Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs)

Isaac J. Jensen, Daisy Flora Selvaraj, Prakash Ranganathan
School of Electrical Engineering and Computer Science
University of North Dakota
Grand Forks, ND, USA
isaac.j.jensen@ndus.edu

***Abstract*—Unmanned Aerial Vehicle (UAV) technology is quickly growing with a wide range of current and planned future applications. As the technology grows in usage, the data gathered by UAV systems as well as the UAVs themselves will become bigger targets for cyber-attacks. New cyber security technologies, such as the immutable ledger technology known as *blockchain*, should therefore be applied to provide a defense against the growing threat of cyber-attacks. This paper explores blockchain technology, first through a general overview of its components and characteristics, and then at what security improvements it can provide to a system. Following this exploration, the application of blockchain to a UAV swarm environment is briefly expanded on. Lastly, one such blockchain framework known as Hyperledger Fabric is explored, that could potentially be applied to a swarm of UAVs to increase its security.**

Keywords—Unmanned Aerial Vehicle (UAV), blockchain, Hyperledger Fabric

I. Introduction

Unmanned Aerial Vehicle (UAV) technology is being continually developed with an already wide array of current and planned future applications. Because of their "*ease of deployment, low maintenance cost, high-mobility and ability to hover*" UAVs have been predicted and/or tested to be useful in such areas as search and rescue, remote sensing, structure inspection, agriculture, package delivery, traffic monitoring, surveillance, and wireless network coverage [1]. The predicted market value of UAVs is $127 billion with the technology expected to create approximately 100,000 new jobs by the year 2025 [1]. The high versatility of UAVs and the applications that this versatility supports means that UAVs will only become more common throughout everyday life and business. Hence this technology must be robust and secure for users and those benefiting from their use.

One of the key components of UAVs is that they operate remotely and will be operating in at least some capacity over a computer network. Any device operating over a computer network is therefore susceptible to cyber-attacks. These cyber-attack challenges are categorized by Shakhatreh et al. into three categories: confidentiality (C), the protection and secrecy of data; integrity (I), the authenticity of data; and availability (A), the accessibility of services and data [1]. By applying various technologies, we can meet the challenges of these categories. One such technology is blockchain technology, an immutable ledger that could provide improvements in all three of the challenges (i.e., confidentiality, authenticity, and availability). Yet many current blockchain technologies have scaling and delay issues that may not fit well within a UAV environments. Choosing a proper blockchain framework that meets these challenges, such as Hyperledger Fabric, will be critical in future applications of blockchain technology.

The paper is organized as follows: First, a general overview of blockchain technology and its key characteristics; Secondly, a look at where industry is currently applying or researching blockchain technology regarding UAVs will follow. Lastly, an evaluation of Hyperledger Fabric to UAV networks is discussed.

II. Blockchain Technology

Though Blockchain is a relatively new technology in the world of cyber-security, it has been the underlying technology that supports Bitcoin system. [2, 3]. Many are speculating the impact it will have on a wide array of applications such as asset management, real estate, healthcare, and Internet of Things (IoT) which contains the UAV domain [3].

A. Blockchain Components

The blockchain network has four main components viz, asymmetric cryptography and node applications, transactions and blocks, the distributed ledger, and the consensus mechanism as shown in Fig. 1 [3, 4].

Each computer or device participating in the network must be running the node application as it allows users to process messages specific to the blockchain network and to interact with it as well (e.g., it allows them to act as nodes in the network) [4]. These messages and interactions must also be kept secure and safe from potential attackers. Therefore, asymmetric key encryption is used to protect the data of the network and its users [3]. Each user's node application is first secured by usage of a private key and only useable via that same private key [3]. Each participant also has a public key, acting as a sort of cryptographic address, which allows other participants to make transactions with them and which may also change after each transaction for a more secure system [3]. In general, the private keys in cryptography methods are known only to their respective user and are used to digitally sign any transactions by that user [3], but in block chain

978-1-7281-0270-2/19/$31.00 ©2019 IEEE

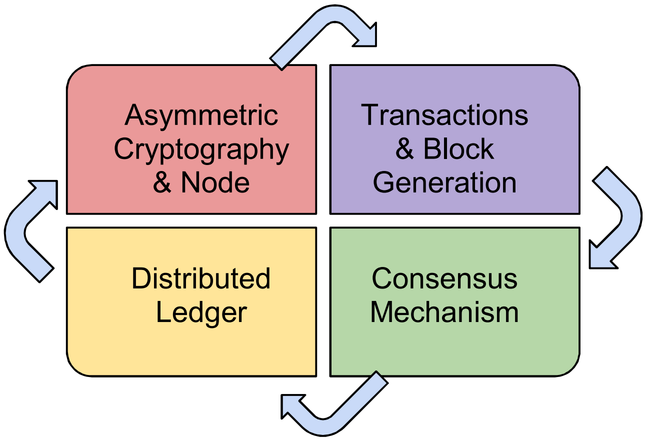
Asymmetric Cryptography & Node
Transactions & Block Generation
Distributed Ledger
Consensus Mechanism

Fig. 1. Depiction of core components of blockchain as depicted by [3]

technology, the transactions are transparent, although the messages encrypted by a user's private key is accessible by other users through their public key, without the need for the same private key, achieving consensus among users are distinguishable factors.

When two or more nodes, or network participants, want to transfer or share information, such as digital assets, between one another, they must go through what is referred to as a transaction [3]. When a transaction occurs, the source node generates a file containing information about the transaction; this file is broadcasted to the entire network or selected nodes for validation depending on the consensus mechanism [3]. Validation entails making sure the transaction is not violating network specific regulations, such as spending assets that do not exist. After validation, these transactions are congregated into blocks of other transactions, the size of which depends on application; these blocks are then approved and added to the blockchain again depending on the consensus mechanism being utilized [2, 3].

The most important component of the blockchain network is the blockchain itself, otherwise known as the shared and distributed ledger. The distributed ledger is a data structure maintained and kept on each node application whose contents are identical to each other participating node that holds a copy [3]. The way the ledger is updated and kept identical on each node depends on the implementation of the blockchain and the consensus mechanism. Authors in [5] describe the blockchain data structure as "a chain of information of blocks in which each current block is connected with the previous block using a unique cryptographic identifier". In other words, the current block utilizes a hash value that depends on the content of the previous block to verify that the blockchain has not been tampered.

The consensus mechanism of a blockchain depends on the specific application for which the network was made. Authors in [4] define the consensus mechanism as "providing the 'rules of the game' for how the blockchain ecosystem will arrive at a single view of the ledger." The paper [3] further adds that all participating nodes must agree on the protocol for updating the ledger and maintaining a consistent state rather than "simply [accepting] to be a part of the blockchain, without majority consent". Network characteristics that may require different consensus mechanisms depend upon the type of network (public or private), and other performance metrics like throughput and latency. The original consensus mechanism was the proof-of-work (PoW) protocol; it features specific nodes referred to as miners competing to calculate a hash needed to add the next block to the chain [3]. This mechanism proves to be secure for a large scale public blockchain, but computationally heavy [6]. A modified protocol known as proof-of-stake (PoS) was developed that features a randomly selected "validator" node to validate new blocks and reduces power consumption and eliminates competition when compared to proof-of-work [3, 6]. Another consensus mechanism called the Practical Byzantine Fault Tolerance (PBFT) algorithm has also been used; this algorithm solves the Byzantine Generals problem by computing a decision by feeding a new received message with the current state of the ledger to decide on consensus [3]. PBFT is suitable if the network is private and it also provides major improvements in efficiency and throughput [7]. Numerous other consensus mechanisms exist depending on the intended application and network of the blockchain [3].

B. Blockchain Characteristics

Perhaps the most important characteristic of the blockchain database is its *immutability*. This feature allows participants in the network to trust that transactions and information on the blockchain is tamper-proof; sequential hashing, cryptography, and the decentralized nature of the network makes modification of network data very difficult [8]. Because a blockchain network operates on a peer-to-peer basis, the network can be described as being *decentralized* [6, 8]. This means that there is no central authority with control over the system, no single point of failure, and, because transactions are broadcasted to participants, there is a certain degree of transparency [3, 8, 9]. Blockchain networks may also be described as *persistent* with high data integrity as once blocks pass consensus and are added to the chain, changes are "infeasible" and users can trust that the blockchain will remain consistent [9]. The distributed ledger can also be described as *auditable* as each transaction can be inspected and traced back to corresponding participants [8, 9].

The last major characteristic of blockchain technology described here is the level of *anonymity and privacy* it provides to participants. Through the asymmetric encryption, the keys relative to any acting party is kept anonymous and therefore confidentiality is ensured [8]. That is to say that even if a malicious entity gains access to data on a blockchain, they will not be able to read this data without the keys of corresponding participants in the blockchain [8]. Furthermore, blockchain networks may have varying levels of privacy as these networks can be categorized into three groups: public, private, and consortium [3]. Public blockchains are open platforms that allow participants from various backgrounds to act in the network; they are also often described as permission-less blockchains as there are no authority restrictions on which nodes can read/write or audit [3]. Private blockchains on the other hand do have such restrictions and are often called permissioned blockchains; these networks have access control in place and often have rules on what nodes can do what actions [3]. Private blockchains are typically limited to either a single organization or multiple select organizations [3]. Lastly, consortium blockchains are described as "partially private and permissioned" [3]. In consortium blockchains, a set of nodes has authority for consensus and for deciding who else can participate; read and writes may also be limited to select participants in a consortium network [3].

C. Security Improvements Provided by Blockchain

Through the inherent characteristics of blockchain technology, it can be seen that by implementing blockchain into a system there are improvements in confidentiality, integrity, and in availability.

Confidentiality according to the National Institute of Standards and Technology (NIST) is the "property that sensitive information is not disclosed to unauthorized individuals, entities, or processes" [8]. A first step in confidentiality is access to the network; inherently, public blockchains have no restrictions, but private or consortium networks may limit who can participate in the network [3, 8]. This limits who exactly can see the data in the network. Confidentiality is further enhanced by usage of Public Key Infrastructures (PKI), which utilize asymmetric encryption [3, 8]. This encryption can be further used to authorize new participants and secure communications on the network [8]. Furthermore, by encrypting the data blocks themselves, confidentiality is maximized as only those with the proper private keys can read the relevant information [8]. [8] summarizes the usage of keys as "protection of user information, confidentiality of data, and authentication and authorization to the network."

According to NIST, *Integrity* is the "guarding against improper information modification or destruction" [8]. The immutability characteristic of blockchains ensures a level of data integrity; once information is added to the ledger, users can trust that the transactions on the ledger are valid [8]. In the scenario where activity must be traced back to acting parties, the blockchain provides a way to identify these parties via digital signatures; this feature relates to non-repudiation or the in-ability to duplicate authenticity [8]. This makes the blockchain "fully traceable" and gives "transparency and security" over the network [8]. The relatively recent development of smart contracts in blockchain applications allows parties to establish and ensure rules between one another, further increasing system data integrity [8].

NIST describes, *Availability* as "ensuring timely and reliable access to and use of information" [8]. Because of the earlier mentioned characteristics of decentralization and the peer-to-peer nature of blockchain networks, availability is greatly increased [8]. In the case of attacks on the network, as long as the majority of nodes are not under attack, the network is able to exclude the nodes under attack and continue operation as normal, increasing the resiliency of the network and therefore the availability of blockchain [8].

D. Preventable UAV Swarm Cyber-attacks via Blockchain

After exploring the components and characteristics of blockchain technology, we can observe types of cyber-attacks that UAV swarms are vulnerable to that can be prevented via a proper application of a blockchain network. The authors of [10] provide a summary of attacks that UAV swarm networks are vulnerable. Via speculation, it can be determined how each of these attacks can be prevented, or at least whose execution is made much more difficult, by applying a blockchain to the swarm network.

The first cyber-attack is injection where "attackers inject [false] messages" into the swarm network [10]. Because the blockchain is considered immutable, injecting these false messages is only possible when adding new information which can be prevented by proper consensus mechanisms to approve new messages. Even if injection does occur, because of the traceability of the blockchain, the source of the false message can be found. Identity spoofing, where "attackers impersonate [actors] in the swarm network," is another preventable attack via blockchain [10]. Identities are embodied via public and private keys, requiring attackers to have a valid set in order to impersonate a valid actor's message which is difficult assuming private keys are secure. Jamming and flooding attacks can hinder the availability of the swarm network by making message broadcast difficult and causing high network traffic [10]. Blockchain does not prevent these attacks, but is resistant to them as nodes that are under attack can be excluded and operation on the remaining nodes can continue as normal. Lastly, eavesdropping, where "attackers listen to [network] communication," is preventable via blockchain. Because the blockchain network again uses public and private encryption keys, an attacker would need to have a private key, which is assumed to be secure to a device, in order to decrypt and read communications intended for that device; this makes eavesdropping difficult.

III. Current State-of-the-Art Research

A substantial amount of research is being committed to the search of applications of blockchain to increase the security of systems. Many planned UAV applications will rely on data heavy technologies such as machine learning, cloud technology, image processing and several other complex data collection, sharing, and processing technologies [1]. Therefore, blockchain technology could be crucial in ensuring that data in a system is secure and can be trusted. The following section discusses some of the research and planned applications of blockchain in the UAV and (inherently) the IoT domains.

A. Research on UAVs and Blockchain

Research relating to multi-autonomous-agent systems consisting of UAVs has been carried out using the Ethereum blockchain network [5]. The authors addressed the complications in a centralized system of directing agents by developing a decentralized system [5]. The authors developed a protocol dubbed the Autonomous Intelligent Robot Agent protocol (AIRA) which utilizes blockchain to manage the "economic activity" between actors in a multi-agent system; it deals with "formalization of interaction and data exchange between robotic networks and smart contracts" with flexibility in agent types, services, and tasks [5]. More specifically the protocol uses the Ethereum blockchain platform's smart contracts, agents in the system utilizing Robot Operating System (a "high-level industrial communication framework"), data storage using the InterPlanetary File System, and lastly the Docker virtualization system [5]. Transactions in the system are executed using both tokens from the Ethereum network and their own custom tokens [5]. The AIRA protocol was utilized to implement a Drone Employee project that worked as an infrastructure-operator system in terms of navigation, regulatory, and economic activities using UAVs [5]. The operation entails a request for service, smart contract creation with request data, acceptance of the service by a UAV agent, and establishment and approval of "air corridor[s]" by "agent-dispatcher[s]" [5].

The authors in [11] explored four specific areas where it was claimed that blockchain could be used to secure a system: securing communication, authenticating users, discovering legit devices, and configuring devices. Secure communication can be accomplished by storing public keys for encryption on the distributed ledger of the blockchain; this way a sender would encrypt a message for a certain destination with the destination's public key and then only the destination or receiver would be able to decrypt the key with its secret and locally saved private key [11]. Authentication could be accomplished by again storing public keys of participants on the blockchain; messages sent by participants are digitally signed by the sender, and the receiver is able to decrypt the signature and check it with the protected hash value of the message [11]. Discovery of legitimate IoT devices can be accomplished by querying root servers for trusted nodes and registering in a trusted node [11]. Lastly, configuration can be accomplished by hosting configuration information on the distributed ledger such as last validated firmware version and configuration files [11].

[12] explores simple blockchain-based structures that could be used to secure a system, claiming to present a concept of application where UAVs in a network act as nodes in the blockchain network and are capable of reading and writing transactions to the blockchain. One proposal is the usage of stochastic blocks where devices on the network are split into equivalent groups and these groups act as blockchain participants for a certain period of time with this role transferred after that period of time (this is a repeating process) [12]. They also explore a new consensus mechanism named "Proof of Graph" which involves finding a minimum path in the network of current blockchain participating nodes [12].

The authors of [13] focused their research on "[securing] drone communication during data collection and transmission, as well as to preserve the integrity of the collected data" by proposing a "distributed solution" called DroneChain that utilizes a blockchain network and a traditional cloud server [13]. The role of the blockchain is for provisioning the integrity of collected data as well as for auditing the information stored on the cloud server [13]. Their simulations and evaluations prove their system to be reliable and distributed with "acceptable overhead and scalability" for assuring data integrity and resilience [13]. They explain their systems components as drones that communicate with the control system; the control system that communicates with the drones and reports to the cloud and blockchain;, the blockchain network which is used for data integrity and cloud auditing,; the cloud database which stores commands sent and original collected data and data access from the cloud server, and finally the cloud server which "handles data from drones and data access records" [13]. They go into detail of how their solution operates all together.

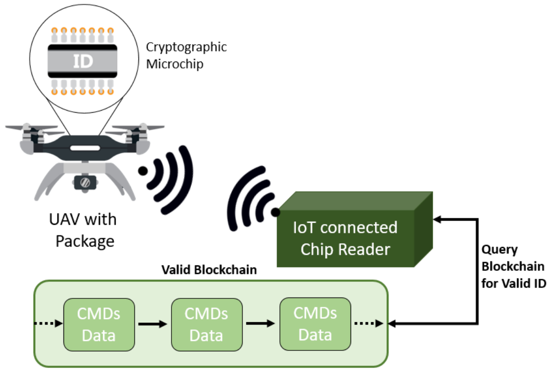

Fig. 2. Depiction of Chronicles package delivery solution [14]

B. *UAVs and Blockchain in Industry*

In general, many industries are exploring the usage of blockchain applied to UAV technologies to secure their operation. One of the UAV applications is a package delivery system that seems to make process quicker, easier, and cheaper. One company, named Chronicled, has developed a "prototype solution" for package delivery to homes [14]. Their solution involves UAVs having cryptographic microchips that act as identifiers; these chips are read by IoT-connected chip reader devices for the UAV's unique cryptographic signature [14]. This signature is checked with a blockchain network for validity and if it passes, permission is granted for package delivery (the process is depicted in Fig. 2) [14]. Well-known company Walmart is also planning to use blockchain in drone package delivery; they have submitted a patent that details how they plan to use blockchain to track information related to package delivery via UAVs [14]. Finally, another company has a delivery drone platform, yet also is working on a much broader "blockchain-based B2R (business to robots) operating platform"; SKYFchain platform's focus is to provide a common place for market participants (clients, providers, etc.) to interact with an "underlying token and smart contract system" inherent of a blockchain network [14].

The other large area of focus for the application of blockchain systems in the UAV industry is related to the tracking and monitoring of UAVs in the airspace. One such company, AERO Token, is developing an Ethereum-based blockchain platform that allows drones to be granted permission to fly over private properties in exchange for economic income [14]. Similarly, a company by the name of Distributed Sky is developing their own version of a "UAS Traffic Control" system that autonomously monitors UAVs [15]. Lastly, IBM has been reported to have submitted a patent in regards to UAVs and their monitoring in both commercial and civilian applications [15]. The IBM authors describe the system as having a blockchain ledger store information about UAV flights in blockchain blocks, especially when UAV flights are tagged as high security risks [16]. The goal of their technology is to provide "airspace controllers and regulators" a way of reliably monitoring UAVs in the airspace [16].

C. *Expanding on UAV Applications: the UAV Swarm*

UAV swarm technology is a complex technology currently being explored and developed that has potential applications in which a singular drone would not suffice or where communication and collaboration of many UAV actors is crucial. Besides many technological obstacles to make such a concept possible, a major challenge is keeping a system of many mobile actors secure from imposters and attacks from malicious entities. Blockchain technology would offer a solution to many security concerns, many of the improvements highlighted under section II. The authors of [13] suggest UAV registration keys that authorize UAVs to submit data to a cloud database, but it could be taken a step further for swarm activity where each UAV would be required to register first before being accepted as a valid actor in the system (Fig. 3). Drones without such a valid, registered key for safely encrypting their data transmissions to the swarm would be labeled as a threat and made aware by the system. The blockchain would be used as a means of safely storing and protecting and managing valid keys. Blockchain would not only be used for identifying valid actors, but also for ensuring that, once data is collected and stored in the network, the data can be considered safe from tampering. This way, once UAVs submit data and commands (to other UAVs in the swarm) on the network, this information is made concrete and unchangeable, allowing the system to trust and audit it. Any attempted change made to the blockchain would be detected and rejected. Blockchain technology could therefore effectively protect UAV swarms against malicious attacks.

IV. HYPERLEDGER FRAMEWORK

The Hyperledger project began late in the year 2015 under the Linux foundation [6]. The goal of the project was to make improvements upon blockchain technology by increasing both performance and reliability; the end result was six types of Hyperledger frameworks as well as six different tools that can be used by developers for a wide variety of applications [17]. Here, the framework known as Hyperledger Fabric will be discussed in short as well as the advantages it can provide over other blockchain platforms such as Bitcoin or Ethereum. A short hypothetical application of Hyperledger Fabric to a UAV swarm environment is discussed afterwards.

A. *Hyperledger Fabric Overview*

Hyperledger Fabric is one of the six available blockchain frameworks developed under the Hyperledger Project. The Hyperledger Fabric framework is a platform that allows developers to develop a private and permissioned blockchain with relative ease [6]. New members of the blockchain are required to register through the platform's Membership Service Provider (MSP), hence the permissioned and private nature [6]. Flexibility is provided in how information is stored in the distributed ledger, how the consensus mechanism can be modified according to requirements, and how different MSPs can be provided [6]. There is also an increased potential for privacy as the platform allows for multiple channels on the network with each channel being able to have its own separate distributed ledger, allowing a network to be divided into groups if needed [6].

The different functionalities of Hyperledger Fabric are outlined in [6] as follows: identity management, privacy and confidentiality, efficient processing, chaincode functionality, modular design, and a state database. Identity management allows the private blockchain to require users to register to the network and give them unique identities in order to monitor and regulate their actions [6, 17]. Privacy and confidentiality is provided through the ability to establish private channels and therefore private blockchains on the network [6]. Efficient processing is manifested in Hyperledger Fabric through parallelism as transaction execution and commitment and ordering can be executed in parallel with multiple transactions being executed simultaneously as well [6]. Chaincode functionality, which is synonymous with smart contract functionality, allows different rules to be applied to different transactions between different groups in terms of validation and endorsement [6]. Modular design gives developers flexibility in terms of the identification, encryption, and consensus used on their blockchain network as well as ways to easily interface with existing systems [6]. Lastly, Hyperledger Fabric allows a state database to "store the current state of the key-value pairs from the ledger"; this increases transaction efficiency [6]. In short, Hyperledger Fabric is a blockchain platform that offers developers a high level of flexibility, offers "much less latency in operation", and is preferred for applications where security and privacy are essential [6, 18].

Yet one of the largest advantages to using Hyperledger Fabric and other Hyperledger blockchain frameworks is the number of tools and online documentation available for developers. One of these tools, known as Hyperledger Composer, makes the process of building "smart contracts and blockchain applications [simple and fast]" [17]. The author was able to quickly build a simple test blockchain network of a very simple UAV swam simulation. Transactions could be made between Masters and Workers and these transactions were saved and recorded on the blockchain. Hyperledger

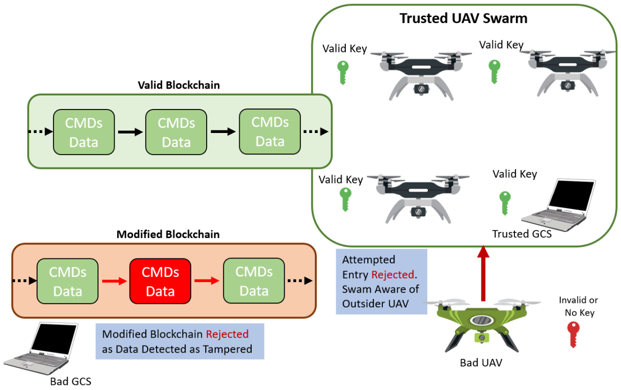

Fig. 3. Depiction of a UAV Swarm utilizing Blockchain technology

Composer proves to offer features that help developers model, control access to, deploy, test, and integrate blockchain networks with existing systems with relative ease [17].

B. *Hypothetical Application: Fabric to UAV Swarm*

Documentation of Hyperledger Fabric features allows developers to see how features of thi framework could be used to help secure their system. Here we explore how various features of Hyperledger Fabric can be used to help secure a UAV swarm network. Assume that the UAV swarm consists of Ground Control Stations (GCSs), Master UAVs, and Slave UAVs.

The Hyperledger Fabric model is described to have "key design features" implemented into the framework; they are listed as assets, chaincode, ledger features, privacy, security and membership services, and consensus [19]. Here we briefly explore what a few of these mean in a UAV swarm environment. Assets are "represented… as a collection of key-value pairs;" in a swarm, the main assets would be Slave UAVs (or contracts for their services) and the data collected by UAVs [19]. Chaincode is software that defines assets as well as how the assets can be transacted or modified; in a swarm, chaincode could represent functions for changing swarm UAV membership or exchanging data collected by UAVs [19, 20]. Privacy and Security and Membership Services are discussed shortly in the following paragraphs while discussing various features of Hyperledger Fabric.

One concept developed into Hyperledger Fabric is the idea of identity management. Any actor on a Fabric network is required to have a X.509 standard digital certificate with an encapsulated digital identity in order to be allowed to act in the system; these identities not only allow the network to disassociate from different actors, but also "determine the exact permissions over resources and access to information that actors have" [21]. By giving out different types of certificates, a swarm network utilizing blockchain can easily define what actions various actors are able to perform. For instance, Slave certificates would limit Slave drones to only communicate with UAVs in their swarm. Master certificates would allow them to not only communicate with their swarm, but also send commands to Slaves in the swarm, communicate with other Masters, and communicate with GCSs. GCS certificates would allow GCSs to communicate with and monitor all UAVs on the network and perform specific GCS only functions. Furthermore, each identity must be "verifiable … [and] come from a trusted authority" which is implemented via MSPs described below [21]. Each certificate in the network must also come from a trusted Certificate Authority (CA) whose role is to issue certificates; Hyperledger Fabric allows what is known as Fabric CA, a "private root CA provider capable of managing digital identities" [21]. In the UAV swarm environment, a select GCS (or a select few) or other separate system would act as the network's Fabric CA. In a swarm environment, it is very possible for UAVs or even other actors to be lost or for other reasons become untrusted; the Certificate Revocation List held by the Fabric CA would allow the swarm network to remove previously trusted actors [21].

Membership in Hyperledger Fabric is acted out via what are called Membership Service Providers (MSPs); these "[identify] which [CAs] are trusted to define the members of a trust domain" [21]. This is done by listing members' identities and or identifying authorized CAs who are trusted to issue valid certificates for said members of what is called an organization, which is defined simply as "a managed group of members" [21]. Furthermore, MSPs also are used to define what roles an actor can play in the network and for what resources this actor has access privileges [21]. This feature plays great importance in securing a UAV swarm. MSPs would define what UAVs belong to which swarms and what roles these UAVs play in that swarm. As an example, an MSP could layout what Slave UAVs are under direction of a certain Master UAV and what role each Slave UAV plays in the swarm.

Peers in a Hyperledger Fabric blockchain network host both the ledger and the smart contracts associated with that ledger [21]. In a swarm environment, it is not desirable for every UAV to act as a peer on the network as managing the blockchain network would become difficult with so many mobile actors. Therefore, only Master UAVs and GCSs may act as peers. Two important types of peers in Hyperledger Fabric are endorsing peers, whose endorsement is needed to approve of ledger updates, and orderer peers, who are responsible for packing blockchain transactions into blocks and distributing these blocks for approval [21]. Changes to the ledger are executed through chaincode and each chaincode has an endorsement policy describing from what organizations a transaction needs endorsement from to be executed [21]. In a swarm environment, an action such as transferring Slaves between swarms would require endorsement from each Master UAV who would act as endorsing peers. A swarm application would utilize endorsing policies to require transactions of say UAVs or the data they carry to require endorsement from the effected entities in the network. Orderers in a swarm environment should be enacted by non-swarm actors such as GCSs who have more reliable access to the network, allowing them to more easily receive transactions and more easily distribute blocks. An interesting feature implemented into Hyperledger Fabric is the idea of channels; channels allow different and "separate ledgers of transactions" between different (or even overlapping) groups of actors [21]. This is not necessary in a UAV swarm environment, but could be used to separate data from different swarms on the same blockchain network or to allow different channels for masters (or slaves) to communicate separate from other UAVs. The full details on how exactly Hyperledger Fabric can be utilized to create a fully functioning, blockchain protected UAV swarm is not presented here due to length restrictions. Many of the details and limitations can only be discerned by an actual application of Hyperledger Fabric to a UAV swarm.

V. Conclusion

The usage of UAVs in industry will only continue to increase, and it is important that the systems that rely on UAV technology are kept as secure as possible from malicious attacks. Blockchain tools (*e.g., Hyperledger Fabric*) offer promising solutions in preserving CIA properties. Applying blockchain appropriately will allow developers to implement trustworthy UAV systems in domains such as search and rescue, traffic management, infrastructure inspection, and many other areas. Development of custom block chain solutions is also very possible and viable, if trade-off between computational and energy limitations are obtained for UAVs.

VI. Acknowledgement

This work is supported by Rockwell Collins Corporation Grant.

References

[1] H. Shakhatreh, A. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. Shamsiah Othman, A. Khreishah, M. Guizani, "Unmanned Aerial Vehicles: A Survey on Civil Applications and Key Research Challenges," April 2018. [Online serial]. Available: https://arxiv.org/pdf/1805.00881.pdf . [Accessed Dec. 19 2018].

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *bitcoin.org,* October 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Dec. 28, 2018].

[3] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," *IEEE Consumer Electronics Magazine,* June 2018. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8386948/authors#authors [Accessed: Jan. 4 2018].

[4] Neocapita, "The Logical Components of Blockchain," *medium.com,* Feb. 2017. [Online] Available: https://medium.com/@neocapita/the-logical-components-of-blockchain-870d781a4a3a [Accessed: Jan 4 2019].

[5] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems,* November 2017. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8101648 [Accessed: Dec. 29 2018].

[6] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," *2018 IEEE International Conference on Innovative Research and Development,* June 2018. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8376323 [Accessed: Dec. 8 2018].

[7] H. Sukhwani, J. M. Martinez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)," *2017 IEEE 36th Symposium on Reliable Distributed Systems,* October 2017. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8069090 [Accessed: Dec. 8 2018].

[8] Deloitte, "Blockchain & Cyber Security. Let's Discuss," *Deloitte,* Performance magazine issue 24, September 2017. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf [Accessed: Dec. 29 2018].

[9] J. Moubarak, E. Filiol, and M. Chamoun, "On Blockchain Security and Relevant Attacks," *2018 IEEE Middle East and North Africa Communications Conference,* June 2018. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8371010 [Accessed: Dec. 8 2018].

[10] Manesh, Mohsen Riahi, and Naima Kaabouch. "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system." International Journal of Critical Infrastructure Protection 19: 16-31, 2017.

[11] M. Singh, A. Singh, and S. Kim, "Blockchain: A Game Changer for Securing IoT Data," *2018 IEEE 4th World Forum on Internet of Things,* May 2018. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8355182 [Accessed: Dec. 29 2018].

[12] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles," *2018 IEEE International Conference on Service Operations and Logistics, and Informatics,* October 2018. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8476785 [Accessed: Dec. 29 2018].

[13] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards Data Assurance and Resilience in IoT Using Blockchain," *2017 Military Communications Conference,* December 2017. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8170858 [Accessed: Dec. 29 2018].

[14] "Drones + Blockchain = Combining Two Exciting Technologies | Projects Around World," *dronesonvideo.com,* [Online]. Available: http://dronesonvideo.com/drones-and-blockchain-technology [Accessed: Jan 4 2019].

[15] "Distributed Sky Launches a Blockchain Framework for Drone Market," *dronenodes.com,* [Online]. Available: http://dronenodes.com/distributed-sky-drone-blockchain-framework/ [Accessed: Jan 4 2019].

[16] "IBM Patent Eyes Blockchain for Drone Fleet Security," *ccn.com,* Sept. 2018. [Online]. Available: https://www.ccn.com/ibm-patent-eyes-blockchain-for-drone-fleet-security/ [Accessed: Jan. 4 2019].

[17] *hyperledger.org,* [Online]. Available: https://www.hyperledger.org/ [Accessed Jan. 4 2019].

[18] L. Siva Sankar, M. Sinhu, and M. Sethumadhavan, "Survey of Consensus Protocols on Blockchain Applications," *2017 4th International Conference on Advanced Computing and Communication Systems,* August 2017. [Abstract]. Available: IEEE Xplore, https://ieeexplore-ieee-org.ezproxy.library.und.edu/document/8014672 [Accessed: Dec. 8 2018].

[19] *hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html,* [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html [Accessed Mar. 25, 2019].

[20] http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220180270244%22.PGNR.&OS=DN/20180270244&RS=DN/20180270244.

[21] *hyperledger-fabric.readthedocs.io/en/latest/identity/identity.html,* [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/identity/identity.html [Accessed Mar. 25, 2019.