Blockchain enhancing IoD network functionality

Anastas Madzharov
Unmanned Robotics Systems Laboratory
Institute of Robotics-Bulgarian Academy of Sciences
Sofia, Bulgaria
a.madzharov@ir.bas.bg

Rumen Georgiev
Unmanned Robotics Systems Laboratory
Institute of Robotics-Bulgarian Academy of Sciences
Sofia, Bulgaria
r.georgiev@ir.bas.bg

Stefan Hristozov
Unmanned Robotics Systems Laboratory
Institute of Robotics-Bulgarian Academy of Sciences
Sofia, Bulgaria
st.hristozov@ir.bas.bg

***Abstract*— The development of Unmanned Aerial System (UAS) presents unique challenges to acquiring, storing, and transmitting data to cloud during flight. One of the primary challenges is the selection methods of interchange and storing data in encrypted form and using it in a Pub/Sub model in real time, without using M2M protocols like MQTT, CoAP and etc.**

One of the biggest challenges related to the integration of blockchain and IoT is the limitations related to, for example, the limited battery life of some IoT devices, low computing power, limited communication resources, safety issues, etc. Blockchain requires huge resources on the background of IoT, computing, energy, communication, etc.

By discussing the trade-offs involved in mixed platform selection Enhancing the Internet of Drones with Blockchain, the intricacies of evaluating the performance of this system in terms of the number of transactions that can be executed per second and also optimizing its performance for application in IoD networks development, aiming to enhance performance and reliability, but also to evaluate its impact on safety and risk assessment.

The idea behind IoT is that physical things will eventually connect to each other via the Internet, creating endless possibilities for nodes to communicate. An investigate is to connect the virtual world with the physical world, block by block. Tokens will incentivize developers to create better DApps for the IoT world.

Keywords—Internet of Things; open-source, blockchain protocols; Internet of Drones; security, Artificial Intelligence.

I. INTRODUCTION

The high-level concept of an IoT network is that smart devices like sensors, actuators, and wearable's gather data about their environments, wirelessly connect to the internet and to other connected devices via routers and gateways, and share the information they've collected within the network. As a typical network architecture, it enables communications between unmanned aerial vehicles (UAVs) and devices on the ground [1, 2] in a coordinated manner [3, 4], allowing drones to have flight control and providing navigation services [3] such as the internal transmission and exchange of data, with integrated mobility, portability, and automation [3, 4].

The Internet of Things (IoT) is becoming a reality, and in the last few years we have indeed witnessed to an enormous growth of technologies designed for its wide and capillary implementation. In particular, many efforts have been made in order to design communication solutions adapted to the specific requirements1 of IoT devices. Such efforts produced a great variety of different communication technologies tailored to low-power devices, ranging from short-range solutions (IEEE 802.15.4, Bluetooth Low Energy) to dedicated long-range cellular-like networks (LoRa/LoRaWAN, Sigfox, Ingenu). However, IoT devices typically have limited computational resources, storage, network coverage, and energy. Therefore, resource-intensive IoT applications often face significant challenges in maintaining the expected Quality of Services (QoS).

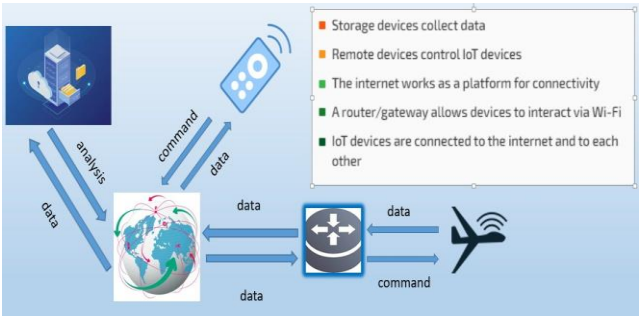

Fig. 1. Architectures and Tools for Internet of Things

Drones primarily utilize a radio frequency spectrum between 900 MHz and 5.8 GHz [6,7,8] for communication. Drones with 2.4 GHz are enabled with live video streaming with a maximum range of 1-8 km over a VLOS. The operational range is a significant challenge that UAV's face in radio communication. For instance, WiFi has an operation range of 50 m indoor and 100 m outdoor. Bluetooth operates in a range of 50 m. Zigbee has 10-100 m of operation, while LoRa works in a range of 50 m indoors and 200 m outdoors. All these communications in the maximum fields are at the VLOS. The communication range is dramatically affected by objects between the LOS.

Another challenge is the security of the system itself. The plans are designed primarily for point-to-point communication. Very few securities are incorporated, making it very vulnerable to the system safety itself. Only a few military-based drone are registered with Air Traffic Control. While small recreational and non-commercial drones need not be registered and need no prior permission to fly. However, European Union Aviation Safety Agency (EASA) has set a strict framework within EU and EASA member countries to fly drones in the European sky.

THIS WORK WAS SUPPORTED BY THE NSP DS PROGRAM, WHICH HAS RECEIVED FUNDING FROM THE MINISTRY OF EDUCATION AND SCIENCE OF THE REPUBLIC OF BULGARIA UNDER THE GRANT AGREEMENT NO. Д01-74/19.05.2022.

Problems: Limited range of operation; Point-Point communication; Identification of any flying drones; Path planning; Data collection beyond VLOS; Limited/No take-off and Landing permissions.

The IoD is integrated with different systems, such as Wireless Sensor Networks (WSNs), i.e., systems spatially separated from UAV's allowing them to function efficiently in an expanding controlled zone, considering connection performance [6], due to congestion prevention, which results in reducing packet loss while ensuring equal bandwidth allocation.

On the other hand, blockchain allows transparent data sharing within a decentralized network, with an immutable ledger facilitating the process of recording transactions and tracking assets [6,7], as well as providing trust, security, and reliability of data processing [8]. The dominant advantages and capabilities of blockchain were soon recognized and leveraged, with relative solutions being applied in different fields, among them UAVs to tackle emerging problems. Today, the integration of blockchain (public or private) within the IoD ecosystem has gained growing attention, providing many benefits in relation to the enhancement of IoD networks, and mitigating security and safety risks, as well as improving reliability[6],[7].

In this paper a investigate IoD and blockchain approaches, additional emerging digital technologies are being incorporated in the respective synergy as impactful enablers [5], such as (a) Artificial Intelligence (AI) [6]; (b) Cloud Computing (CC) [7]; (c) Edge Computing (EC), including Edge AI for smarter computational systems as well as intellectual tasks of robotic machinery [8]; (d) IoT [9]; and (e) communication technologies, such as 5G/6G for smarter communication, fast and accurate processing of big data, transmission, and handling [10,11].

II. INVESTIGATE IOD AND BLOCKCHAIN SELECTION

Interoperability occurs when two or more heterogeneous systems or devices on the networks communicate with each other to attain a common purpose [9]. IoT systems and devices are disintegrated and cannot share their data with each other due to lack of communication protocols, data formats, and technologies [9,10]. This means that data cannot be switched across interconnected devices.

With the aid of cross-chain technology, blockchain has the ability to share information across different systems, devices and networks. Cross-chain technology focuses on chain interoperability across private networks or between public blockchains and private networks [9, 10].

Blockchain has more robust level of encryption than IoT as such parties cannot overwrite existing records on the network. IoT data stored in blockchain will create additional layer in the IoT security to block cyber-criminals from gaining easy access to the network

Blockchain allow securely recording of data in IoT machines as such all detailed transactions are carried out without any human interference. With this the data integrity is preserved and all parties in the supply chain will it. Every participant in blockchain technology has a unique identity which is linked to the account and this ensures that the owner operates the transactions. The encryption on blockchain makes it difficult to hack or disturb the traditional setup of the chain [10]. Minors monitor all transactions on the blockchain system, thus maintaining the integrity of the blockchain. For the purpose of security, any block or transaction added to the blockchain program cannot be edited. Hackers have been unable to succeed on attacking or threating blockchain, proving that blockchain is trustworthy, tamper-proof, and resistant to technical failures and malicious attacks [3,7]. This is achievable through decentralization.

TABLE I. UAS LINKS AND THEIR SECURITY REQUIREMENTS (CONFIDENTIALITY, INTEGRITY, AUTHENTICATION, NON-REPUDIATION).

Type of communication	**operation safety model**		
	Data	***Impact***	***Security Requirements***
UAV-GCS	command	critical	(C), I, A, (NR)
	video	critical	(C), I, A
	telemetry	important	(C), I, A,
	mission data	specific	Non Applicable
UAV-UTM	emergensy	critical	I, A, (NR)
	direct	critical	(C), I, A, (NR)
	telemetry	critical	I, A, (NR)
UAV-UAV	relay	important	(C), I, A, (NR)
	riuting	important	I, A, (NR)
	environmental	important	I, A, (NR)

Current protocols for telemetry, like the MAVlink are particularly vulnerable to eavesdropping. Kwan et al. [3,6] detail these flaws in an empirical analysis of the MAVlink protocol. The lack of confidentiality can cause privacy issues, even with the telemetry being the only information leaked. The MAVlink can be transmitted over a secure channel, but as telemetry is not usually considered sensitive, operators do not generally bother and simply use the MAVlink over unencrypted channels.

TABLE II. COMMUNICATION LINK ATTACKS ON UAVS

Security objectives	**MAVlink vulnerable**	
	System objectives	***Attack methods***
Confidentiality	Ground control station	Virus
		Malware
		Key loggers
		Trojans
	UAV	Hijacking
	Communication link	Eavesdropping Man-in the -middle
Integrity	Communication link	Packet injection
		Replay attack
		Man-in the -middle
		Message detection
Availability	GCS	DoS
	UAV	Fuzzing
	Communication	Jamming, Flooding, Buffer overflow, DoS

III. INTEGRATION ON BLOCKCHAIN IN IOD NETWORK

Three possible approaches to developing a blockchain-based IoT network architecture are considered in the literature.

The first thing is where will the interactions take place? Interactions can occur not only on the IoT network or on the blockchain, but also within a hybrid architecture that includes both the IoT network and the blockchain.

Another major IoT and blockchain convergence scenarios could be fog computing. This technology has already revolutionized IoT networks, adding a new layer between cloud computing and IoT devices.

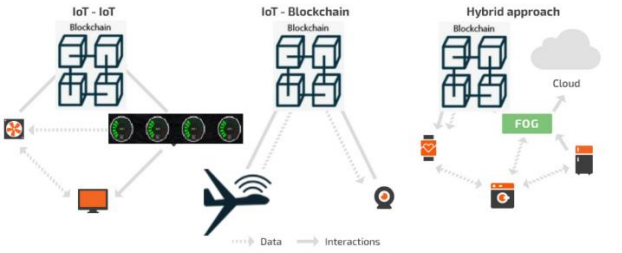

Fig. 1. *IoT and blockchain convergence scenarios*

A. IoT–IoT

This approach entails using the blockchain to store only part of the IoT data. IoT devices communicate without using the blockchain, instead using discovery and routing mechanisms. Transactions are transmitted fast because of low latency. This approach is also considered one of the most secure because it allows devices to work offline.

B. IoT–blockchain

In this case, all communications between IoT devices go through the blockchain, which basically takes the place of the cloud in a traditional IoT network. Records stored in the blockchain are immutable, traceable, and secured from third-party access.

C. Hybrid approach

This approach ensures that most data and interactions are shared directly between IoT devices, whereas the blockchain stores only some data. Thus, this design leverages the benefits of both the blockchain and real-time IoT interactions.

The hybrid approach allows for implementing fog and cloud computing to make up for the limitations of blockchains and IoT devices. For example, fog computing uses gateways and other edge devices to conduct mining or store data. Analyzing sensitive data locally with edge devices instead of sending it to the cloud significantly reduces operating expenses.

Conclusions: Blockchain technology provides very strong encryption, making it virtually impossible to manipulate existing records. On the other hand, blockchain technology provides the necessary degree of transparency to obtain the right of control that occurs in traditional transactions.

When using cooperative drone devices to collect information, IoT sensors can send important events to the blockchain, such as location data, route, etc., to improve management and develop more informative and reliable mission monitoring practices.

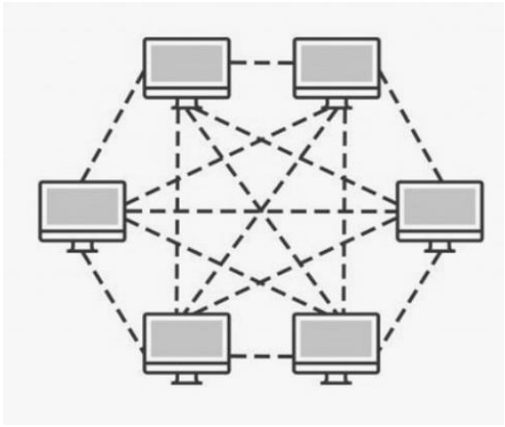

Fig. 2. *Pure P2P model for cooperative network*

Blockchain is a peer-to-peer network that acts as a decentralized ledger for one or more digital assets, i.e. a decentralized peer-to-peer system in which each computer stores a complete copy of the ledger and verifies its authenticity with other nodes to ensure data accuracy.

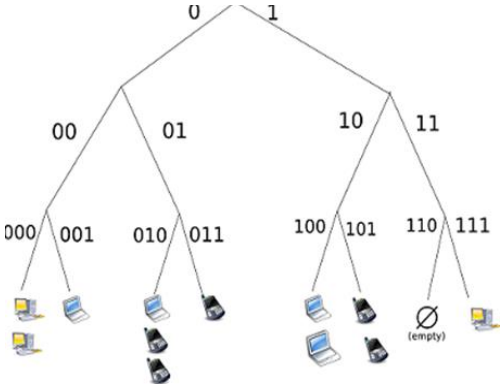

Fig. 3. Hybrid P2P model for cooperative network

The considered collaborations are: a) Things-UAV, b)UAV-Edge, c)Things-Edge, d) Things-UAV-Cloud, e)UAV-Edge-Cloud, and f) Things-UAV-Edge-Cloud.

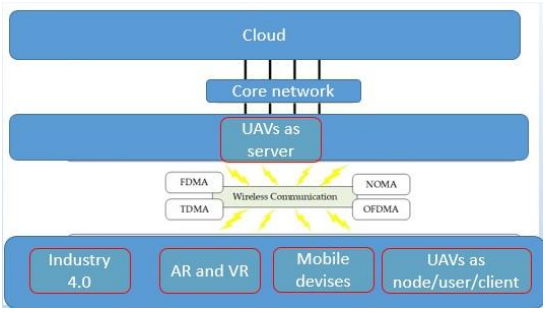

Fig. 4. Architecture for Resource Management in UAV-enabled Edge Computing Environment

A typical UEC architecture consists of three layers including things, edge, and cloud. Existing studies investigate different types of scenarios for resource management in a UEC environment. As a result, different types of collaborations between things, UAV, edge, and cloud can be found in the existing studies.

Blockchain technology can provide robust solutions for enhancing the security of the IoD environment in various ways. It can be used to create unique digital identities for individual drones, which are stored and managed on the

blockchain, assisting in the prevention of impersonation attacks.

Specifically, each drone in the network is given a unique identity, with the identity being stored in the blockchain. When a drone attempts to join the network or perform a transaction (e.g., sending data), it has to prove its identity. This is done through a process called cryptographic verification. The drone provides a digital signature, which is a piece of cryptographic data, while other participants in the network (which could be other drones, or base stations) can use this digital signature to verify the drone's identity. If the identity cannot be verified, the drone is not allowed to join the network or perform transactions [12, 13].

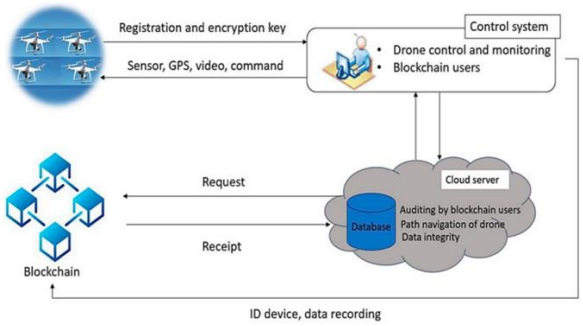

Fig. 5 Blockchain solutions for enhancing the security of the IoD environment

IV. Difficulties in Choosing a Consensus Protocol

Consenting nodes (i.e., nodes who vote for ordering the transactions) compose a fully-connected network. There is a leader (often referred to as primary node) among the nodes who first prepares an incoming request message to the other nodes by suggesting a sequence number for the request in broadcasted PREPARE messages. The other nodes verify the PREPARE messages and subsequently broadcast a COMMIT message in the network. Finally, the nodes who have received f+1 (where f is fault-tolerance, a number of tolerated faulty nodes) consistent COMMIT messages execute the request locally and update the underlying service state. If the leader is perceived as faulty, a view change procedure follows to change the leader node.

In the following section considered PBFT is a Byzantine fault tolerance protocol for state machine replication. The state machine replication is a method for avoiding the unavailability of the online services due to failures by duplicating the system states over multiple machines to have some degree of redundancy. How do all replicated state machines reach the consensus between each other?

In a situation where consensus can be achieved exclusively by relying on communication, the well-known consensus problem in decentralized systems commonly known as the Byzantine Generals Problem.

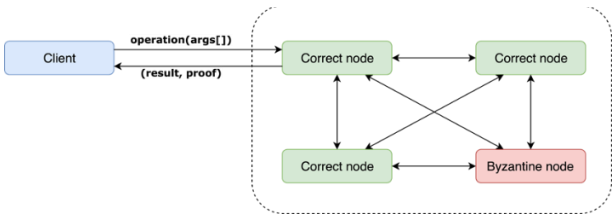

Fig. 6 State machine architecture

Each node carries a state which is updated using transactions furnished through the consensus engine. Assuming that more than 2/3 of the cluster nodes are honest, the BFT consensus engine guarantees correctness of state transitions. In other words, unless 1/3 or more of the cluster nodes are Byzantine there is no way the cluster will allow an incorrect transition.

The component is implemented based on Efficient Byzantine Fault-Tolerance paper, a BFT protocol that leverages secure hardware capabilities of the participant nodes

The original data topics from **Mission Commands**: Navigate to GPS location; Loiter at location for infinite; Loiter at location for time; Return to launch location; Take off; Set system mode; Change home location; Calibrate sensors; Shut down component. **Information Requests**: Pitch angle; Yaw angle; Roll angle; GPS latitude; GPS longitude; Altitude from ground; Altitude from sea level; Latitude speed; Longitude speed; Altitude speed; Compass heading; Time since system boot.

V. Setup Blockchain-python and Discussion

The Blockchain-python implements simple blockchain and transactions. Currently, the implementation already has mining, transaction, communication between nodes, and file persistence of blocks and transactions. The communication between nodes is via remote procedure call (RPC) based on http, rather than p2p network. Because the implementation of p2p is more complicated, it is too complicated to understand the framework of blockchain.

The verification based on cryptography has not yet been realized, and the verification of blocks between nodes and the verification of transactions have not yet been realized.

About Blockchain-python block

Blockchain-python simplified block structure, a blockchain-python block data is as follows sections:

```
{
    "index":
    "timestamp":
    "tx": [    ],
    "previous_block":
    "nouce":
    "hash":
}
```

The calculation of block hash is roughly the same as that of Bitcoin. Our difficulty setting is relatively low, so the hash in front of this block has only 4 zeros. This is for easier mining to understand the principle and generally can be produced in a few seconds. One block. In addition, Bitcoin's tx field represents the root node hash of the merkle tree that consists of the transaction hash.

VI. Conclusion

This paper details the design is a pluggable software component that allows to achieve Byzantine fault-tolerant consensus with fewer consenting nodes and less communication rounds comparing to the conventional BFT protocols.

Consenting nodes (i.e., nodes who vote for ordering the transactions) compose a fully-connected network. There is a leader (often referred to as primary node) among the nodes who first prepares an incoming request message to the other nodes by suggesting a sequence number for the request in broadcasted.

A node might become unavailable because of the network issues, failing hardware or simply because the malicious node decided to start dropping requests. If this happens when the client is making requests, it can get noticed using timeouts. In this case the client simply retries the request, but now sends it to a different node. For the cluster it also doesn't create too many issues, because even with a fraction of unavailable nodes the cluster is able to reach consensus [9, 10, 11].

Few different approaches can be used, however – the first is to send a no-op transaction and wait for it to appear in the selected node blockchain. Because including a transaction into the blockchain means including and processing all transactions before it, the client will have a guarantee that the state has advanced. Another approach is to query multiple nodes at once about their last block height and compare it to the last block height of the selected node. Finally, the client might just expect some maximum time until the next block is formed and switch to another node if nothing happens.

The number of blocks required to make sure that a transaction won't be rolled back is called 'blocks to finality'. The verification process involves multiple nodes, and reaching consensus is not just a matter of speed, it involves coordination, communication, and agreement between these nodes. TTF is essentially a factor that affects the efficiency of this consensus process. A short TTF not only indicates fast transaction processing, but also a fast and efficient consensus mechanism. This includes factors such as network latency, bandwidth, and gossip protocol design, which affect how quickly nodes can communicate and reach consensus.

ACKNOWLEDGMENT

THIS WORK WAS SUPPORTED BY THE NSP DS PROGRAM, WHICH HAS RECEIVED FUNDING FROM THE MINISTRY OF EDUCATION AND SCIENCE OF THE REPUBLIC OF BULGARIA UNDER THE GRANT AGREEMENT NO. Д01-74/19.05.2022.

REFERENCES

[1] Kyriaki A. Tychola, Konstantinos Voulgaridis, Thomas Lagkas, Beyond Flight: Enhancing the Internet of Drones with Blockchain Technologies, Drones 2024, 8(6), 219; https://doi.org/10.3390/drones8060219

[2] BLOCKCHAIN - BASED SOLUTION FOR INTERNET OF DRONES SECURITY AND PRIVACY, United States Patent Application Publication, Pub . No .: US 2021/0209956 A1 Allouche et al . Pub . Date: Jul . 8 , 2021

[3] Dharna Nar, Radhika Kotecha, Enhancement of Drone-as-a-Service Using Blockchain and AI, INTERNATIONAL JOURNAL OF NEXT-GENERATION COMPUTING, November 2022, DOI: 10.47164/ijngc.v13i4.567https://ijngc.perpetualinnovation.net/index.php/ijngc/article/view/567

[4] Tri Nguyen, Risto Katila, Risto Katila, Tuan Nguyen, An advanced Internet-of-Drones System with Blockchain for improving quality of service of Search and Rescue: A feasibility study, Future Generation Computer Systems, Volume 140, March 2023, Pages 36-52, https://doi.org/10.1016/j.future.2022.10.002

[5] Uddin, A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: Challenges and solutions. Blo Mazhar, T.; Talpur, D.B.; Al Shloul, T.; Ghadi, Y.Y.; Haq, I.; Ullah, I.; Ouahada, K.; Hamam, H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sci. 2023, 13, 683. ckchain Res. Appl. 2021, 2, 100006.

[6] Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. IEEE Internet Things J. 2020, 8, 6406–6415.

[7] Kumar, M.S.; Vimal, S.; Jhanjhi, N.; Dhanabalan, S.S.; Alhumyani, H.A. Blockchain based peer to peer communication in autonomous drone operation. Energy Rep. 2021, 7, 7925–7939.

[8] Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. 2018, 14, 352–375.

[9] Sharma, D.K.; Kaushik, A.K.; Goel, A.; Bhargava, S. Internet of Things and Blockchain: Integration, Need, Challenges, Applications, and Future Scope. In Handbook of Research on Blockchain Technology; Elsevier: Amsterdam, The Netherlands, 2020; pp. 271–294.

[10] Porkodi, S.; Kesavaraja, D. Integration of Blockchain and Internet of Things. In Handbook of Research on Blockchain Technology; Elsevier: Amsterdam, The Netherlands, 2020; pp. 61–94.

[11] M. Noura, M.Atiquzzaman, and M Gaedke,. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Network Application vol.24, 2019: pp.796–809 https://doi.org/10.1007/s11036-018-1089-9.

[12] Vandana Mohindru, Yashwant Singh, Ravindara Bhatt, Anuj Kumar Gupta, Unmanned Aerial Vehicles for Internet of Things (IoT): Concepts, Techniques, and Applications, ISBN: 978-1-119-76882-1.

[13] The Industrial Internet Reference Architecture v 1.9|Industrial Internet Consortium./ https://www.iiconsortium.org/IIRA.htm / https://www.iiconsortium.org/pdf/Applying-IIRA-to-Smart-Grid-Testbed-WP-PUB.pdf

[14] Giuliana Veronese, Migel Correia, Alysson Bessani,Lau Lung, Paulo Verissimo, Efficient Byzantine Fault Tolerance, December 2012IEEE Transactions on Computers 62(1):16-30, DOI: 10.1109/TC.2011.221