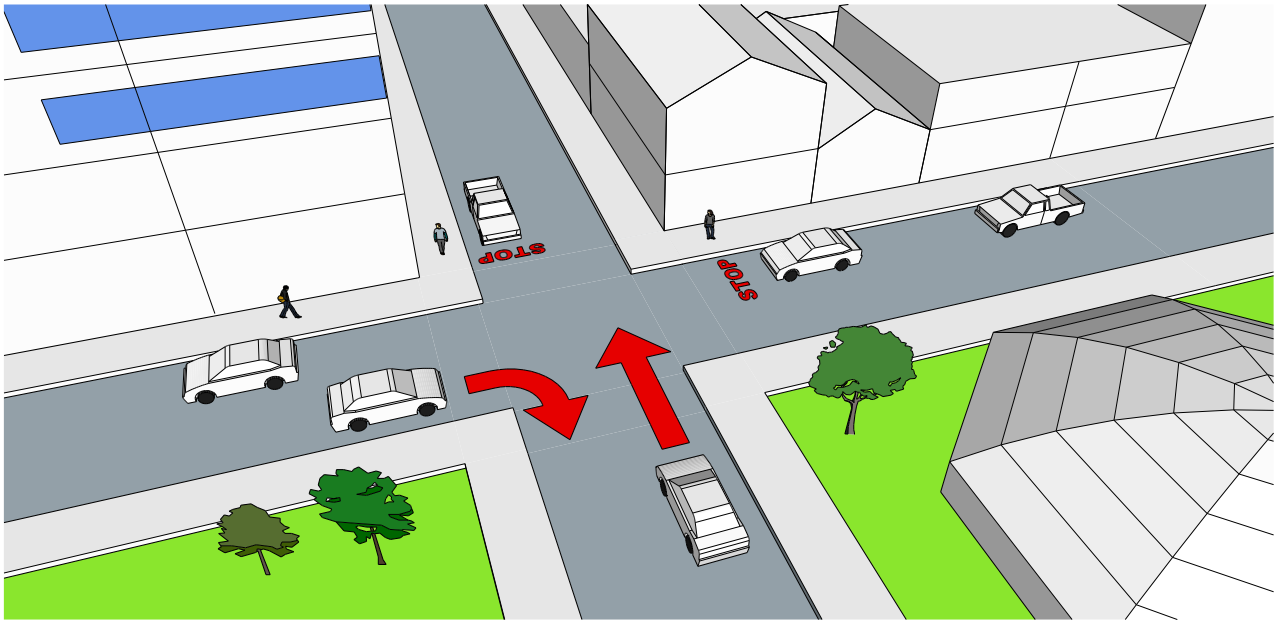
Blockchains and Content-Centric Networking for Trusted 5G Vehicular Networks

Victor Ortega, Casa Systems
Fayza Bouchmal, Universitat Politècnica de València
Jose F. Monserrat, Universitat Politècnica de València



Vehicular communications are already a reality, but they still need to evolve in order to support higher throughput and, above all, ultra-low latency to accommodate new use cases such as the fully autonomous car. In addition, cybersecurity must be guaranteed, since the risk of losing control of vehicles in the face of an attack is undoubtedly a matter of national security. This article presents the technological enablers so that all these requirements can be reached: under the umbrella of a dedicated network slice, this article proposes the use of Content-Centric Networking instead of conventional TCP/IP routing, and permissioned blockchains that allow controlling dynamically the reliability of the source and the integrity and validity of the information exchanged.

Introduction

It is 7 AM, thousands of commuters join the motorway on their way from home to their place of work. Fully autonomous cars are not widespread yet, but many drivers prefer to make use of the autopilot and leave the car drive the boring trip to the office. Vehicles exchange their intentions and neatly organize themselves increasing the efficiency and avoiding traffic jams. This is not science-fiction, although it still requires some more time to become a reality.

One of the key aspects to make this feasible will be the vehicle to vehicle (V2V) and vehicle to any other element of the road (V2X) communications. 5G will bring new capabilities to these connected vehicles: higher capacity, lower latency, edgeless connectivity, and a radical change of the connection paradigm enabled by network slicing [1]. With network slicing, the 5G network will adapt to the requirements of the vehicles and not the contrary. This is a unique opportunity to forget about old network conventions and embrace new technologies.

Conversely, one of the main requirements of a network formed by a large quantity of heterogeneous devices is trust. For instance, vehicles regularly will send cooperative awareness messages (CAM) to inform other nodes about their status. In this framework, faulty or malicious vehicles could

easily destabilize the network sending untrue messages, causing traffic retentions or even accidents.

It is therefore necessary to guarantee the veracity of the shared information, providing the means to verify the origin and reliability of the transmitted data. Past studies have shown different approaches to the problem and concluded that the most efficient solution consists of a distributed network of trusted validators [2]. This article explores the advantages and challenges of complementing centralized control or even replacing the traditional client-server architecture by fully autonomous and decentralized permissioned blockchains. The main objectives are to eliminate the risk of data tampering or corruption, provide robustness, high performance and reduced costs. The next section introduces and analyses the proposed blockchain solution. Afterwards, in order to improve the protocol efficiency and mobility, we propose combining the blockchain with content-centric networking (CCN) [3] and 5G network slicing.

The last section draws important conclusions and future research lines derived from the combination of the named elements: permissioned blockchains, CCN and network slicing.

The vehicular blockchain

When Bitcoin was released as open-source, the term blockchain was linked together with it in the same solution. Bitcoin was the first application of a blockchain, but today blockchains are a widespread and very powerful solution with a growing range of network applications [4]. This section aims at introducing this concept and how it fits with vehicular ad-hoc networks (VANETs).

Overview

In the last years, we are witnessing the transition from centralized computing and storage to decentralized architectures and systems. Cloud computing has enabled global access to Internet services as social networks or video streaming from a variety of devices. However, although these services are decentralized in terms of servers, they are still centralized around a handful of client applications or web services.

Blockchain and the distributed ledger technology is one key innovation that may allow creating completely decentralized services. A distributed ledger is a replicated and synchronized database physically spread across several locations and entities that agree in the validity of the data. Each node in the network participates in the administration of the database. The consensus protocol guarantees the security of the network and integrity of the data.

Although Bitcoin was not the first distributed ledger, it added the concept of mining and cryptocurrency and, ultimately, popularized the blockchain technology. However, the technology is not limited to cryptocurrencies. To understand its possibilities, it is necessary to know the three basic components of a distributed ledger:

- The **data model** that captures the ledger.
- The language of **transactions** that change the ledger.
- The **consensus protocol** that controls which transactions are included in the ledger.

All three together define the blockchain and are prone to be changed according to the requisites of the application. For example, while the Bitcoin blockchain uses *proof of work* (PoW) as the consensus algorithm, other blockchains are proposing a large variety of consensus algorithms, like *proof of stake*, *proof of burn*, *proof of capacity*, *proof of elapsed time*, and many others [5].

A blockchain is typically an ordered and timestamped list of blocks comprising multiple transactions. New blocks are added in a secure cryptographic way that is permanent and unalterable. Besides, the blockchain database is not stored in any single location, each entity belonging to the distributed ledger independently stores its own copy of the blockchain. At any given moment, more than half of the nodes in the ledger need to have exactly the same blocks in their blockchain. This state is known as *consensus*.

Because the database is distributed, several nodes will try to add a new block with transactions at the same time. In order to avoid disagreements, a consensus protocol is needed. Bitcoin solves this problem with a mathematical operation that processes the new block applying multiple hashes until the result of the hash operation contains a specific number of zeros in a row. The hash operation is extremely complex and forces computers to compete until one of them gets the next valid block. This process is referred to as mining. Every added block includes an encrypted reference to the previous block so as to guarantee that the blockchain is consistent and unaltered.

Mining has demonstrated its validity and popularity but also important flaws. Especially problematic are the huge amount of processing resources expended and the extremely limited transaction rate. Considering this, it is unavoidable to look for a more appropriate consensus mechanism.

Amongst the most important alternative blockchains, Ethereum introduced the concept of smart contracts [6], and IOTA, a cryptocurrency for Internet of Things (IoT), changed the data model for a most complex Directed Acyclic Graph (DAG) system, which may provide faster data processing.

One of the most promising developments is Hyperledger, an open source effort created to promote cross-industry blockchain technologies. Hosted by The Linux Foundation, it is a global collaboration of members from various industries and organizations.

Since we are still in the early days of blockchain technology, there is no agreement on standards in the developer and business communities. Standards are critical in ensuring interoperability and avoiding risks associated with a fragmented ecosystem, not just for the distributed ledger itself, but also to support services. For this reason, it is so important the collaboration between the open source community and the industry.

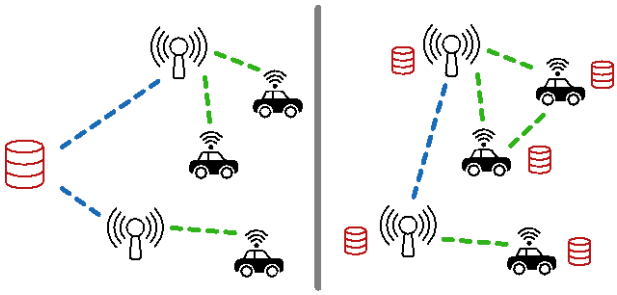


Figure 1 *Distributed ledgers will provide faster access to the information than traditional cloud computing.*

Permissioned blockchains

Traditional blockchains like Bitcoin are permissionless. Anyone can join the network, create new transactions and add them to the ledger. The reason because Bitcoin scheme is viable is the mining process and the cryptocurrency attached to it. In contrast, permissioned blockchains are closed and monitored systems where the access is well defined and differentiated based on roles. Hyperledger offers a framework whose main purpose is to allow creating enterprise grade, open source, distributed ledgers and code bases to support specific business use cases. As the main difference with Bitcoin, the resultant blockchain does not need to be cryptocurrency-based and can implement more suitable consensus protocols.

Considering VANETs as enterprise networks formed by different automobile manufacturers, transportation companies and government entities, permissioned access is a must for the sake of the security of the network. To allow this, each vehicle and road-side equipment will be linked to a digital identity [7]. Permissioned blockchains provide the security of a private network, keeping the advantages of a distributed ledger.

	Bitcoin	**Hyperledger framework**
Cryptocurrency based	Yes	No
Permissioned	No	Yes
Anonymous	Yes	No
Privacy	Yes	Yes
Immutable ledger	Yes	Yes
Distributed	Yes	Yes
Smart contracts	No	Yes
Consensus protocol	Proof-of-Work	Several options
Transaction rate	Very low	High

Table 1 *Comparison of Bitcoin and the proposed blockchain framework.*

Creating a distributed ledger to quantify the trust in the nodes of network

One of the most promising applications of using distributed ledgers in VANETs is to democratize the trust in the vehicles (and other devices like road-side units) that are part of the network. Each participant of the network can potentially verify the data transmitted by other participant and inform the network about its reliability. Afterwards, the consensus protocol validates and add the new information to the ledger. The stored information is distributed and made available to any other vehicle for future reference. The usage of own and others observations to identify the behaviour of nodes has been successfully employed in the past for misbehaviour detection [8]. The idea now is to use it within the context of a distributed ledger to guarantee trust in the VANET.

The process begins when a new vehicle enters the network. Despite being a new participant with no previous history, it can already start sending information to the rest of the vehicles. For example, its CAM messages. The vehicle shall always use its private key to add a digital signature to all its transmitted messages. With this basic mechanism, the rest of the network, the receivers, can unequivocally identify the source and verify that the message has not been tampered.

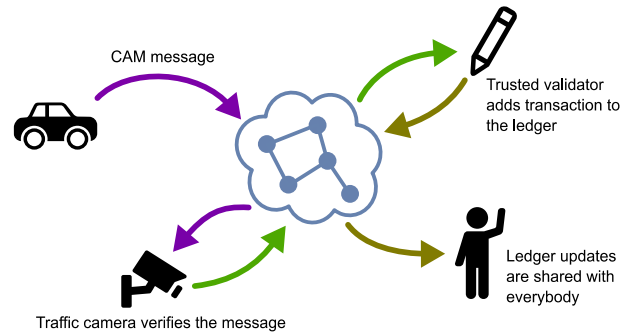


Figure 2 *The verification process gives veracity to the data transmitted by vehicles.*

However, although the identity of the sender and the integrity of the message can be immediately verified, the veracity of the content must be put under suspicion. It is the task of the receivers to verify the content. Nearby devices, equipped with their own cameras and location services, have the capability to verify the received messages. As far as technically possible, the receiver should compare the sender message with their own estimation of the same information. For example, the receiver could estimate the exact location of the sender based on the detection of the sender in the camera or could check that its declared speed and direction corresponds to its estimations.

This verification process adds veracity to the data transmitted by the new vehicle and can be stored in the ledger. Moreover, the process is accumulative and provides different degrees of veracity. For instance, after several transactions in different locations, the new vehicle will have received different reviews from different participants and all this information will be available in the ledger. Moreover, similarly as other distributed ledgers do, when the majority of reports confirm the validity of the sender, it could be added as a secured node in the blockchain. In this sense, the blocks of transactions in our proposal become blocks of trustable nodes for the VANET.

It is important to remark that the distributed ledger provides the means to store and share certified data. Due to the heterogeneous nature of the participants, it would be vendor discretionary to decide upon how to interpret this information or how to revoke this certify when a node starts behaving in a non-trusted way.

The consensus protocol

In a traditional blockchain as Bitcoin, the consensus protocol consists of a competition between miners to solve a cryptographic puzzle as fast as possible. This process, known as *proof of work* (PoW), requires enormous amounts of computational power and the winner is rewarded with newly created cryptocurrency. This scheme has demonstrated its validity in the real world but has serious scalability issues, and several alternatives have arisen over the last years.

The most accepted alternative is *proof of stake* (PoS). It has been already implemented by other cryptocurrencies and it is expected to be put under real test when Ethereum, the second most popular cryptocurrency, starts using it likely in the near future [9]. Despite being more resource friendly, PoS has the same limitation of requiring an attached cryptocurrency. Without the possible gain or loss of coins, there is no stake, and the scheme is unworkable.

While PoW and PoS approaches cannot be applicable to VANETs because they require cryptocurrencies, Hyperledger framework proposes a broader concept of consensus that do not require high processing PoS. These alternatives are faster and more scalable but provide lower security against malicious or faulty nodes [10].

Thanks to the permissioned blockchain, the lower security is not an issue. The ability to modify the ledger can be granted only to a trustable group of validators and, subsequently, use one of the faster consensus protocols. As a possible improvement, the same verification system used to detect trustable transmitters could be ultimately used to decide the validators of the network. Besides, in case of attack or malfunction, one compromised validator could be quickly expelled from the network by the rest of the validators.

Further study in this direction will allow defining the right consensus protocol capable of dealing with the properties and limitations of vehicular ad-hoc networks.

Increasing the performance with content-centric networking

At this point, it can be concluded that the use of a permissioned distributed ledger provides multiple advantages in the creation of trusted VANETs. Especially important are the scalability, reliability and autonomy of the final network. However, VANETs also require efficiency, speed and adaptability to a changing network.

Traditional blockchains are slow because they rely on complex peer to peer protocols needed to work over long-distance TCP/IP connections. VANETs however provide short-distance, low latency connections. Moreover, thanks to the 5G network slicing concept, a parallel network can be set up to carry specific VANET traffic and, as last instance, there will be no need to still rely on TCP/IP connections. This topic will be discussed in the next section.

Several studies have shown that the TCP/IP networking approach is outdated, and its drawbacks can be overcome by using Content-Centric Networking [11].

CCN philosophy decouples the content from the classical client-server paradigm. Conversely, data can be stored in all nodes, which can send it whenever another node ask for this content using a kind or identifier or name univocally pointing to these data. Rather than having IP addresses, CCN identifies contents, which simplifies caching and forwarding from multiple sources.

In a CCN approach, after the users selects a content that wants to retrieve, the node creates a so-called interest packet and forwards it to nearby nodes, which check if they have this content already stored. If this is the case, the content is sent directly to the source of the request. Otherwise, the interest packet is forwarded including new labels about the routing. The main novelty is that in CCN any node may copy and store any content it forwards, whereas in classical Internet only the original host or a limited set of servers can make this caching.

In the case of supporting a distributed ledger for vehicular safety, CCN seems exactly the right choice:

- CCN is based on two main packet types: interest and content. Interest packets would be used for transactions and to request pieces of the blockchain (represented with a green arrow in the left part of Figure 3), while the content would be the blockchain itself (blue arrow in the left part of Figure 3) or a safety local broadcasting message (blue arrows in the right part of Figure 3).
- Automatic caching. This means no need to expressly store the blockchain. When a node needs to access the content of the ledger, it uses a CCN request. If the desired piece is already in the cache, it is immediately available. Otherwise, it is requested to the network.
- It is natively P2P. No need to implement inefficient protocols over UDP or TCP connections.
- Reduced congestion and latency. Something of critical importance in VANETs.
- No IP addresses. Participants communications is based on the type of data, content and identity, not in the source or destination network addresses. This increases speeds, reduces the number of hops and eliminates redundant messages.
- Security model is oriented to messages instead of connections. Complex end-to-end connections are unnecessary because individual messages are explicitly secured.
- Adaptive and dynamic. CCN routing can easily cope with the volatility of VANETs [12].

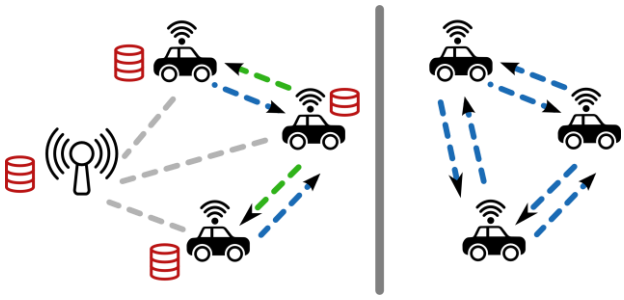


Figure 3 *Different alternatives for the communication using CCN. Interest packets are represented in green and content packets in blue.*

It is important to highlight that CCN is a good networking candidate for V2X communication, not only because its good alignment with the distributed ledger paradigm, but also because V2X are by definition a kind of local communication type in which the addressing is not as important as the proximity of the nodes. It is, therefore, more interesting for V2X communications to forget about conventional TCP/IP architectures and focus on content delivery with simple MAC protocols and CCN networking.

In summary, the combination of CCN and the distributed ledger will simplify and empower network efficiency. Note that the proposal is to use CCN not only for the distributed ledger exchange, but also for the broadcasting of safety messages, since in most cases they can be efficiently cached.

Secure Content-Centric Networking

The synergy of blockchains and CCN is not only one way. Past studies have shown that CCN is susceptible to receive Denial-of-Service (DoS) attacks [13]. This attack consists of flooding the network with interest packets. The problem is that CCN security checks cannot verify whether the interest is legitimate or not.

The distributed trust system would easily avoid this kind of attacks. In the combined system, interest packets need to be signed by the senders and their identity and trust rating is known by all the network. Basically, only packets signed by trustworthy nodes would be treated as real Interest packets.

Blockchains adds a new layer of depth to CCN that is out of the scope of this article but is asking to be researched in more depth.

Network slicing

Contrary to previous mobile technologies, the 5G technology aims at providing a unique solution to comply with heterogeneous services and requirements [14]. The novel network slicing concept enables operators to deploy, on demand, multiple logical instantiations of its physical network, each one isolated and fully dedicated to a specific service.

To efficiently support network slicing, Network Function Virtualization (NFV), Software Defined Networking (SDN), and Software Defined Radio (SDR) concepts need to be integrated. NFV separates network functions from the hardware they run on, by using virtual hardware abstraction mechanisms. This approach enables to configure, select, and allocate network functions in software that runs on commodity hardware, and that can be placed in different network locations without requiring additional network equipment. SDN is a solution to instantiate and configure network elements and software by decoupling the control-plane from the data-plane [15]. The basic idea of SDR is defining specific radio procedures that can provide flexibility, agility, and responsiveness to be easily adapted and deployed on the virtualized baseband units, including the radiofrequency part.

With 5G network slicing it will be possible to create VANETs based on CCN as depicted in Figure 4. In this slice, any vehicle will be able to communicate with their neighbour vehicles and road-side equipment without needing to know anything about them. All nodes will automatically create a mesh network, where they could be in the same 5G cell, neighbour cells or even in different operators. Thanks to SDR, the transceiver could adapt to several Radio Access Technologies (RATs) (in the figure, there are two, one for regular Internet access and another for V2X). NFV allows the telematics unit to treat data in a different manner depending on the slice, and this is how, software-based, CCN can be easily integrated in this solution, acting as an isolated network but integrated with the rest of the operator services.

The main benefit of creating this additional network slice for V2X traffic is that the resultant CCN does not have IP traffic and acts independently from the rest of the operator network. The separate network will have all the benefits of CCN and the permissioned distributed ledger without requiring any additional hardware from the operator side. This is a completely software-based permissioned blockchain with the power of CCN. Note the relevance of the network slice manager, which is a new entity that requires for a more detailed investigation.

In the V2X network slice operated with CCN, vehicles would share with other nearby vehicles or road side units safety messages, including also specific signalling messages for the management of the distributed ledger and the creation of new blockchains including the list of trustable entities. Network slicing could allow including, on top of this level of security, other end-to-end ciphering methods negotiated with a centralized server.

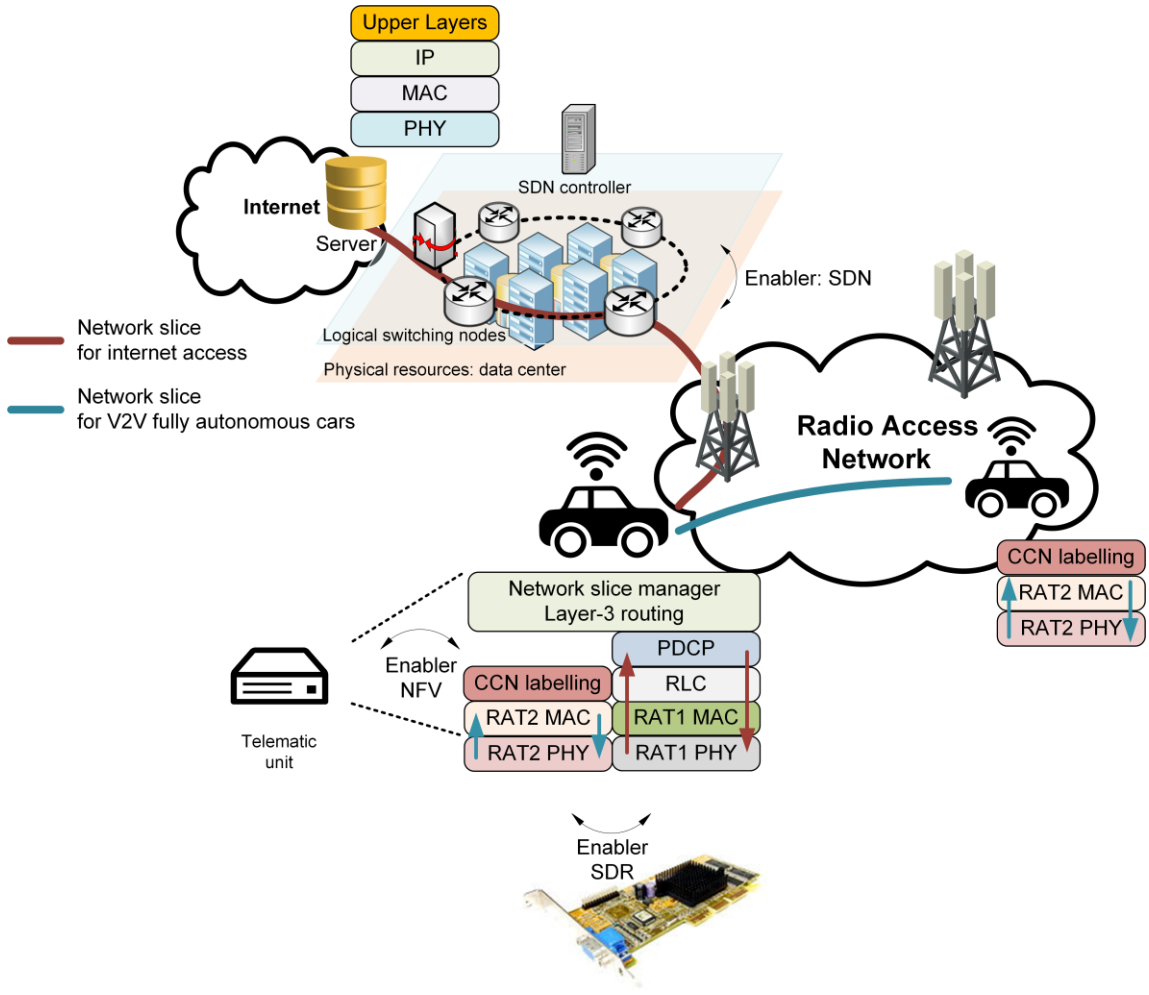


Figure 4 *Network slicing enables fast and trustable V2X communications.*

Conclusions

The means of transportation as we know them today are about to change. The recent advances in wireless communication networks, mainly with the 5G advent, and the technological development of the automotive industry have paved the way for a safer transportation of passengers and goods. Multiple technologies can be integrated in one autonomous and intelligent vehicle that shall remove human error from the crash equation. Mobile networks will be an essential part of the solution. Trust, privacy and stability are paramount in this V2X communication framework.

In this article, we have shown that permissioned blockchains combined with content-centric networking are exceptionally adequate to the task, both are exciting fields of research for the future. Thanks to 5G network slicing, these two concepts will easily form a complete solution, without additional deployment costs and maintaining backward compatibility with conventional Internet traffic.

Several challenges are still open for researchers interested in this area. First, specific consensus protocols should be designed for the VANET use case. The dynamic nature of VANETs makes the validators be changing in time and space, and therefore decisions should be made first partial and then definitive, allowing current validators to search into the tree of block chains for past judgement of other validators.

Second, security of distributed ledgers and CCN could be combined in different manners, and it could be possible also to link in the blockchain not only the record of trustable nodes, but also the exchanged safety messages. This kind of information could be useful for insurance companies or for national authorities to determine the causes of accidents and to be able to discern about the responsibilities of the vehicles involved. Other use cases related to the combination of VANETS and CCN could be explored, like the exchange of high-resolution maps or congestion status reports.

Finally, it is out of the scope of this paper to go into the details of the network slicing interfaces and specific framing and functions of the protocols depicted in Figure 4. Moreover, further research is needed on the functionalities related with the network slice manager, since so far network slicing has been mainly treated from the core network point of view.

References

[1] H. Xiang, W. Zhou, M. Daneshmand and M. Peng, "Network Slicing in Fog Radio Access Networks: Issues and Challenges," in IEEE Communications Magazine, vol. 55, no. 12, pp. 110-116, Dec. 2017.

[2] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," in IEEE Access, vol. 4, pp. 9293-9307, 2016.

[3] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher and B. Ohlman, "A survey of information-centric networking," in IEEE Communications Magazine, vol. 50, no. 7, pp. 26-36, July 2012.

[4] I. Eyal, "Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities," in Computer, vol. 50, no. 9, pp. 38-49, 2017.

[5] L. S. Sankar, M. Sindhu and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1-5, 2017.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

[7] R. Rivera, J. G. Robledo, V. M. Larios and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," International Smart Cities Conference (ISC2), pp. 1-4, 2017.

[8] S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," IEEE Wireless Communications and Networking Conference, pp. 1-6, 2016.

[9] V. Buterin, "A Proof of Stake Design Philosophy," Medium https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51, Dec. 2016.

[10] White Paper, "Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus," https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, Aug. 2017.

[11] G. Edens and G. Scott, "The packet protector," in IEEE Spectrum, vol. 54, no. 4, pp. 42-48, Apr. 2017.

[12] D. Kim, et al. "Efficient content delivery in mobile ad-hoc networks using CCN," Ad Hoc Networks, vol. 36, p. 81-99, 2016.

[13] S. Choi, et al. "Threat of DoS by interest flooding attack in content-centric networking," International Conference on Information Networking (ICOIN), pp: 315-319, 2013.

[14] H. Tullberg et al., "The METIS 5G System Concept: Meeting the 5G Requirements," in IEEE Communications Magazine, vol. 54, no. 12, pp. 132-139, Dec. 2016.

[15] K. Tsagkaris, et al., "Customizable autonomic network management: integrating autonomic network management and software-defined networking," in IEEE Vehicular Technology Magazine, vol. 10, no. 1, pp. 61-68, Mar. 2015.

Biographies

Victor Ortega is software engineer at Casa Systems and Ph.D. student at the Universitat Politècnica de València. He is currently working on Casa's 4G small cell solution and researching on 5G networks and their applications. Before joining Casa, he was R&D engineer in Marvell Semiconductor and DS2. He has actively participated in the design of G.hn (G.996x) and worked closely with the ITU-T and the HomeGrid Forum to promote this technology.

Faîza Bouchmal studied with honours in the National school of applied Science - ENSA the speciality of System of Telecommunication and Networks. In 2017 joined the Universitat Politècnica de València (UPV), where is currently doing research on 5G V2V communications and network slicing.

Dr.-Ing. Jose F. Monserrat [SM] is associate professor at the Universitat Politècnica de València. His research focuses on the design of future 5G wireless systems and V2X systems. He has been involved in several European Projects, like METIS/METIS-II leading the simulation activities. He co-edited the Wiley book "Mobile and wireless communications for IMT-Advanced and beyond" and the Cambridge book "5G Mobile and Wireless Communications Technology". Professor Monserrat has published more than 50 journal papers.