On Using Blockchains for Beyond Visual Line of Sight (BVLOS) Drones Operation: An Architectural Study

Tahina Ralitera  
Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France  
tahina.ralitera@cea.fr

Agnes Lanusse  
Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France  
agnes.lanusse@cea.fr

Önder Gürcan  
Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France  
onender.gurcan@cea.fr

ABSTRACT
Beyond Visual Line of Sight operation enables drones to surpass the limits imposed by the reach and constraints of the eyes of their operator. It extends their range and, as such, productivity and profitability. Drones operating BVLOS include a variety of highly sensitive assets and information that could be subject to unintentional or intentional security vulnerabilities. As a solution, blockchain-based services could enable secure and trustworthy exchange and storage of related data. They also allow for traceability of exchanges and synchronization with other nodes in the network. In this context, we develop simulation models to evaluate different blockchain-based solutions before implementing them in real systems. However, most of these blockchain-based approaches focus on the network and the protocol aspects of drone systems. Few studies focus on the architectural level of on-chip compute platforms of drones. Based on this observation, the contribution of this paper is twofold: (1) a generic blockchain-based service architecture for on-chip compute platforms of drones in a simulated environment, and (2) an illustration of the proposed generic architecture in a simulated environment for authentication.

CCS CONCEPTS
• Security and privacy;

KEYWORDS
blockchain, drone, bvlos, authentication, simulation

1 INTRODUCTION
International Civil Aviation Organization (ICAO) defines BVLOS operation as "an operation in which the remote pilot or Remotely Piloted Aircraft (RPA) observer does not use visual reference to the remotely piloted aircraft in the conduct of flight" [15]. This operation is crucial for the large-scale expansion and economic feasibility of drone business applications such as logistics, mapping, surveying, etc. BVLOS operation enables drones to surpass the limits imposed by the reach and constraints of the eyes of their operator, extending their range and, as such, productivity and profitability.

However, drones include a variety of highly sensitive assets and information that could be subject to unintentional or intentional security vulnerabilities. Attacks may arise from different sources. For example, malicious intellectual property blocks (IPs) in the hardware, malicious or vulnerable firmware and software, insecure communication of the system with other devices, eavesdropping or "man-in-the-middle" attacks, breach of confidentiality of the stored data, corruption of the integrity of collected data [22]. Therefore, secure, resilient, and tamper-proof storage is essential for the security and accountability of the data.

As a solution, blockchain technology has the potential to secure data that is being dynamically updated through its security capabilities such as hashing, smart contracts, consensus protocols, public and private keys, etc. The data is stored in an immutable manner, making it impossible to modify neither intentionally nor unintentionally. The blockchain also allows for traceability of exchanges and performs synchronization with other nodes in the network. Blockchain-based services could enable trustworthy exchange and storage of the drones related data. Moreover, it is ideally suited for drone applications which are very dynamic [1].

Drones can be used for various purposes and use cases. However, using a concrete blockchain-based solution with well-defined transaction types and parameters may be complicated for these different purposes and use cases. Consequently, we identify the generic component necessary at the architectural level and propose a solution. The contributions of this paper are as follows:

• A generic blockchain-based service architecture dedicated to BVLOS drones operation.
• An illustration of the proposed generic architecture for authentication.

To evaluate different blockchain-based solutions before their application in a real environment, we are setting up simulation models on the Multi-Agent eXperimenter (MAX) [12] blockchain simulation framework. So, the solutions proposed in this paper focus on simulation. The simulation model will allow evaluating the performance of the suggested architecture, in the future, based on the following metrics:

• Metrics on embeddability such as the running time, the energy consumption, the latency/delay
Metrics on authentication such as the probability of authentication, the degree of Reliability of the authentication

This paper is organized as follows. Section 2 describes the background on blockchain. Section 3 describes our proposed generic blockchain-based service architecture for drones operating BVLOS. Section 4 shows the effectiveness of the proposed architecture on a realistic case study. Section 5 gives related work and Section 6 concludes the paper.

2 BACKGROUND

Blockchain systems [20] are composed of participants communicating over a peer-to-peer network using transactions. Its overall objective is to maintain the consistency and coherency of all transactions in a replicated immutable, transparent append-only data structure called the blockchain [13, 14].

As illustrated in Figure 1, this data structure consists of blocks connected using cryptographic links. Each block contains an ordered list of transactions. A transaction can be defined as any operation that changes the state of the blockchain.

Blockchain accounts are used to send and receive transactions. An account consists of a pair of public and private keys. The public key is used by senders and receivers of transactions, while the private key is used for transaction authorizations.

Participants of a blockchain system can play different roles in a blockchain network [23]. While some can be responsible for issuing transactions, others can be responsible for creating the blocks and having consensus on the created blocks.

Similarly, storage may also differ. While some participants store the full replica of the blockchain (i.e., full nodes) [8], others may choose to store less information due to their needs and capabilities (i.e., light nodes) [24].

3 GENERIC BLOCKCHAIN-BASED SERVICE ARCHITECTURE

Blockchain-based services consist of subsystems that use a blockchain-based solution integrated with the communication architecture of the BVLOS drone operation. The objective is to design a blockchain solution deployable to the drones and the Ground Stations (GS) computing platforms. This solution will add services such as authentication and trust management, using trustworthy data securely.

For that purpose, we model the entities of the U-Space (i.e.; drones and ground stations) as communicating network nodes, where a local replicate of the shared blockchain is maintained. The proposed solution is intended to be embedded inside drones and ground stations for securing the sensitive data to be used by future on-chip compute platforms.

This work is part of the Airborne Data Collection on Resilient System Architectures (ADACORSA) European project [21]. Figure 2 shows the blockchain-based services (LS_Blockchain_based_services) positioning within the overall ADACORSA system architecture. The communication layer handles most of the communications. It is important to note that the position of these components is for evaluation purposes and is not currently embedded in real drones. That is why, in this figure, secure communications, drone services and external entities (i.e., drones and ground stations) are represented as Logical Actors. In future real implementations, the blockchain-based services would be integrated at the Reliable Communication component level.

Figure 1: Schematic View on the Blockchain Data-Structure

As illustrated in Figure 1, this data structure consists of blocks connected using cryptographic links. Each block contains an ordered list of transactions. A transaction can be defined as any operation that changes the state of the blockchain.

Blockchain accounts are used to send and receive transactions. An account consists of a pair of public and private keys. The public key is used by senders and receivers of transactions, while the private key is used for transaction authorizations.

Participants of a blockchain system can play different roles in a blockchain network [23]. While some can be responsible for issuing transactions, others can be responsible for creating the blocks and having consensus on the created blocks.

Similarly, storage may also differ. While some participants store the full replica of the blockchain (i.e., full nodes) [8], others may choose to store less information due to their needs and capabilities (i.e., light nodes) [24].

3 GENERIC BLOCKCHAIN-BASED SERVICE ARCHITECTURE

Blockchain-based services consist of subsystems that use a blockchain-based solution integrated with the communication architecture of the BVLOS drone operation. The objective is to design a blockchain solution deployable to the drones and the Ground Stations (GS) computing platforms. This solution will add services such as authentication and trust management, using trustworthy data securely.

For that purpose, we model the entities of the U-Space (i.e.; drones and ground stations) as communicating network nodes, where a local replicate of the shared blockchain is maintained. The proposed solution is intended to be embedded inside drones and ground stations for securing the sensitive data to be used by future on-chip compute platforms.

This work is part of the Airborne Data Collection on Resilient System Architectures (ADACORSA) European project [21]. Figure 2 shows the blockchain-based services (LS_Blockchain_based_services) positioning within the overall ADACORSA system architecture. The communication layer handles most of the communications. It is important to note that the position of these components is for evaluation purposes and is not currently embedded in real drones. That is why, in this figure, secure communications, drone services and external entities (i.e., drones and ground stations) are represented as Logical Actors. In future real implementations, the blockchain-based services would be integrated at the Reliable Communication component level.

Figure 2: Block Diagram within the Overall System Architecture

The blockchain-based services system consists of a main component called Tamper-proof Storage Service (TSS) and dedicated service components, both embedded in the drones and the ground stations. Because of TSS, the drones and the ground stations collaboratively maintain and share sensitive data in such a way that it is traceable and that its integrity is protected from intentional and unintentional modifications. Blockchain technology is used to store, distribute and validate data using a chain of cryptographically connected blocks. In practical use, the blockchain peer-to-peer network consists of drones and grounds stations and the blockchain data structure is stored and managed by TSS.

TSS provides a common abstract view and interface to allow in-depth study of the characteristics and performances of blockchain solutions. It makes explicit interactions and transaction management so that interactions with the blockchain are externalized; for
example, TSS interacts with other services using interfaces for transaction submission. In addition, it provides internal management services for node synchronization and protocol support. As illustrated in Figure 3, TSS is composed of two components: Blockchain Management and Local Blockchain Storage.

Figure 3: Block Diagram of Blockchain-Based Services

3.1 Blockchain Management

Blockchain Management is responsible for generic blockchain operations, including data registration into the Local Blockchain storage, data validity verification, stored data reading and data synchronization within the network. This sub-component manages the data structures and operations of external services (Service A and Service B). It also contains dedicated APIs and libraries, as well as internal management and applicative transactions.

The two categories of transaction types supported are:

- default blockchain transactions such as coin base transaction and token transfer transaction
- applicative transactions dedicated to specific services (section 4).

3.2 Blockchain Storage

The Local Blockchain Storage is responsible for storing data in the form of a time-stamped network of secure data logs. To provide services in a trustworthy and decentralised way, the blockchain-based services can require the data be stored in the Local Blockchain Storage.

Due to the memory and computation requirement, not every device maintains a full replica of the blockchain locally. Depending on the needs and capabilities of the support devices, TSS can be implemented in two ways: as a lightweight node or as a full node. In the example illustrated in section 4 "Blockchain-based Authentication Architecture", full nodes are deployed on ground stations while light nodes are deployed on drones. TSS for drones communicates with and relies on full nodes (i.e., TSS for Ground Station) to provide it with necessary information.

4 CASE STUDY: BLOCKCHAIN-BASED AUTHENTICATION ARCHITECTURE

This section provides a concrete application of the generic architecture described previously in section 3: a blockchain-based authentication service for BVLOS drones operation.

Providing decentralised authentication functionalities contributes to secure communication and trustworthy cooperation in open networks of drones. In traditional centralised approaches, drones rely on information from a trusted third party such as a ground station to perform authentication services. However, in BVLOS operation, the connection with the ground stations is interrupted. In this case, drones could benefit from a decentralised ledger that allows them to access a local copy of the necessary information to continue providing authentication services.

The Authentication subsystem (LC_Authentication illustrated in Figure 4) enables drones operating BVLOS to authenticate other entities in the network and subsequently establish secure communication channels between those drones. In networks of drones, the main functions provided are decentralised entity authentication and secure storage of authentication-related data.

The system consists of two main components:

- TSS component (LC_DLT_TamperProofStorageService), previously described in section 3. In this context, TSS is responsible for the management of the authentication data and decentralised, secure, permanent storage. This component allows the drones and the Ground Stations to maintain and share sensitive data in a non-alterable way collaboratively.
- Authentication Service (AS) component (LC_Authentication) which provides the protocol and cryptographic operations required for decentralised authentication using TSS. For its operation AS requires the data stored in the TSS component. AS also handles authentication requests.

Figure 4: Block Diagram of the Blockchain-Based Authentication Service Architecture

AS component provides its service (i.e., entity authentication) to cooperative applications between drones. These applications communicate with other drones using the reliable communication hardware and software of the drone. In this context, the authentication protocol provided by the AS is used in the process of establishing secure communication channels for the communication partner authentication.

Blockchain-based technologies ensure storage, consistency, decentralised resilient and tamper-proof properties. Thus, the TSS
component brings security properties such as verifiable interactions, resilience, and accountability to the system. The distributed nature of the TSS ensures that, in principle, the drones do not necessarily have to maintain such a component. However, it is assumed that each drone maintains its own TSS component. This way, in cases where a drone does not have access to a TSS component on a trusted ground station, it can still provide an authentication service.

### 4.1 Authentication Service (AS)

This component allows the authentication of drones and other entities in networks of drones operating BVLOS. The authentication service outlined in this paper is based on the blockchain-based Public Key Infrastructure (PKI) described in detail in [16]. Its operation can be summarised as follows:

The PKI binds identities to public keys that are used securely during the authentication process. It guarantees that a public key belongs to an identity. The blockchain-based PKI stores the identities, their corresponding public keys and the confirmations of bonds between identity and public keys.

The authenticity of a previously unknown identity public key pairing has to be checked before using it, i.e., the entity has to ensure that the public key is controlled by the stated identity. To this end, the entity requires a confirmation from a trusted source. Confirmation establishes trust relationships between the entities and can take different forms, such as a digital certificate or a special transaction of the blockchain system.

Mathematically, the authors of [16] model these relationships as a directed graph, called a trust graph. Nodes of the trust graph represent the identities and their public keys. Directed edges between the nodes represent confirmations. The trust model defines how confirmations are interpreted, how "chains" of confirmations are evaluated and who is allowed to create confirmations.

Therefore, in their model, a dedicated blockchain of the PKI is used to store, update, and provide the trust graph. For that purpose, in addition to the default transaction types (i.e., coinbase transaction and token-transfer transaction), the system uses the following applicative transactions for authentication:

- **Entity transaction**: This applicative transaction is used to store authentication-related public keys with a signature and the information about the entity identity, such as name and characteristic properties. It allows the creation of a node in the trust graph. Every blockchain account can only make at most one entity transaction.

- **Revoke entity transaction**: This transaction can only be made if the account has previously issued an entity transaction. Its role is to delete a node and all incoming and outgoing edges in the trust graph.

- **Confirmation transaction**: The sender uses this transaction to confirm the binding between a receiver identity and a key. The confirmation transaction creates a directed edge from the sender node to the receiver node in the trust graph. It also assigns the maximal allowed path length. In the case an edge between two nodes already exists, it updates the number.

- **Revocation transaction**: A sender uses this transaction to revoke a confirmation transaction that it previously performed. The revocation transaction deletes an edge in the trust graph.

As drones have limited data storage and processing capacity, it is hardly feasible that they participate in the consensus process or store the entire blockchain. In particular, for authentication purposes, they only need their own key pairs and the trust graph. They only store the trust graph parts that are relevant to them, i.e., the data of the entities to which they are connected via a valid path. To update the trust graph during a mission and to use the channels to the blockchain network, they can also store the block headers. The nodes and edges are then stored in an appropriate format.

Therefore, it is assumed that each drone maintains its own TSS component to provide a blockchain-based authentication service in cases where a drone does not have access to a TSS component on a ground station. TSS for drones takes the form of a lightweight node. It does not store the entire copy of the chain but only queries the current state to determine the last block and broadcasts transactions for processing. TSS for Ground Station takes the form of a full node. It holds a copy of the entire blockchain, participates in the consensus process, and verifies transactions. TSS for drones communicates with and relies on information stored on full nodes (TSS for Ground Station).

### 5 RELATED WORK

Blockchain technology enables decentralised and trustworthy exchange and storage of drone system data. It also allows for traceability of exchanges and performs synchronisation with other nodes in the network.

In this context, according to our observation, most of the proposed blockchain-based solutions focus on the network and communications aspects of drone systems [2, 3, 5, 7, 9]. For example, [5] presents a blockchain-based network model for unauthorized drone detection in Internet of Drone (IoD) environment. In their approach, blockchain technology is used to record various events in the IoD environment that facilitates any AI-enabled Big data analytics to read this data from the blockchain and provide various statistical analytics to improve the system. Another approach for blockchain-based IoD is also described in [2]. The solution is called UTM-Chain. It allows to secure drone flight plans and store flight data records of drones. In their architecture, the users, drones, and ground stations act as nodes, holding the whole blockchain and participating in the consensus protocol to verify blocks. [3] proposes a system architecture of blockchain-assisted 5G drone network where data processing and storage are handled at the edge or the cloud. Blockchain authenticates communications among drones by tracking all their transactions, making it available to all network nodes, and achieving data integrity (i.e., cryptography) to provide tamper resistance. In [9], the authors designed a drone and blockchain-based system for Industry 4.0 inventory and traceability applications. The proposed solution consists of a communication architecture that uses a blockchain to store inventory data collected by drones. The ground station makes use of a software module that acts as a blockchain client. The authors of [7] also proposed
a blockchain-based general architecture for data collection and management of components in drones.

While the above examples deal with network and communication aspects, several contributions have also been made on protocols and algorithms [4, 10, 17, 19]. The authors of [19] proposed a blockchain-based solution to achieve cross-domain authentication for 5G-enabled drones. Their approach employs multiple signatures based on threshold sharing to build an identity federation for collaborative domains. Reliable communication between cross-domain devices is achieved by utilizing smart contracts for authentication. A blockchain-based technique to support multi-party authentication to facilitate trustworthy communications between a group of drones is proposed in [10]. In [4], the authors proposed a lightweight blockchain-based model to provide distributed authentication and anonymous authorization in IoT. The authors of [17] proposed a decentralised architecture of flying ad hoc nodes based on blockchain and using Practical byzantine fault tolerance (PBFT) for consensus among nodes.

In the end, few studies focus on the architectural level of on-chip compute platforms of drones. An example is described in [6], where the authors proposed a concept based on blockchain embedded in the drones and some nodes on the ground stations. Their solution is composed of two main block components:

- High level applicative component based on a Robot Operating System (ROS) middleware in which the main drone functionalities are implemented and which integrates at least three nodes:
  - The Navigation node or drone state estimation node that provides the drone position and velocities, which are necessary to the other nodes;
  - The Control node or automatic pilot node that manages the behavior of the drone according to information received from the Navigation node and the Blockchain Management node;
  - The Blockchain management node that links the blockchain and the other nodes.
- A blockchain component that is assumed to communicate with ROS nodes through a web API (REST/RPC). This block implements all the blockchain functionalities (e.g., synchronization with the other nodes, blockchain network management, insertions of new transactions, execution of smart contracts).

They assume that the drones only communicate together through the blockchain. The synchronization of the blockchain clients allows transferring the written data.

While most approaches tackle network (or communication) and protocol (or algorithms) aspects, few studies focus on the architectural level of on-chip compute platforms of drones. Therefore, there is a lack of proposal on lightweight blockchain-based service architecture for on-chip compute platforms of drones. On the other hand, our proposed solution deals with a lightweight generic blockchain-based service architecture for on-chip compute platforms of drones.

6 CONCLUSION AND FUTURE WORK

In this paper, we provided, in a first step, a generic blockchain-based service architecture. This solution consists of a main component called Tamper-proof Storage Service (TSS) and dedicated service components embedded on drone and ground station on-chip compute platform. TSS allows the drones and the ground stations to collaboratively maintain and share sensitive data in such a way that it is traceable and that its integrity is protected from intentional and unintentional modifications. For that purpose, TSS contains components that are responsible for blockchain management and the local blockchain storage.

In a second step, we provided a concrete realization of this generic blockchain-based service architecture which is a blockchain-based authentication service. It enables secure communication and trustworthy cooperation in open networks of (semi-)autonomous drones and the Internet of Things. This blockchain-based authentication service is composed of an Authentication Service (AS) that provides the protocol and cryptographic operations required for authentication and a TSS that is used by the AS for secure, permanent storage and management of the authentication data in a decentralised way.

In this study, we focus on open networks of drones. Our proposed solutions may also be suitable for cars or smart sensor networks.

As the proposed solution is intended to be embedded inside drones and ground stations for securing the sensitive data used by the on-chip compute platforms, simulations will permit the evaluation of different protocols and algorithms for future implementation on real drones and ground stations. To this end, a UTM blockchain simulation environment model is being developed in the continuation of this work. This model will be used for tests and evaluation based on scenarios parametrized with different types and numbers of drones. For that purpose, implementations are performed using the MAX agent-based modeling and simulation framework dedicated to blockchains [11, 12, 18].

ACKNOWLEDGMENTS

This work is supported by ECSEL Joint Undertaking (JU) through the Project ADA4CORS under grant agreement No 876019. The JU receives support from the European Union’s Horizon 2020 research and innovation program and Germany, Netherlands, Austria, Romania, France, Sweden, Cyprus, Greece, Lithuania, Portugal, Italy, Finland, Turkey.

The authors also thank Nicholas Jäger [16] who collaborates with us on the presented case study focusing on the algorithmic details.

REFERENCES

[1] Tejasvi Alladi, Vinay Chamola, Nishad Sahu, and Mohsen Guizani. 2020. Applications of blockchain in unmanned aerial vehicles: A review. *Veh. Commun.* 23 (2020), 100249. https://doi.org/10.1016/j.vehcom.2020.100249

[2] Azza Allouch, Omar Cheikhrouhou, Anis Koubia, Khalifa Toumi, Mohamed Khalgui, and Tuan Nguyen Gia. 2021. UTM-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones. *Sensors* 21, 9 (2021), 3049. https://doi.org/10.3390/s21093049

[3] Moayed Aliqaly, Ouns Bouachir, Azeddine Boukerche, and Ismaeel Al Bidhawi. 2021. Design Guidelines for Blockchain-Assisted 5G-UAV Networks. *IEEE Netw.* 35, 1 (2021), 64–71. https://doi.org/10.1109/MNET.011.2000170

[4] Nittish Andola, Raghav, Vijay Kumar Yadav, S. Venkatesan, and Shekhar Verma. 2021. SpyChain: A Lightweight Blockchain for Authentication and Anonymous
Authorization in IoD. *Wirel. Pers. Commun.* 119, 1 (2021), 343–362. https://doi.org/10.1007/s11277-021-08214-8

[5] Başudeb Bera, Ashok Kumar Das, and Anil Kumar Sutrala. 2021. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Comput. Commun.* 166 (2021), 91–109. https://doi.org/10.1016/j.comcom.2020.12.005

[6] Mário Gabriel Santos De Campos, Caroline F. C. Chanel, Corentin Chaufaut, and Jérôme Lacan. 2021. Frontiers Robotics AI 8 (2021), 557692. https://doi.org/10.3389/frobt.2021.557692

[7] Rupa Ch, Gautam Srivastava, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, and Sweta Bhatacharya. 2020. Security and privacy of UAV data using blockchain technology. *J. Inf. Secur. Appl.* 55 (2020), 102670. https://doi.org/10.1016/j.jisa.2020.102670

[8] Bitcoin Core. [n.d.]. Running A Full Node. https://bitcoin.org/en/full-node#what-is-a-full-node Accessed: 09.11.2021.

[9] Keke Gai, Yulu Wu, Liehuang Zhu, Kim-Kwang Raymond Choo, and Bin Xiao. 2021. Blockchain-Enabled Trustworthy Group Communications in UAV Networks. *IEEE Trans. Intell. Transp. Syst.* 22, 7 (2021), 4118–4130. https://doi.org/10.1109/TITS.2020.3015862

[10] Önder Gürcan. 2019. Multi-Agent Modelling of Fairness for Users and Miners in Blockchains. In 2nd Workshop on Blockchain Technologies 4 Multi-Agent Systems (BCT4MAS), co-located with PAAMS 2019, Avila, Spain, June 26-28, 2019

[11] Önder Gürcan. 2020. On Using Agent-based Modeling and Simulation for Studying Blockchain Systems. In *JFMS 2020 - Les Journées Francophones de la Modélisation et de la Simulation - Convergences entre la Théorie de la Modélisation et la Simulation et les Systèmes Multi-Agents*. Cépaduès, Cargèse, France, 23–24

[12] Önder Gürcan, Antonella Del Pozzo, and Sara Tucci-Piergiovanni. 2017. On the Bitcoin Limitations to Deliver Fairness to Users. In *On the Move to Meaningful Internet Systems. OTM 2017 Conferences*, H. Panetto, C. Debruyne, W. Gaaloul, M. Papazoglou, A. Paschke, C-A. Ardagna, and R. Meersman (Eds.). Springer International Publishing, Cham, 589–606.

[13] Önder Gürcan, Alejandro Ranchal Pedrosa, and Sara Tucci-Piergiovanni. 2018. On Cancellation of Transactions in Bitcoin-Like Blockchains. *Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11229 LNCS (2018), 516–533.

[14] ICAO. 2017. Remotely Piloted Aircraft System (RPAS) Concept of Operations (CONOPS) for International IFR Operations. https://www.icao.int/safety/UA/Documents/RPAS%20CONOPS.pdf Accessed: 29.10.2021.

[15] Nicholas Jager and Andreas Aßmuth. 2021. An Approach for Decentralized Authentication in Networks of UAVs. *CLOUD COMPUTING 2021* (2021), 22.

[16] Sandip Ray, Eric Peeters, Mark Mohammad Tehranipoor, and Swarup Bhunia. 2018. System-on-Chip Platform Security Assurance: Architecture and Validation. *Proc. IEEE* 106, 1 (2018), 21–37. https://doi.org/10.1109/JPROC.2017.2714641

[17] Hector Roussille, Önder Gürcan, and Fabien Michel. 2022. AGR4BS: A Generic Multi-Agent Organizational Model for Blockchain Systems. *Big Data and Cognitive Computing* 6, 1 (2022). https://doi.org/10.3390/bdc6010001

[18] Ethereum Wiki. [n.d.]. Light Client Protocol. https://eth.wiki/en/concepts/light-client-protocol Accessed: 09.11.2021.

[19] Yang Xiao, Ning Zhang, Wenjing Lou, and Y. Thomas Hou. 2020. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Commun. Surv. Tutorials* 22, 2 (2020), 1432–1465. https://doi.org/10.1109/COMST.2020.296706