Blockchain and IoTA Systems for Automotive sector: A Comparative Analysis

Lorenza Cotugno[a], Simona Franci[a], Giordano Galli[a], Alessandro Vizzarri[a] and Giuseppe Perrone[b]

[a]*Department of Enterprise Engineering "M. Lucertini", University of Rome Tor Vergata, Rome, Italy*
[b]*EY Italy S.p.A.*

Abstract

In the last years the automotive sectors are affected by the effect of the innovation digital technologies in several vertical applications. In this ecosystem, the automotive sector is also impacted by the adaption of innovative technologies as blockchain and IoTA as decentralized network systems. In the first part of the paper the authors provide a first analysis of the two systems. In the second, a comparison analysis is presented and commented.

Keywords

5G, Wireless networks, Blockchain, IoTA, Automotive, Smart contract.

1. Introduction

In the last years the digital technologies have been the center of the innovation in different sectors, as health [1, 2], automotive [3], space [4] or energy [5, 6, 7]. To provide connectivity to persons and to smart objects worldwide, some telecommunication architectures have been proposed in the literature, including fixed access, 5G and ultra-dense wireless networks and satellite [8], including the IoT communication technologies as wireless sensor networks and Bluetooth [9, 10, 11, 12]. In this ecosystem, the blockchain systems have gained the interest of the scientific communities since they are able to managed the data in a secure way and anti-tampered way [13]. This happens thanks to the adoption of a decentralized network topology, asymmetric cryptography schemes and digital signature techniques. In the case of automotive sector, the possibility to connect the on-board sensors and the Electronic Control Unit (ECU) is very important in order to collect data with high levels of integrity.

The Tangle is the technology heart of the IOTA, a permissionless, feeless and multi-dimensional distributed ledger [14].

The IoTA system is based on the Tangle. It is a technology that enables Internet of Things (IoT) innovation through innovative machine-to-machine applications, e.g. micropayments and more.

The authors present the overview of the blockchain and IoTA systems in the context of the “Blockchain and IoT Lab”, a joint research laboratory between The University of Rome Tor Vergata and EY Italy Spa.

The Section 2 the application of the blockchain system in the automotive sector. In the section 3 the smart contract are described. In the Section 4 the IoTA system and its application to the automotive sector are described. The Section 5 provides a comparison analysis of the blockchain and IoTA systems. In the Section 6 the main conclusions are summarized.

2. Blockchain System for Automotive

The new mobility models that are being studied and implemented involve an increasing use of data and information, leading these systems, which can be defined as smart, to become increasingly complex and critical. The automotive sector, such as construction, insurance and entertainment, has realized that, by now, the concept of ownership has become completely “liquid” and there is no longer interest in the product “car” but in the mobility service. However, this new paradigm implicitly provides some problems:

- Electronics already for several years, take control in the car system. Each car, even in the cheapest models, provides an on-board computer that constantly monitors the "health status" of the vehicle, in the most advanced models this becomes a collector for all the latest safety sensors and must be sure that everything is working

ICYRIME 2020: International Conference for Young Researchers in Informatics, Mathematics, and Engineering, Online, July 09 2020
lorenza.cotugno@uniroma2.it (L. Cotugno); simona.franci@uniroma2.it (S. Franci); giordano.galli@uniroma2.it (G. Galli); alessandro.vizzarri@uniroma2.it (A. Vizzarri); giuseppe.perrone@it.ey.com (G. Perrone)

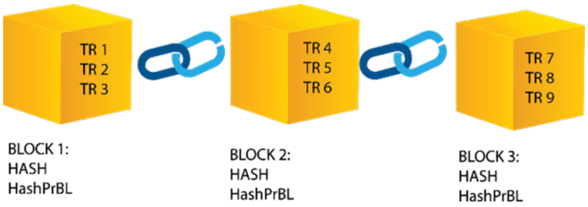

Figure 1: Example of concatenation of blocks.

fine;

- The software, therefore, that manages the electronics described above, must be updated constantly paying attention to bugs that could undermine the operation of the car itself, especially in critical functions such as safety. One of the issues experiencing now is managing software updates, knowing which release is installed on a specific car can be a problem;
- If the new paradigm does not involve the purchase of the car, the manufacturers will have all the interest to keep the vehicle in the best possible way to ensure that it still has market finished the rental offer. Thanks to connection services the car company constantly monitors the status of the car remotely and optimizes maintenance. However, the customer is still not in any way guaranteed that maintenance is done properly and with quality parts, unless personally checking the installed parts;
- Data collected remotely on cars many times is redundant and falsified;
- The e-station for charging vehicles are operated by different providers means different account to recharge the car.

DLT and specifically blockchain fit comfortably into this system becoming an essential tool for this constantly and rapidly evolving industry. In fact, the blockchain ensures that the data entered in the ledger, the main transaction's database is, as well as safe and traceable, also immutable, ensuring that critical transactions such as those of software installation on the car or the tracking of certified spare parts or the management of litigation by accident are managed, tracked and archived in a simple and searchable way. Each transaction to be modified requires confirmation of more than half of the participants in the blockchain itself, making it perfectly transparent to change attacks.

A team of researchers from the University of Nottingham, Ningbo in collaboration with China's iCarForce is developing a smart contract-based (automated software contracts installed on blockchain) insurance system that involves the use of sensors on board the car and a driver's remuneration system based on its driving mode, a dynamic pricing that does not remain constant but which can decrease and increase depending on the use that is actually made of the car [1].

Instead, there are many proposals for a blockchain-based supply chain management system, a unique system that certifies, mathematically, all transactions in the supply chain, from receiving demand, to taking charge from the warehouse, following all logistical transactions up to receiving and installing, ensuring the customer that the work is done well. The same approach is given to raw material, this ensure that all the supply chain from mine to factory is guaranteed and traceable, BMW is creating a blockchain-based platform to do so.

A team from Cornell University research into the topic of software update and release monitoring, proposing a blockchain-based system that would ensure the traceability of software releases on individual vehicles, their updating and the security of an immutable system that therefore would not allow attackers to operate vehicle compromise activities.

Blockchain can also resolve the problem of payment in e-charging stations using traceable transaction in a unique platform that give the customer the freedom of payment old fuel stations give [3].

However, the typical features of blockchain do not guarantee useful transaction recording times for IoT applications, such as the connected cars we've talked about so far. For this reason, another type of DLT has developed over time that still guarantees the characteristics of the blockchain but adds in its favor rapid exchanges of transactions even on high volumes, the TANGLE.

3. Design of Blockchain Smart Contract

As per the perfect definition by Andreas M. Antonopoulos and Gavin Wood, "smart contracts are immutable computer programs that run deterministically in the context of an Ethereum Virtual Machine as part of the Ethereum network protocol. The word contract has no legal meaning because the contracts are so defined only because they can control valuable things like ETH or other digital assets. Are immutable because once

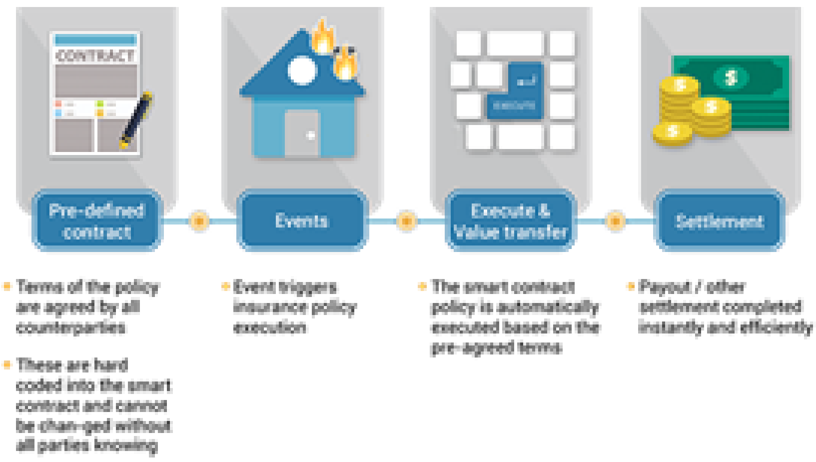

Figure 2: Flow of smart contract usage.

Table 1
Traditional vs Smart Contracts

Traditional Contracts	Smart Contracts
Days	Minute
Manual finalization	Automatic finalization
A real cost for the enterprise and the user	Fraction of the cost
Need of physical presence	Need of virtual presence with digital signature
Lawyers and guarantors	No need of layers and guarantors

written and implemented, the smart contract cannot be modified and requires another smart contract to modify its system logic. Runs deterministically because implements a series of if-than-else that allow it to function in a deterministic way upon the occurrence of a specific event. Smart contracts are used whenever there is a need to automate transactions that require unnecessary human intervention for example are heavily used in logistics. We can summarize the strengths and drastic changes that the use of this technology will bring:

Smart contracts can be used in different ways and different fields: trade finance, property ownership, insurance, peer to peer transaction and a lot others, changing deeply the concept of transaction.

Figure 3: IOTA Alliance.

4. IOTA for Automotive

4.1. Description of IOTA System

IOTA was founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik Schiener, and Dr. Serguei Popov. IOTA refers to the ecosystem which has two main components:

- The Tangle represents the architecture of the distributed ledger,
- IOTA cryptocurrency.

The project was born specifically to create a DLT that could play the role of backbone for data from the Internet of Things (IoT) world.

Experts estimate that by 2020 30 billion IoT devices will be active, distributed in every imaginable area. The problems arising from the need to manage the large amount of data generated by IoT devices could

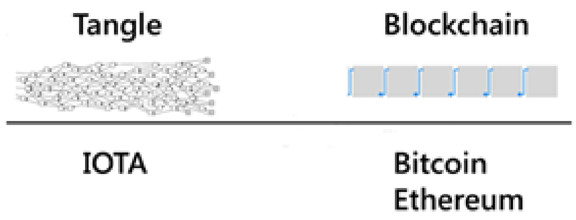

Figure 4: Releation of IOTA and Bitcoin/Ethereum.

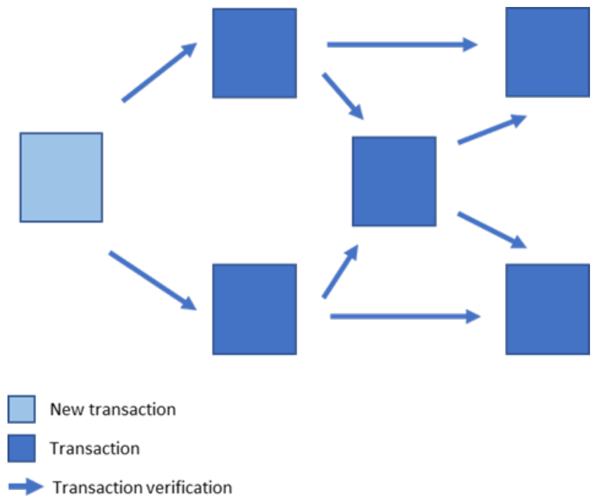

Figure 5: Iota transactions.

be solved by DLT technologies. In this scenario IOTA is one of the projects that aims to made this come true. One of the principal goals of IOTA is the Machine-to-Machine (M2M) Payments, which consists of an economy managed entirely autonomously by machines. To achieve success some limits offered by the classic blockchain architectures have been overcome: several innovations were introduced, and several changes were made to the algorithms normally used in previous DLTs.

The Tangle is a data structure created by IOTA as a basis for cryptocurrency. A tangle is a special type of distributed ledger architecture based on a direct acyclic graph (DAG). A DAG is a graph in which each node is connected to other nodes via direct connections and there are no cycles. In a tangle there is no concept of blocking, of chains or of mining. In order to be able to execute a transaction, each user must first validate two other transactions, effectively becoming a miner.

The imposed rule serves to ensure the functioning of the network, since there is no incentive mechanism that remunerates the miners to approve the transactions.

Unlike blockchain technologies, IOTA does not create a sequence of synchronized static blocks (each containing a number of transactions) but a single transaction can be associated with itself and in parallel with other transactions.

The IOTA system makes each node part of the validation process, effectively eliminating any scalability limit: as more transactions are created, as more transactions are validated. The result is a self-sustainable and infinitely scalable system (there is no theoretical tps limit).

In the Bitcoin blockchain (but also in its derivatives) there is a balance of the difficulty of the PoW in order to limit the creation of a block in an average time of ten minutes. In IOTA, the absence of blocks implies that the waiting time for the validation of transactions is very low. Being the consensus parallelized one has the ability to scale infinitely with the increase in the number of nodes. The more nodes they belong to, the faster the consent mechanism and the transaction confirmation is put in place [15].

4.2. Transactions in IOTA

The transaction is the basic data structure of any DLT, it describes the transfer of tokens from one address to another. Transactions are logged in the DLT database and are visible in plaintext within the log.

To create a new transaction on the network, a node does the following steps:

- prepare the transaction
- select two more transactions
- sign the transaction
- calculate Proof of Work
- transmit across the network.

When a user tries to execute a transaction, the transaction will be first prepared. This contains the filling in most of the fields of the transaction subject, such as the amount of transactions, the recipient's address. The next step is to select two more transactions. The new transaction will validate these two existing transactions. The transaction can now be signed using the user's private key. Before the transaction can be transmitted over the network, the PoW must be calculated.

After the transaction has been transmitted, the user will have to wait for other transactions to select this transaction for validation. Once enough other transactions directly or indirectly approve the transaction, it will get the “confirmed” status. Usually, when 95% of new transactions approve a given transaction, this will be enough to have the status “confirmed”.

4.3. Consensus

The term "consensus" refers to the process that leads all nodes to agree on the same state as the DLT. In IOTA the entire network is responsible for the consensus, as opposed to what happens in Bitcoin, where only miners have the right to decide.

Consensus in IOTA is intrinsic in the transaction issuance process and it is one of the main features of this DLT.

It is said that one transaction approves another transaction by referencing it directly or indirectly. A transaction is said to be confirmed when it is validated directly or indirectly by all tips (where the tips are transactions that are not yet approved). The weight parameter measures the weight of the transaction and is proportional to the amount of Proof-of-Work performed during the attach operation. The cumulative weight is defined as the weight of a transaction plus the sum of all weights of all those that approve it directly or indirectly.

The Markov Chain Monte Carlo algorithm is used for the selection of the two tips to be referenced. It plays a key role in the security of the system since protection from double spending attacks comes from a right choice of tips. The idea is to put some random walkers in the Tangle area that will be confirmed transactions, and then let them move towards the tips in a pseudo-random way. The tips so reached are those that are taken to be approved. Along the way, the choice of the next transaction to move depends on the cumulative weight of each one. Starting from anywhere, the set of upcoming transactions is defined by all transactions that directly refer to the current transaction. Assume that the walker is on transaction x.

The next set is indicated with w. A y transaction of the w set has a P_{xy} probability to be selected to continue the path. This probability is given by:

$$P_{xp} = \frac{e^{-\alpha(H_x - H_y)}}{\sum e^{-\alpha(H_x - H_y)}} \tag{1}$$

The equation indicates that the walker tends to choose a transaction with the minimum cumulative weight gradient between the current one and the next potential transaction.

In the figure the walker is located on x and it must choose the next transaction on which to move between z and y. From the calculation of the P_{xy} and P_{xz} probabilities (considering $\alpha = 1$ for simplicity) we obtain:

$$P_{xp} \approx 4.25 \cdot 10^{-18}; \quad P_{xz} \approx 1 \tag{2}$$

As we can see the probability of going towards y is negligible. This is because z is already approved by many transactions and its cumulative weight is high, while the branch of y has a much lower weight.

4.4. Coordinator

In the early stages of the Tangle, the network is subject to numerous attacks. A user who controls most of the hashing power can do double-spending. Unlike Bitcoin where a miner competes with all other miners, in IOTA an attacker competes only with nodes that actively issue transactions. Therefore, when not many transactions are issued, an attack becomes more feasible to execute. To protect against such attacks, the IOTA foundation operates a special node called Coordinator (Coo). This node has a checkpoint function. By periodically issuing zero-value transactions, the Coo creates milestones. Every two minutes, the IOTA foundation issues a fundamental transaction, and all transactions approved by it are treated as having a 100% “confirmation trust”. This is the main reason why the Coo is a central entity in the tangle.

4.5. Real use cases for IoTA in Automotive

One of the areas in which IOTA is applying a lot is precisely that of mobility so much to participate in the conference of MOBI (mobility open blockchain initiative) a consortium of companies that deal with applying blockchain to the new mobility system.

One of IoTA’s most important partners is Jaguar Land Rover, for which they have developed a car wallet system for their I-Pace car that can, in this way, send and receive payments for physical and digital services and can communicate with parking meters and tolls. The wallet allows the user to make micro-transactions in almost instantaneous time and then collect this information for future use. In addition, they collaborated with the city of Trondheim to communicate to the user the source of the energy they are using [6].

"Smart Wallet" eliminates the need for small coins or to sign up for multiple accounts to pay for a variety of services. Unlike other similar systems and thanks to its structure, it does not require a commission to operate; over time, transactions will become faster across the entire network, which is estimated to reach 75 billion connected devices by 2025. Users will be able to integrate the "Smart Wallet" with conventional payment methods.

Another interesting application of the Tangle is the one described in the previews chapter. IoTA in collaboration with ElaadNL (knowledge and innovation centre in the field of smart charging infrastructure in the Netherlands) created an IOTA-enabled Smart Charger, so the problem of different accounts for different energy providers is no longer an issue.

When connecting cars to the charging station, these devices will be able to independently resolve transactions and related payments. The technique is safe, reliable, fast and it has a derisory cost [16].

5. Blockchain and IOTA: a comparison analysis

The features that a blockchain network must have to ensure its use in IoT, can be summarized here:

- Scalability: the network must ensure its performance even with millions of connected devices,
- Applicability, must ensure fast, economic, privacy and automated transactions,
- Consensus techniques that enable scalability and applicability,
- Developability to ensure ease of development of devices operating on the network itself,
- Interoperability to work with other blockchain networks without problems.

In the beginning, blockchain technology was not born for IoT purposes but, from Nakamoto's whitepaper, to build a tax-free, high-speed global money exchange system. Over time, it was realized that the characteristics of the blockchain could be applied to the most diverse applications, especially in the IoT field, and many realities were born in a short time with different protocols, consensus algorithms and network topology, one on all IoTA. The differences that IoTA brings to the standard blockchain are many and specific:

- We are no longer talking about blockchain but about tangles, an acyclic graph composed of nodes in which the individual nodes represent the individual transactions,

Table 2
Traditional vs Smart Contracts

System	IOTA	Blockchain
Topology	Tangle	Blockchain
Miners	No	Yes
Fees	No	Miner cost per transaction
Transaction speed	3 min (mean)	6 min (mean)
Energy consumption	No mining means less consumption	Mining

- Transactions are fee-free,
- Fully scalable with the ability to validate multiple transactions in parallel without compromising network security,
- Much more decentralized than other networks because there are no miners (there is no hierarchy); each participant in the network also participates in the consensus algorithm and carries on transactions.

The cons of this system are undoubtedly the great complexity of development by new developers as opposed to Ethereum that has now become the standard for industrial applications, plus it does not guarantee a certain time (average) of reaching consensus, it can happen that your transaction remains stalled for a long time before being validated. This is why the IoTA foundation is working, together with industrial partners, to improve the structure and the system in general.

6. Conclusion

The blockhain and the IoTA Systems are two importat decentralized network systems very important. Their implementations in the automotive sector is very interesting due to the involvement of several on-board sensors node and the possibility to enhance their security. In this way, the two systems provide several features in terms of security, efficiency and trusted transactions among the nodes on the basis of common and different features analyzed in the paper. The authors also provide a comparison analysis of the two systems. The blockchain is mainly characterized by the decentralized topology, a chain of blocks, the presence of the miner, their corresponding costs and a transaction speed of about 6 minutes. The IoTA system is based on the tangle, the absence of miners and relative fees and a transaction speed of about 3 minutes.

In the next steps, the authors will perform simulation activities in order to provide numerical results to be analyzed.

Acknowledgment

The authors would like to thank EY company for supporting the Blockchain and IoT joint lab activities.

References

[1] M. Asif-Ur-Rahman, F. Afsana, M. Mahmud, M. S. Kaiser, M. R. Ahmed, O. Kaiwartya, A. James-Taylor, Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things, IEEE Internet of Things Journal 6 (2018) 4049–4062.

[2] G. Capizzi, G. Lo Sciuto, C. Napoli, D. Polap, M. Woźniak, Small lung nodules detection based on fuzzy-logic and probabilistic neural network with bio-inspired reinforcement learning, IEEE Transactions on Fuzzy Systems 6 (2020).

[3] J. P. Trovao, Trends in automotive electronics [automotive electronics], IEEE Vehicular Technology Magazine 14 (2019) 100–109.

[4] G. C. Cardarilli, L. Di Nunzio, R. Fazzolari, D. Giardino, M. Matta, M. Re, L. Iess, F. Cialfi, G. De Angelis, D. Gelfusa, et al., Hardware prototyping and validation of a w-δdor digital signal processor, Applied Sciences 9 (2019) 2909.

[5] F. Bonanno, G. Capizzi, G. L. Sciuto, C. Napoli, G. Pappalardo, E. Tramontana, A novel cloud-distributed toolbox for optimal energy dispatch management from renewables in igss by using wrnn predictors and gpu parallel solutions, in: 2014 International Symposium on Power Electronics, Electrical Drives, Automation and Motion, IEEE, 2014, pp. 1077–1084.

[6] S. Chen, B. Guo, H. Yan, Q. Qin, B. Li, B. Qi, Application and prospect of integrated energy interoperability management system based on blockchain, in: 2019 IEEE International Conference on Energy Internet (ICEI), IEEE, 2019, pp. 421–425.

[7] F. Bonanno, G. Capizzi, G. Sciuto, C. Napoli, Wavelet recurrent neural network with semi-parametric input data preprocessing for micro-wind power forecasting in integrated generation systems, in: 5th International Conference on Clean Electrical Power: Renewable Energy Resources Impact, ICCEP 2015, 2015, pp. 602–609.

[8] F. Mazzenga, R. Giuliano, F. Vatalaro, Fttc-based fronthaul for 5g dense/ultra-dense access network: Performance and costs in realistic scenarios, Future Internet 9 (2017) 71.

[9] S. L. Ullo, G. Sinha, Advances in smart environment monitoring systems using iot and sensors, Sensors 20 (2020) 3113.

[10] R. Giuliano, G. C. Cardarilli, C. Cesarini, L. Di Nunzio, F. Fallucchi, R. Fazzolari, F. Mazzenga, M. Re, A. Vizzarri, Indoor localization system based on bluetooth low energy for museum applications, Electronics 9 (2020) 1055.

[11] C. Napoli, G. Pappalardo, E. Tramontana, Improving files availability for bittorrent using a diffusion model, in: 2014 IEEE 23rd International WETICE Conference, IEEE, 2014, pp. 191–196.

[12] G. Capizzi, S. Coco, G. Lo Sciuto, C. Napoli, A new iterative fir filter design approach using a gaussian approximation, IEEE Signal Processing Letters 25 (2018) 1615–1619.

[13] A. Pieroni, N. Scarpato, L. Felli, Blockchain and iot convergence—a systematic survey on technologies, protocols and security, Applied Sciences 10 (2020) 6749.

[14] IoTA Foundation, Iota developer documentation, 2020. URL: https://docs.iota.org/.

[15] Y. Chen, Blockchain in enterprise: An innovative management scheme utilizing smart contract, in: 2020 9th International Conference on Industrial Technology and Management (ICITM), IEEE, 2020, pp. 21–24.

[16] Elaadnl, Iota charging station, 2020. URL: https://www.elaad.nl/projects/iota-charging-station/.