PROPOSAL FOR RESEARCH Ph.D.

Warwick Manufacturing Group

P-H7A2 - Engineering Ph.D. - Full Time

[D R A F T]

The potential of cryptographic, de-centralised, trust-less (blockchain) technology to protect embedded micro-controller networks in connected vehicles.

Steven F. Ratheram.
steve.ratheram@inspiring.co.uk

July 2015.

- Contents -

Abstract.

Contemporary vehicle electronic systems have evolved, since mass adoption 1980s, to become a complex tangle of distributed devices operating on open networks using public protocols.

Hacking is a prescient danger exacerbated by ubiquitous internet connectivity deployed in vulnerable centralised gateways that mediate and span sub networks. Since it serves to multiply so called attack surfaces.

The IoT's vision of *ubiquitous utility* has not reached mass acceptance since it raises concerns about trust. Solving the engineering challenges of secure messaging, identity and authentication that are vital if connected cars are to interoperate safely and gain acceptance on a large scale.

Much has been made of the fundamental innovation of Bitcoin. Whilst the public are attuned to matters of vehicle safety the vast majority remain unaware of the underlying potential of the blockchain.

Manufacturers and OEMs recognise that cryptography has a major role to play in future systems design. The key question is can nascent cryptographic blockchain technology inform automotive network design and if so - how - and can it be demonstrated ?

Urgent research is called for that must not only assures safety but addresses social and political concerns such as privacy and net neutrality. Since in future people will increasingly reject products and services that do not guarantee it.

1. Research Context.

1.1 Vehicle Networks.

The now ubiquitous CAN (Controller-Area-Network) was developed by Bosch & Intel in the late 1980's primarily to reduce sensor redundancy (cost) and harness (weight).

CAN uses differential signalling to afford noise immunity and be tolerant of power fluctuations.
The CAN specification covers the OSI model - *physical* layer (Level 1) and *data link* layer (Level 2) with provision for an *application* layer (Level 7) for HLPs. Higher Level Protocols facilitate diagnostics, development and sector specific solutions such as SAE-J1939 which is commonly used in trucks and buses.

Maximum transfer rates, for optimal integrity and synchronization depend on bus length.
Automotive applications use bus speeds classified as low-medium [125-250 kbit/s ,L<500m]) and high [500 kbit/s - 1 Mbit/s ,L<40m].

CAN is a multi-master, priority based, shared, serial bus consisting of twisted-pair (TP) cable.
Connected control modules are designated as nodes. CAN is fault tolerant and ensures network wide data consistency, error detection and auto retransmission allowing nodes to shut off if necessary.

CAN combines collision sense multiple access / collision detect (CSMA/CD) rules with non-destructive *bit-wise arbitration* (NDA) whereby nodes may detect bus availability and reconcile messages collisions.

Messages consist of *data* frames which include an (8 byte) payload and a unique (11-29 Bit) address. *Remote* frames handle requests for specific identifiers. *Error* frames transmit node errors. *Overload* frames manage delays between frames.

Cyclic Redundancy Checks (CRC) allow all nodes to check message receipt, set flag bits and request re-transmission.

Bit wise arbitration enforces a binary model of dominant (0) and recessive (1) bits. If two messages are sent at the same time the dominant bit will win (IE logical AND). So crucially the address structure confers precedence whereby a lower numerical address has priority.

CAN's intrinsic utility has led to it's adoption in every vehicle sector. It is standard on most automotive micro-processors often with direct memory access (DMA). it's application simplicity for connecting low cost micros's has prompted many applications outside of automotive.

1.2 Vehicle Controls.

Advances in embedded micro-processor based control systems have been driven by emissions legislation and safety regulations, consumer demand for refinement and the market need for differentiation. They have been further boosted by innovation in silicon manufacture and software development methodology.
Modern premium passenger vehicles now contain tens of millions of lines of code, spread across 50–70 independent ECUs and are more complex than the latest fighter jets or passenger aircraft.

Beneath the instrument and infotainment controls visible to most drivers reside a plethora of inter-connected devices. EMS (Engine Management) incl. Stop-Start and ACM (Exhaust after-treatment), TCU (Transmission Control), DSC (Dynamic Stability), IPK (Instrument Pack), BMS (Battery Management), BCM (Body Control) and PATS (Anti-Theft) systems.

To the potential buyer tangible electronic gadgetry represents c30% of the vehicles value.
To the manufacturer software alone amounts to over half of the platform development cost.
To automotive engineers these devices represent a nightmare of real world hazards to consider.

1.3 Safety and Validation.

It has suited manufacturers and vendors to engineer distinct control modules to protect IPR whilst allowing for interoperability and collaborative development. However the resulting topology makes systems integration troublesome and the validation of cross functional controls incredibly complex.

In a typical engine management system, besides performance and driveability related functions, more than half (and growing) of the software is solely intended to *ensure* safety diagnostics and *evidence* robust emissions.

Calibrating the Diagnostic System Manager [DSM] alone in a Bosch MEDC17 EMS, for a single model, can easily take three engineers over a year. An electrical pin and CAN FMEA, assuming extensive automation, a similar time allowing for prototype procurement, actual testing and peer reviews.

Each engineer requires £7-50K worth of development tools, backed up by maybe four vehicles, overseas testing, track hire. Validation fleet drivers covering 3 x 100k+ miles (c£120k) and a HIL rig typically costing £100k+. If the engineers are inexperienced then OEM training can add another £50K.

The ECU documentation, defining each software function with detailed flow charts, can exceed 4000 pages. A short series of automated tests conducted with standard tools might generate 30GB of data for analysis.

1.4 Control Interaction.

Whilst EMS and DSC control modules may collect and process sensor data in the rotational domain. They inter-operate over CAN in the (<100mSec) time domain to manage safety critical functions.

Considerations of optimal message structure, integrity and signal latency are fundamental.
To a module subscribed bus data is as important to normal control function as that of it's own sensors. However If nodes publish corrupt data or receive nothing at all the condition must be detected immediately and fail-safe operation assured.
To illustrate. The Engine Management and Dynamic Stability control systems share powertrain torque data. The EMS and DSC can agree (wheel) torque (MSR) increases or (ASR) decreases in milliseconds.
So on an icy road at night If the DSC detects loss of traction via the yaw or steering angle sensor

and informs the EMS. The EMS validates the command and reduces torque to the wheels until traction is recovered.

1.5 Process Intermediation.

As complexity has grown engineers have sought to address supervisory control and inter-mediation by the introduction of centralised solutions.

Gateways span sub-networks such as LIN (Local interconnect Network), HS-CAN (powertrain) and LS-CAN (body) thereby concentrating access to vehicle systems for the purpose of data aggregation, model/variety configuration and maintenance.

The Body Control Module often mediates both high and low speed CAN networks, LIN, etc. and must concur key-relay energisation with the EMS before and engine can start. Without authorisation from the PATS (Anti-theft) module and the proximity of a driver-key (RFID tag) the EMS will not energise the fuel injectors.

Cruise or active speed limiter requests from the steering wheel are relayed (via LIN) to the central BCM and re-transmitted over CAN to the EMS.

Stop-start systems rely on data obtained from sub-networks such as; ignition status, pedal position, battery state-of-charge, gear and clutch position, bonnet status, driver-in-seat, etc. to operate safely.

1.6 On-board Diagnostics.

Since 2005 On-Board-Diagnostics (OBDII) have converged around international standards such as ISO-14229-3 / ISO-15765-2 whereby UDS (Unified Diagnostics Services) are conducted over CAN via a standard in car DLC (Diagnostic Link Connector) [SAE-J1962] using generic service tools.

Communications allows for a range of diagnostic modes such as data monitoring via parameter identifiers (PIDs) and freeze frames [*modes $01,$02*]. Reading and clearing DTCs (Diagnostic Trouble Codes) [*modes $03, $04, $07, $0A*]. Allowing emissions critical components to be

interrogated [*modes $05,$06*] and statutory [*mode $09*] vehicle reports created.

Crucially both standard and manufacturer specific diagnostic and service tests can be invoked [*mode $08*]. The most recent vehicles supporting UDS extended services [*modes $18-$31*] have enhanced capabilities allowing rapid data monitoring, akin to speed of calibration protocols, and low level access to manufacturer services.

EURO6 emissions regulations mandate that [mode $09] *In Use Performance Monitoring Ratios* (IUMPR) be calculated and prove that safety and emissions critical systems are monitored for over 30% of the the engine's operating time.

The dissemination of manufacturer service diagnostic information is crucial to adding value and delivering profits from the ownership experience. In turn this spawns countless sub tier enterprises delivering solutions and hardware that use these standards.

These days an ECU's diagnostic system manager [DSM] functions are calibrated concurrently with performance, emissions and driveability. In deference to web standards OBD PIDs and DTCs are expressed in an XML file according to the ASAM ODX (Open Diagnostic Exchange) standard.

1.7 Use of Cryptographic Techniques.

Cryptographic techniques are commonly used in vehicle controls but not in a robust manner.
For example RSA encryption is used in 'extended' OBD UDS sessions. Access to low level, manufacturer specific, functions and module re-programming normally requires a security DLL.
Dealer service tool must routinely support these functions. So the security 'seed and key' DLLs must compiled and released to 'trusted' third-parties world-wide.

After a manufacturer has released an engine control system for production, the supplier OEM may spend up to three months validating safe operation and configuring high level safety monitors that detect and mitigate irrational dynamics.

Preparing production ECU software involves obfuscating the data whereby checksums and signatures are inserted in the ECU file via process known as HEX post treatment. Normally, but not

always, at this stage development protocols are removed or protected with the security DLL.
However checksums that prevent arbitrary tampering with production code and data may be de-activated in ECU RAM if the memory address of the boolean value concerned is known.

1.8 Development Protocols.

Hidden development protocols such as (CAN Calibration Protocol), XCP or arcane interfaces such as ISO K-Line (KWP2000, McMess) offer deep access to controls but remain secure only by obscurity.

Such protocols address the needs of stake-holders in the vehicle eco-system whom are concerned with development (calibration), end of line test (configuration), dealer (diagnostic) or legislative (compliance).

Engine control software is extremely complex. Optimal engine performance relies on the robust calibration of characteristic data comprising hundreds of control functions, thousands of 2D/3D/4D (pedal, ignition angle, fuel limit) *lookup tables*, discrete control *parameters* and and *variables* (speed, torque, boost) residing in physical memory.

For development purposes CCP, adopted globally, establishes a continuous, master-slave, connection allowing primitive memory transfers between the slave ECU and a calibration tool.
CCP uses two reserved CAN IDs for Data Transmit Objects (DTO) and Command Receive Objects (CRO). These carry messages as regular data that perform direct read / write operations upon control parameters residing in ECU RAM in near real-time.

Accordingly a driver pedal map or a vital unitary constant that dictates the EMS consult the immobiliser - even computed output variables, such as those directly controlling fuel quantity or start of injection, may be manipulated in a split-second manually or programatically.

1.9 Micro-processor Interfaces.

Tools to facilitate the calibration of control functions operating in the crank domain, such as knock sensing, use memory emulators [ETKs] to provide very fast monitoring and flash re-programming. These interfaces high-jack the micro-processors own debug interfaces such as AUD, NEXUS and

JTAG and can operate at one hundred times the speed of CCP.

Since automotive micro-processors are COTS designs many generic tools exist. These same tools are widely used chip-tuners to re-programme engine controllers. To extend the performance of a vehicle beyond it's design limits can involve changing as few as seven critical memory locations governing characteristics such as torque limitation and turbocharger boost.

1.10 Security by Obscurity.

During development the overall structure of the messages to be exchanged between nodes is pre-defined in a symbolic ledger known as a CAN database. Other more recent automotive networks such as LIN [.LDF] and Flexray [FIBEX] adopt similar approaches.

The [CAN.dbc] file produced contains addresses, messages and signals published by each node and discloses the CAN IDs of messages relating to OBD diagnostic and CCP. The CAN database is a non-encrypted text file and although sensitive often needs to be shared amongst developers and suppliers.

OBD PIDs and DTCs are commonly defined in a manufacturer Part 4 diagnostic specification. This is later expressed in a, handy to parse, XML file according to the ASAM ODX standard. This schema extends to every control module in the entire vehicle and includes the information required for module re-flashing.

The actual layout of control parameters in memory at run-time are typically documented in a non-obfuscated text file generated when the ECU software is compiled and linked. According to ASAM MCD standards these .A2L files describe all available (CAN/OBD/CCP/ETK) interfaces and the physical memory address of every map, curve, control parameter and variable in the ECU.

Aside from an ECU pin/harness diagram all of the information required to access the ECU is contained within *three* important text files. Whilst access to these files is restricted dozens of engineers and suppliers whom collaborate globally to calibrate an engine control system require them.

Evidently security by obscurity cannot be relied on. For without access at least some data from these files the chip tuning industry could not have moved on from 'placing it's hand in a barrel of snakes'.

1.11 The adoption of web standards.

As internet standards have advanced so too automotive systems have adopted WiFi to solve physical challenges such as remote tyre pressure monitoring. More recently wireless technologies have extended beyond GPS and GPRS to applications such as intra-vehicle mesh networks.

Drivers seek mobile productivity and thus demand connectivity. Legislators mandate compliance and generally require evidence. In many vehicle applications CAN bus loading becomes critical and sub networks are spawned which in turn require intermediation. Consequently control system requirements and complexity grow.

Many better performing network standards compete for dominance amongst them Flexray, CAN FD offering faster data bit-rates and more interestingly Automotive Ethernet.

In bandwidth terms Automotive Ethernet offers performance akin to a dedicated twisted pair CAN bus for each individual message. In practical terms anything ever invented to work with Ethernet might potentially be re-used in a car. If it succeeds then the automotive supply chain will be disrupted by countless new market entrants whom have cut their teeth out there on the web.

Vehicle topology will start to resemble web infrastructure. Hubs will replace gateways, users granted roles and communication interfaces built onto the silicon itself will be capable of continuous communication using internet protocols.

1.12 Connected Vehicles.

Modern vehicles 'go out connected' and most manufacturers talk a good 'cloud strategy'. They play down privacy issues so as not to appear overly focused on the potential savings in warranty costs and revenue from monetising 'big data'.

The problem is the data gathered is often managed on back-end systems consisting of - to quote the CTO of a British global vehicle manufacturer - *"70s designed, '80s deployed and operated, overloaded applications which run in the business"*.

State legislators advocate more onerous monitoring under the guise of road safety. The political and social outrage that these policies can provoke are not widespread - yet.

The IoT's vision of ubiquitous *utility* has not reached mass acceptance since it begs the question - *for whom?*. It's failure to gain mass adoption due to the association with privacy, moreover state surveillance and corporate hegemony, cause mistrust. This illustrates how progress is being held back.

1.13 Dis-intermediation.

Wherever security warrants that disproportionate amounts of trust be vested in a relatively few individuals history has shown that trust eventually breaks down.

It is now widely acknowledged that the promise of billions of IoT connected devices has failed to materialise because; single point of failure, broken by design, centralised solutions for mediation and authentication cannot be relied on. [7]

The existing paradigm of centralised, trusted intermediaries be they programmatic or human is unlikely to deliver robust trusted solutions. Servers simply fall into two categories - those that *have* been hacked and those that *will* be hacked.

1.14 Attack surfaces.

Hacks that exploit public OBD protocols via CAN are well documented [2]. Others use denial of service (DOS) techniques to flood a node with requests and force it to shut down IE Bus-off [3].

These scenarios are covered in CAN FMEAs. In all operating states, nodes are spoofed with corrupt data and bus behaviour observed. To perform such a test on a running HIL Rig takes three mouse clicks.

The systematic scanning of PID address is a technique also used by development tools to identify those which are responding and populate an ODX template for use in other applications.

Bus-off states trigger multiple diagnostic alerts but safety critical modules detect them and adopt fail-safe states. In any event, EMS safety monitoring functions governed by modelled plausibility and dynamic vehicle react immediately, the engine de-rates, lost frame are counted and the ECU switches to replacement data. Much the same can be achieved by shorting the physical CAN_H and CAN_L signal lines at the OBD connector.

During validation every ECU pin is tested - whilst driving - for electrical; open circuit, intermittent signal / contact (corrosion), shorts to 12V/5V supply and ground - whilst concurrently monitoring software fault detection in RAM via an ETK and resulting diagnostic messages via OBD on CAN.

In order to mitigate such attacks FMEA dictates that every conceivable fault state be ranked for severity, occurrence and detection. Hardware or software design changes must be made to reduce aggregate risk to acceptable levels.

Concerning re-programming modules via the micro-processor debug interface using generic tools.
Successful ECU programming, of production controllers, relies on knowledge of memory size, code / data partitioning and requires a security DLL. There is no doubt that without an ECU SW function definition and key data from confidential A2L file this would not be easily discovered.
It is said the best bootlegs are recorded by the original artist - and even sanctioned by the label.

Hacking OBD on CAN is straightforward for anyone with access to the vehicle [3].
Even legitimate applications use CAN-Bluetooth interfaces to combine sampled data with phone devices such as accelerometers to measure vehicle performance. Devices and OS that support both electrical and WiFi/Bluetooth-CAN interaction are readily available. The danger is that a poorly integrated device is reprogrammed with malware to mount a concerted attack.

In the dark on an icy road. A hazardous environment readily detectable by vehicle systems. Should loss of traction occur AND the EMS-DSC ASR/MSR requests be subverted the EMS will cope.

Though It would be a different matter if development protocols were still active in the ECU.
IF checksums were disabled CCP could programatically overwrite control data from a distance.
All that might be required would be a Raspberry Pi with CAN (*and code*), WiFi, and a hot-spot set up on the phone. The code on the Pi could be activated remotely via a web browser.
Wireless data packets have been successfully exchanged between vehicles travelling at 160 mph.

1.15 Identity and Authentication.

Imagine that the car braking in front - or five cars in front - wirelessly transmits the exact force and timing of the braking to every car behind it ?. Or a car five miles ahead informs every following vehicles of congestion or an accident ahead?

"Ford estimates that one in 10 cars would have to be part of this wireless network to create a high-resolution, real-time traffic map. One in three cars would need to be connected to increase public safety." [4]

To make this a reality the vehicle identities must be robustly authenticated and their real time-position securely transmitted. In a connected car users will expect control of profiles and private data. So the real challenges are *secure random number* and *pseudonym generation*.

Continental estimate that between 1000 and 5000 IDs per car may be required. Which in Germany means 2.9*10^11. In short, the secure operation of 'connected' vehicles, at scale, will rely on hitherto hard to guarantee security. Continental [1] believe that any successful solution must address technical, financial and social targets by balancing security and privacy.

Trust will become a crucial attribute since in future people will reject product and services that do not guarantee both security and privacy. Driver-less cars cannot hope to reach acceptable safety levels and mass deployment without it.

1.16 Bitcoin.

When Satoshi Nakamoto published the Bitcoin white paper on a cypher-punk website in 2008 it was initially dismissed. Many leading developers believed distributed consensus to be impossible to achieve [13].

Seemingly out of nowhere it called the convergence of internet technology and the results of two decades of intense development by nearly anonymous crypto-garphic researchers.

The Bitcoin protocol's major discovery is to claim to have solved the elusive "Byzantine Generals Problem". Ensuring message integrity end-to-end without corruption and reaching consensus across a distributed network without the need to trust a central intermediary.

If it proves to have done so it may herald a new network design paradigm and become the most important computer science innovation since the world-wide-web. For which 'currency' is merely the first obvious application, just as email was to the internet.

"technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it." [12].

1.17 The Bitcoin Protocol.

Bitcoin is a open-source protocol. A network centric platform for recording ownership and trust on a peer-to-peer basis. It may be better though of as a digital bearer instrument, a value exchange mechanism, currency as a content type or essentially *programmable money*.
Crucially this implies that embedded devices can conduct complex transactions securely according to programmatic rules.

The Bitcoin eco-system secures crypto-currency transactions by leveraging the combined hashing power of a trust-less, dis-intermediated, P2P network.

It uses pseudonymous public (addresses) and private key encryption, based upon asynchronous elliptic curve digital signatures [ECDSA] and secure hashing [SHA] algorithms. These combine to

instantiate transactions featuring one way mathematical trap doors that are relatively easy to verify but very hard to decompose. The protocol rewards miners for risking energy and computing power to validate transactions by conducting proof-of-work.

Bad actors capable of subverting the network, are dissuaded since, should they posses the vast resources needed to mount a 51% attack, they must suspend self interest. For they stand to gain far more by abiding by the rules and winning Bitcoin.

So equilibrium is maintained. New coins are created algorithmically by the protocol. The mining 'block reward' halves every four years. The production 'difficulty' is controlled to be ten minutes hard irrespective of the amount of participating peers. The difficulty of mining decreases if participation falls.

The protocol uses game theory to derive majority consensus about transactions assembled into blocks by validating cryptographic inputs to confirm entitlement. This is represented in the form of an immutable shared ledger (the blockchain) constructed on a longest chain wins basis.
Every peer has access to to an up to date copy, even if nodes leave and re-join the network at will.

1.18 Potential Applications.

The Blockchain is heralded as a solution to; notarisation, asset transfer (Factom), smart multi-signature contracts (via OP_RETURN scripts), tokenisation (coloured coins), DNS (Namecoin), distributed computing (Ethereum) and indeed entire new models of commerce. In economic terms, for two thirds of the world that are unbanked, it may prove profound.

IBM has cited the blockchain as the solution to IoT identity, sensors ubiquity, privacy and device democracy. [7]. They describe ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) where network-connected devices can interact autonomously on the IoT using freely available technology including bittorrent, Telehash, and bitcoin.

Bitcoin enables frictionless, high lubricity transactions and promises innovation without permission. There is no doubt it will be equally disruptive in the automotive space.

Whilst libertarians heap ideals upon it and herald it a bulwark against intrusive surveillance. The salient political question is that of privacy VS public safety. The technology of bitcoin remains far from the public consciousness. Whilst many seem prepared to cede freedom to the threat of vulnerability the irony is that de-centralisation may reduce systemic risk.

2. Research Questions.

The primary question is can cryptographic, de-centralised, trust-less (blockchain) technology be used to protect embedded micro-controller networks in connected vehicles ?.

How might cryptographic digital signatures and secure hashing algorithms be applied to secure messaging in automotive electronic controls ?.

Can psudonymity address; identity, authentication and privacy in connected vehicles ?.

Can dis-intermediation reduce vehicle vulnerability and attack surfaces ?.

How might decentralised, immutable ledgers protect network symbolic databases from hacking?.

What might be the benefits of distributed file storage to vehicle data management ?.

How might future vehicle sensor and mesh networks be designed to reconcile safety, security, net neutrality and device democracy ?.

3. Research Methods.

My research intends to combine over 25 years of experience calibrating and validating automotive electronic controls with a profound realisation of the innovation possible with nascent blockchain technology.

Moving quickly on from known attack points to extend research thus far conducted [2,3] and expose undisclosed vulnerabilities using UDS extended diagnostic and lesser known development protocols based upon the researchers own experience. Focusing on failure cases that represent high *severity*, may well *occur* and yet are difficult to *detect*.

The major task is to examine how crypto-currency and vehicle networks relate, in theory, and determine the extent to which the technology might be applied ?. The aim being to abstract design characteristics.

To devise vehicle specific equilibrium policies and cost functions that proxy Bitcoin's proof of work. Establish key metrics and derive models that allow simulation of cryptographic techniques in a real vehicle. To consider the feasibility of cryptographically secure transactions between controllers given the computational resources of available devices. And by observation and data correlation attempt to assess their potential benefits.

Tests will involve practical experimentation with ECU/networks in a recent production vehicle gathered on public roads and test tracks. This may include third party data, offered on a confidential basis by manufacturers or OEM's

Experimentation will necessitate full node access to the blockchain in vehicle for testing and executing crypto-graphic functions via APIs.

Experiments will involve monitoring controller and network data and be conducted using industry standard equipment supporting ASAM standards including telemetric monitoring and ideally rapid-prototyping tools.

Data analysis will be conducted with industry standard applications, ideally supplemented by modelling and simulation tools likely to be used widely within WMG.

Beyond answering these key questions outcomes might include the development of useful tools and techniques, learning materials, a road map, topology guidelines or contribution to new standards or protocols. Also to represent both the sponsor and the university in terms of subject expertise and advocacy.

4. Significance of Research.

Vehicle hacking is a prescient danger. Threats increase when intermediate gateways become connected to the internet since they expose safety-critical control modules and render them vulnerable single points of failure.

Cyber security advocates believe the need for research to be urgent given the economic and societal importance of vehicles [5]. If the research is to lead to real improvements it must involve the industry itself. Research will require specialist knowledge, a detailed understanding of the underlying technology and consideration of threats posed to vehicle systems in a connected context.

This is timely since very recent press articles exposing vulnerabilities in certain vehicles have exacerbated public concerns and prompted manufacturers to rush to fix them. Recently manufacturers have been forced to recall vehicles due to problems associated with key-less entry. They are well aware of the associated costs and impaired reputation.

Research conducted from an objective engineering perspective is more likely to elicit the co-operation of manufacturers whom are sensitive to matters of safety, security and product liability. It may also head off regulators whom typically impose regressive centralised approaches which might actually impair safety

As manufacturers attempt to unlock the added value of connectivity they struggle to solve the engineering challenges of secure messaging, identity and authentication that are vital if connected

cars are to interoperate safely on a large scale.

Major OEMs acknowledge concerns and recognise that cryptography has a major role to play in future systems [1]. Industry centric research that informs rather than sensationalises may lead to a more candid exchange and hasten adoption.

In order to preserve the essential value proposition that underpin consumer demand - freedom and mobility. Auto-makers must not just focus on safety within technological and economic constraints but advocate ways forward and address social and political concerns such as privacy and net neutrality. Because in future people will increasingly reject products and services that do not guarantee their privacy.

Nascent blockchain technology and automotive control clearly warrants symbiotic comparison.
If the benefits of crypto-currencies and the blockchain grow in the public's wider consciousness, prove robust and become trusted. Then perhaps they may contribute to public reassurance at large *and answer the question* **-- how best shall we drive trust.**

5. Bibliography. [ref]

[1] - H. Gregor Molter, (2015). Automotive Security and Privacy - Future Challenges for the In-Vehicle Network, Continental AG.

[2] - Dr. C. Miller & Chris Valasek (2015). Adventures in Automotive Networks and Control Units.

[3] - Eric Evenchick, E. (2015), Hopping On the CAN Bus, Black Hat Asia.

[4] - Anthony, S (2011), Ford working on car-to-car wireless mesh network for real-time telemetry and government use. (extremetech.com).

[5] - Cotton, R. (2014), NCC Group launches Automotive Cyber Security Research Partnership with the University of Warwick, (warwick.ac.uk/newsandevents).

[6] - Ratheram,S, (2015), Keynote : Driving the Blockchain. Symposium on Powertrain Controls. Birmingham City University.

[7] - IBM, (2015), Device democracy. Saving the future of the Internet of Things. IBM Institute for Business Value.

[8] - Higginbotham, Stacey (2014), "Check out IBM's proposal for an internet of things architecture using Bitcoin's block chain tech".

[9] - Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System.

[10] - Andreessen, M. (2014), Why Bitcoin Matters, New York Times.

[11] - Andreas A. Antonopoulos (2014), Mastering Bitcoin, O'reilly Media.

[12] - Prof. Maurer, B. & Prof. Patterson D.J, (2014), online course, "From Barter to Bitcoin: Society, Technology and the Future of Money".

[13] - Maxwell, G. at al. (2014), Enabling Blockchain Innovations with Pegged Sidechains, Blockstream.

[14] - Irvine, D. (2014), MaidSafe.net announces project SAFE to the community, github.com/maidsafe

[15] - Buterin, V. et al., V. (2014), Ethereum White Paper: A Next Generation Smart Contract https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf

oo0oo