AI

Existing non-AI cars already use OTA. Examples: Ford, GM and Tesla

Keith Barry 2018 (car writer for Consumer Reports) Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair? 20 Apr 2018 <https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/> (accessed 17 Nov 2021)

Ford and GM, among others, recently announced that some of their 2020 models will allow over-the-air (OTA) updates that can upgrade a vehicle with new features, or even remotely fix faulty vehicle software. It’s similar to how Apple or Samsung, for example, can update or repair the software on a smartphone. Tesla, the electric car company, upgrades its vehicles remotely.

Violation: OTA isn’t AI

If existing Non-Autonomous, Non-AI cars already use OTA, that proves that OTA isn’t part of nor dependent upon AI.

Impact: Negative ballot

No one in the room is affirming substantial reform to AI. If no one is affirming the resolution, then no matter who wins, you should vote Negative.

INHERENCY

1. “Uptane” solves in Status Quo

Uptane already exists in Status Quo and provides security against attacks using a distributed system

Amit Agarwal 2020 (with PathPartner - a specialist in product engineering, providing concept-to-production services to customers across automotive, consumer electronics, broadcast, medical and internet-of-things domains ) Understanding Automotive OTA (Over-the-Air Update) 26 June 2020 <https://www.pathpartnertech.com/understanding-automotive-ota-over-the-air-update/> (accessed 17 Nov 2021)

**OTA update using Uptane**
The Update Framework (TUF) is designed to create a security system to protect users of software repositories from the security attacks. It has been designed, keeping in mind that the backend server may not be secure, or the key used for the cryptography can be stolen. So, what it does is it creates a distributed system, where the dependency on a particular system is not there, and in case of the attacker’s thread, all the systems cannot be hacked so easily at the same time. The Update Framework (TUF) has divided the roles into four parts (Root of trust, Timestamps, Snapshot, Targets) Uptane builds on The Update Framework (TUF), which is distributed (Timeserver, directory and image repository, manifests, Primary/secondary ECU’s, full and partial verification.

Definition of Uptane

Amit Agarwal 2020 (with PathPartner - a specialist in product engineering, providing concept-to-production services to customers across automotive, consumer electronics, broadcast, medical and internet-of-things domains ) Understanding Automotive OTA (Over-the-Air Update) 26 June 2020 <https://www.pathpartnertech.com/understanding-automotive-ota-over-the-air-update/> (accessed 17 Nov 2021)

The most challenging part of the component is when the data/Images are exposed to the n/w and they are easy for the attackers to manipulate. There are many techniques, open-source and third-party solution for secure update to the head unit Most commonly used is Uptane. Uptane is the first comprehensive security framework guiding the implementation of OTA update systems on a design level.

2. OTA already in use (it’s not a “new” problem that has to be solved to make AI cars work)

Existing (non-autonomous) cars are already using OTA updates

Doug Newcomb 2020 (journalist) 6 Nov 2020 “The Upsides and Downside of Over-the-Air Software Updates for Automobile Dealers” <https://www.wardsauto.com/dealers/upsides-and-downside-over-air-software-updates-automobile-dealers> (accessed 17 Nov 2021)

For example, starting with the 2020 Cadillac CT5, General Motors is implementing a new electronic vehicle architecture that will underpin most new GM vehicles by 2023 that, in addition to managing the large amounts of data required for modern connected cars and semi-autonomous features, will enable seamless OTA updates.

Existing OTA already has methods to patch security flaws well enough to outweigh security concerns

Keith Barry 2018 (car writer for Consumer Reports) Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair? 20 Apr 2018 <https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/> (accessed 17 Nov 2021)

If a hack does happen at some point in the future, though, Koscher says that OTA updates should make it easier to fix—much the same way that your phone or computer can patch a security flaw with a software update. “The security concern will be outweighed by the ability to catch security issues,” Koscher says.

[Not something we need to solve before AI cars are deployed] OTA is already deployed - $35 billion expected in 2022

Dr. Subir Halder, Dr. Amrita Ghosal and Mauro Conti 2020 (Halder – PhD; works at Univ. of Limerick, Dept of Electronic & Computer Engineering. Ghosal – PhD; works at Univ. of Limerick, Dept of Computer Sci. & Info. Systems. Conti - Senior Member, Institute of Electrical and Electronics Engineers ) June 2020 Secure Over-The-Air Software Updates in Connected Vehicles: A Survey <https://www.researchgate.net/publication/341848182_Secure_Over-The-Air_Software_Updates_in_Connected_Vehicles_A_Survey/link/5f019527a6fdcc4ca44e700d/download> (accessed 18 Nov 2021)

The introduction of OTA updates in the automotive industry offers both the Original Equipment Manufacturer (OEM) and the driver several advantages. According to IHS Automotive, an auto-industry data consulting company, the total worldwide OEM cost savings from OTA updates are forecasted to grow to over $35 billion in 2022.

3. More study needed (and already underway)

Status Quo standards being set right now: ISO committee is defining standards for automotive OTA security

Russ Bielawski 2021 (Engineer with GuardKnox US, a **Technology And Engineering Company Specializing In Products for the Automotive Market**) 11 Feb 2021 “SOFTWARE-DEFINED VEHICLES NEED SECURE OTA AUTOMOTIVE UPDATES” <https://blog.guardknox.com/software-defined-vehicles-ota-automotive-updates> (accessed 18 Nov 2021)

Right now, ISO is preparing a committee for [regulation 24089](https://www.iso.org/standard/77796.html) that will define minimum requirements for secure automotive OTA updates.

A joint working group between the International Standards Organisation (ISO) and the Society of Automotive Engineers (SAE) created a comprehensive and robust worldwide standard, [ISO/SAE 21434](https://learn.guardknox.com/hubfs/Automotive%20Cybersecurity%20Standards_ISO%2021434_WP..pdf), for automotive cybersecurity. It addresses the entire vehicles lifecycle from concept to decommissioning and also lays out requirements and activities on an organizational level.

HARMS / SIGNIFICANCE

1. Hacking risk is low

Risk of OTA hacking on cars is low and impacts easily avoided

Doug Newcomb 2020 (journalist) 6 Nov 2020 “The Upsides and Downside of Over-the-Air Software Updates for Automobile Dealers” <https://www.wardsauto.com/dealers/upsides-and-downside-over-air-software-updates-automobile-dealers> (accessed 17 Nov 2021)

OTA updates also provide a gateway for hackers, although most security experts agree remotely accessing a car’s critical systems is very difficult and time-consuming. They also point out there’s currently far less incentive to hack a car compared to, say, accessing someone’s bank account. And security concerns could be outweighed by the ability to catch and fix security issues more quickly. If a hack occurs, OTA updates make it easier for a vehicle to protect itself in the same way phones and computers patch a security flaw with a software update.

SOLVENCY

1. More study needed

Blockchain is still in its infancy and is full of scams and hype

Louise Matsakis 2018 (journalist) 22 May 2018 “Following a Tuna from Fiji to Brooklyn—on the Blockchain” https://www.wired.com/story/following-a-tuna-from-fiji-to-brooklynon-the-blockchain/

For now, the technology is still in its infancy. The industry around blockchains is riddled with [scams](https://www.wired.com/story/cryptocurrency-scams-ico-trolling/), [false promises](https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115), and has been met with a heaping load of skepticism. Many of the "problems" to which its evangelists have tried to apply it don't make much sense, like [bacon](https://www.inc.com/erik-sherman/cross-bitcoin-with-bacon-you-get-oscar-mayers-latest-promotion-almost.html), [iced tea](http://fortune.com/2018/02/02/long-island-iced-tea-blockchain-2/), and [ending bullying](https://techcrunch.com/2017/08/28/mark-cuban-behind-new-blockchain-messaging-platform/).

Years of further analysis and study needed. You can’t just implement it quickly

Louise Matsakis 2018 (journalist) 22 May 2018 “Following a Tuna from Fiji to Brooklyn—on the Blockchain” https://www.wired.com/story/following-a-tuna-from-fiji-to-brooklynon-the-blockchain/

The second problem is governance. Because blockchains aren't centralized, it's difficult to decide how they should be managed. "Who can use the data? Who can see the data? Who can do analytics on the data? Can they share the data? All of these questions have to be answered to the satisfaction of the ecosystem," says Gopinath. It's likely going to take years to solve these issues and to square them with government regulators. If someone says that they can be solved in six months, "I'll just laugh at them, because it's not going to happen. You can just tell them, sorry, I'm just not going to believe you," says Gopinath.

2. Blockchain isn’t secure

If you think Blockchain is unhackable, you’re “dead wrong”

MIT Technology Review 2019 (journalist Mike Orcutt) 19 Feb 2019 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/> (accessed 18 Nov 2021)

Blockchains are particularly attractive to thieves because fraudulent transactions can’t be reversed as they often can be in the traditional financial system. Besides that, we’ve long known that just as blockchains have unique security features, they have unique vulnerabilities. Marketing slogans and headlines that called the technology “unhackable” were dead wrong.

Hackers have stolen $2 billion from blockchain cryptocurrencies so far

MIT Technology Review 2019 (journalist Mike Orcutt) 19 Feb 2019 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/> (accessed 18 Nov 2021)

In total, hackers have stolen nearly $2 billion worth of cryptocurrency since the beginning of 2017, mostly from exchanges, and that’s just what has been revealed publicly. These are not just opportunistic lone attackers, either. Sophisticated cybercrime organizations are now doing it too: analytics firm Chainalysis recently said that just two groups, both of which are apparently still active, may have stolen a combined $1 billion from exchanges.

Blockchain can be hacked too – it’s already happened

Bruce Schneier 2019 (security technologist who teaches at the Harvard Kennedy School of Government) 6 Feb 2019 “There's No Good Reason to Trust Blockchain Technology” <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/> (accessed 18 Nov 2021)

Blockchain technology is often centralized. Bitcoin might theoretically be based on distributed trust, but in practice, that’s just not true. Just about everyone using bitcoin has to trust one of the few available wallets and use one of the few available exchanges. People have to trust the software and the operating systems and the computers everything is running on. And we've seen attacks against wallets and exchanges. We’ve seen Trojans and phishing and password guessing. Criminals have even used flaws in the system that people use to repair their cell phones to steal bitcoin.

Coinbase blockchain was hacked in 2019

MIT Technology Review 2019 (journalist Mike Orcutt) 19 Feb 2019 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/> (accessed 18 Nov 2021)

Early last month, the security team at Coinbase noticed something strange going on in Ethereum Classic, one of the cryptocurrencies people can buy and sell using Coinbase’s popular exchange platform. Its [blockchain, the history of all its transactions](https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/), was under attack. An attacker had somehow gained control of more than half of the network’s computing power and was using it to rewrite the transaction history. That made it possible to spend the same cryptocurrency more than once—known as “double spends.” The attacker was spotted pulling this off [to the tune of $1.1 million](https://www.technologyreview.com/the-download/612728/hackers-just-stole-1-million-from-the-ethereum-classic-blockchain-in-a-rare-51/).

Largest Bitcoin exchange in the world was hacked… twice (2011 and 2014)! And went bankrupt when most of their money was stolen

Robert McMillan 2014 (technology journalist) 3 March 2014 “The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster” <https://www.wired.com/2014/03/bitcoin-exchange/> (accessed 18 Nov 2021)

FROM A DISTANCE, the world's largest [bitcoin](https://www.wired.com/story/guide-bitcoin/) exchange looked like a towering example of renegade entrepreneurism. But on the inside, according to some who were there, Mt. Gox was a messy combination of poor management, neglect, and raw inexperience. Its collapse into bankruptcy last week -- and the disappearance of $460 million, apparently stolen by hackers, and another $27.4 million missing from its bank accounts -- came as little surprise to people who had knowledge of the Tokyo-based company's inner workings.
**[END QUOTE. THEY GO ON LATER IN THE SAME CONTEXT SAYING QUOTE:]**

This would be the second time the exchange was hacked. In June 2011, attackers lifted the equivalent of $8.75 million.

3. High Data Volume

Blockchain not workable in high-volume data environments

Jillian Oderkirk and Luke Slawomirski 2020 (with the Organisation for Economic Co-operation and Development Health Division) Dec 2020 Opportunities and Challenges of Blockchain Technologies in Health Care https://www.oecd.org/finance/Opportunities-and-Challenges-of-Blockchain-Technologies-in-Health-Care.pdf

Importantly, Blockchain is ill-suited to storing high-volume data due to the computational and capacity constraints of replicating the blockchain across every network participant (node). Storing large records on the blockchain, such as full electronic medical records or genetic data records, would be inefficient and costly. It is also difficult to query data within a blockchain, limiting clinical, statistical and research uses of data.

Failure: Car OTA systems are high data volume environments

Sam Abuelsamid 2021 (degree in mechanical engineering; principal analyst with Navigant Research covering alternative fuels, advanced driving technologies and connected vehicles) 25 May 2021 “Providing Vehicle OTA Updates While Managing Distribution Costs” <https://guidehouseinsights.com/news-and-views/providing-vehicle-ota-updates-while-managing-distribution-costs> (accessed 18 Nov 2021)

Within the next few years, manufacturers will likely be shipping tens of millions of vehicles with OTA capabilities every year. As anyone who has ever grappled with the cost of smartphone data plans knows, carriers don’t give out bandwidth for free. With OTA capability spreading to mass-market vehicles, there is no guarantee that they will be parked within range of a Wi-Fi connection, so making cellular updates more cost-effective is critical. Large file downloads are also more prone to failures, especially in a moving vehicle, which may require restarting the download, further raising the cost. Providing regular updates to fleets of millions of vehicles can quickly escalate into the hundreds of millions of dollars just for data transmission over a cellular network.  The auto industry needs solutions to manage the size of update files to keep the costs of bandwidth, cloud storage, integration, and the on-vehicle storage in check and to provide a reliable user experience.

Example: Solana blockchain crashed in Sept 2021 during high data volume incident and took hours to get restarted

Michael McSweeney 2021 (journalist) 15 Sept 2021 “CRYPTOCURRENCY Solana blockchain validators restart network after transaction stoppage” <https://www.theblockcrypto.com/linked/117711/solana-blockchain-validators-restart-network-after-transaction-stoppage> (accessed 18 Nov 2021)

The Solana blockchain is back online after an hours-long outage. As [previously reported](https://www.theblockcrypto.com/linked/117624/solana-experiences-transaction-stoppage-as-developers-report-intermittent-instability), Solana's transaction blocks came to a stop on Tuesday. Developers later said that Solana's mainnet "encountered a large increase in transaction load which peaked at 400,000 TPS. These transactions flooded the transaction processing queue, and lack of prioritization of network-critical messaging caused the network to start forking." Ultimately, the network's stakeholders moved to execute a restart, a [laborious process](https://docs.google.com/document/d/1vS4ATFCF4tCGxcdH7IBMTej6zZktSajisQcNNMKYhig/preview?pru=AAABfAoSZOk*tJOYlfpPo58tm2P15YJNcA) that played out in the community's Discord channel. The restart path was taken after efforts to stabilize the network proved unworkable. Ultimately, a second restart patch was released to validators, and the successful reactivation occurred in the early hours of Wednesday.  Still, the return to service wasn't immediate, as noted by the Solana Foundation: "The Solana validator community successfully completed a restart of Mainnet Beta after an upgrade to 1.6.25. Dapps, block explorers, and supporting systems will recover over the next several hours, at which point full functionality should be restored."

DISADVANTAGES

1. Less security

Blockchain doesn’t solve, and false confidence in it makes security weaker

Bruce Schneier 2019 (security technologist who teaches at the Harvard Kennedy School of Government) 6 Feb 2019 “There's No Good Reason to Trust Blockchain Technology” <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/> (accessed 18 Nov 2021)

Do you need a public blockchain? The answer is almost certainly [no](https://medium.com/%40kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec). A blockchain probably doesn’t solve the security problems you think it solves. The security problems it solves are probably not the ones you have. (Manipulating audit data is probably not your major security risk.) A false trust in blockchain can itself be a security risk. The inefficiencies, especially in scaling, are probably not worth it. I have looked at many blockchain [applications](https://www.oreilly.com/ideas/blockchain-applications), and all of them could achieve the same security properties without using a blockchain—of course, then they wouldn’t have the cool name.

Non-Blockchain solutions would have been better

Bruce Schneier 2019 (security technologist who teaches at the Harvard Kennedy School of Government) 6 Feb 2019 “There's No Good Reason to Trust Blockchain Technology” <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/> (accessed 18 Nov 2021)

To answer the question of whether the blockchain is needed, ask yourself: Does the blockchain change the system of trust in any meaningful way, or just shift it around? Does it just try to replace trust with verification? Does it strengthen existing trust relationships, or try to go against them? How can trust be abused in the new system, and is this better or worse than the potential abuses in the old system? And lastly: What would your system look like if you didn’t use blockchain at all? If you ask yourself those questions, it's likely you'll choose solutions that don't use public blockchain. And that'll be a good thing—especially when the hype dissipates.

A/T “But we’re not using “public” blockchain” – Then you’re not really using blockchain. “Private” blockchain is no different from status quo systems we’ve had for 60 years now

Bruce Schneier 2019 (security technologist who teaches at the Harvard Kennedy School of Government) 6 Feb 2019 “There's No Good Reason to Trust Blockchain Technology” <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/> (accessed 18 Nov 2021)

Private blockchains are completely uninteresting. (By this, I mean systems that use the blockchain data structure but don’t have the above three elements.) In general, they have some external limitation on who can interact with the blockchain and its features. These are not anything new; they’re distributed append-only data structures with a list of individuals authorized to add to it. Consensus protocols have been studied in distributed systems for more than 60 years. Append-only data structures have been similarly well covered. They’re blockchains in name only, and—as far as I can tell—the only reason to operate one is to ride on the blockchain hype.