The International Blockchain Registry of Mobile Assets

Erich P. Dylus*

Moving the International Registry of Mobile Assets onto a blockchain registry system that digitally 'tokenizes' each registered asset would provide a more efficient and secure mechanism of authentication, mitigate existing potential liability in registry maintenance for the Registrar, and effectively eliminate many current risks of syntax errors and noncontiguous asset histories. This may be accomplished in accordance with the current legal framework, without complicating the user interface on the front end, and allows for potential future inclusion of the asset tokens into smart contracts.

1 INTRODUCTION

The Convention on International Interests in Mobile Equipment, signed in Cape Town on 16 November 2001 (the 'Convention') operates to facilitate the efficient financing and leasing of mobile equipment including certain aircraft, rail, and space assets.[1] One of the primary objectives of the Convention was to establish a registration of international interests in such assets, thus providing notice to third parties and enabling creditors to preserve priority against unregistered and subsequently registered interests and creditors in the event of a debtor's insolvency.[2] The International Registry (the 'IR') is monitored by the Convention's Supervisory Authority, who appoints a registrar every five years.[3] The IR is publicly searchable online for current registrations, entities, or contracting states. Entities seeking to register interests on the IR must first apply on the website to become an Approved Administrator, complete the required application and review by IR officials, and supply 'any additional information which the Registry Officials need'.[4] The IR is purely digital and will neither perform nor permit registrations or

* Associate in the Global Transportation Finance practice group of Vedder Price P.C.
Email: edylus@vedderprice.com.

1 Official Commentary to the Convention on International Interests in Mobile Equipment, s. 2.1 (3rd ed. Rome 2013) http://www.unidroit.org/instruments/security-interests/cape-town-convention.

2 *Ibid.,* s. 2.6 (accessed 11 Dec. 2018).

3 Convention on International Interests in Mobile Equipment, Art. XVII (Cape Town 2001).

4 Welcome to the International Registry, International Registry of Mobile Assets (accessed 8 Jan. 2018) https://www.internationalregistry.aero/ir-web/index (accessed 11 Dec. 2018).

Dylus, Erich P. 'The International Blockchain Registry of Mobile Assets'. *Air & Space Law* 44, no. 1 (2019): 45–52.

other actions based on external documents or communications other than the electronic consents of all relevant parties provided through the Approved Administrator. This article posits that a blockchain registry system, specifically a 'permissioned' variant of the Ethereum[5] blockchain utilizing a non-fungible ERC721[6] standard to digitally 'tokenize' each registered asset, would provide a more efficient, error-resistant and secure mechanism of authentication and registry for the IR and would mitigate existing potential liability for the Registrar in its assurance of the registry's data security and integrity. Further, moving the IR onto a blockchain registry system need not affect the Supervisory Authority's approval process or confidentiality protocols, which remain essential for the protection of sensitive entity data and Convention compliance.

2 BLOCKCHAIN BACKGROUND

A blockchain is an example of a distributed ledger system, in which any transacted or registered information must be validated as legitimate by the blockchain's applicable consensus protocol and is thereafter permanently preserved.[7] Blockchain registries generally benefit from increased security, accuracy, and efficiency by distributing computation and verification amongst numerous nodes (avoiding a single system intermediary choke point for verification) and by securing information via complex cryptography.[8] Blockchains also maintain systemic transparency by permitting access to block metadata and address transaction history (according to the type of blockchain used, which in this instance could mirror the limited public access of the IR's search function), while upholding security by hashing[9] (or encrypting) any confidential information or values. In this case, to remain compliant with the Convention and current IR protocol, the categories of confidential data or identifiers within the blockchain registry could be encrypted at the discretion of Registry Officials, in line with current practice. These benefits of security, immutability and efficiency have led governments and private entities alike to use blockchains for such varied applications as supply chain management, food and pharma source and quality control, land title record systems, anti-counterfeiting, creative content licensing, and financial instrument trading and

---

5 *See* Ethereum.org.

6 ERC721 is a protocol for digital 'token' asset representation on the Ethereum blockchain that allows each token to carry and be identified by non-fungible (unique) characteristics or labels such as its owner or time of its creation. *See* erc721.org.

7 *See* Blockchain Technology Overview, NIST Internal Rep. 8202, National Institute of Standards and Technology (Jan. 2018) https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf/ (accessed 11 Dec. 2018).

8 *Ibid.*

9 *Ibid.,* Ch. 2.1.

settlement. Specifically for the aviation industry, blockchain has been proposed as a potential solution to aircraft maintenance recordation, along with the facilitation of more cost-efficient commercial and leasing transactions by using cryptocurrency settlement and even a dedicated blockchain for the aviation ecosystem.[10] Blockchain technology provides an opportunity for a simple, efficient and cost-effective overhaul for the essential yet imperfect IR system.

3 VALIDATION AND SECURITY

The IR would be well-suited for a 'permissioned' blockchain,[11] in which the basic history and information of all blocks may be publicly observed but permission must be given to perform certain tasks in writing, reading, and reaching consensus (for example, transacting, adding or validating information or accessing certain encrypted sensitive data – as opposed to a 'permissionless' chain such as bitcoin in which there are no qualifiers to transact and contribute to consensus). Approved Administrators and the Supervisory Authority would receive permissioned status via a cryptographically secured identifier, but their activity could still be publicly monitored on the blockchain in compliance with the Convention, albeit with encrypted values where appropriate. In this way, the Approved Administrators and Registrar would maintain their discretionary admission requirements and administration of the Registry users per the Convention,[12] but the backend security and authentication mechanisms of the IR would be drastically improved by blockchain technology.

An asset's registration history would not only be permanently preserved as a past status modification (for example, the occurrence of a registration of an interest or discharge), but also each entity effectuating a change in the asset's registration would have their unique encrypted identifier permanently preserved along with it, which would help to prevent fraud and tampering by leaving a forensic digital imprint. Importantly, permissioned blockchains still entirely resist alteration of historical data, even by the permissioned entities. All entities seeking to record new data or otherwise transact must be authorized by (1) receiving permissioned status and (2) receiving consensus validation by the

---

[10] *See* Lory Kehoe & John Hallahan, *Blockchain – A Game Changer in Aircraft Leasing?*, Airfinance Ann., 84–87 (2017/2018); *See also* Aviation Working Group, *Global Aircraft Trading System: Modernizing Aircraft Transfers* (16 May 2018) www.awg.aero/assets/docs/GATS%20modernizing%20aircraft%20transfers.pdf (accessed 11 Dec. 2018).

[11] There are numerous options for such a permissioned chain designed for enterprise or organization-level requirements built on Ethereum in order to utilize the ERC721 protocol, such as a native private fork of Ethereum, the Linux Foundation's Hyperledger Burrow (https://www.hyperledger.org/projects/hyperledger-burrow, using the Ethereum Virtual Machine), and Quorum (https://www.jpmorgan.com/global/Quorum) (accessed 11 Dec. 2018).

[12] *See supra* n. 5.

network of nodes to write to the blockchain, mitigating conventional centralized security risks. All transactions or new entries by the permissioned actors would leave permanent and irreversible evidence of a change in state or new entry upon the blockchain – any intrusion or attempt by a non-cryptographically permissioned entity to alter the registry system would be rejected. Any such rejection could leave permanent evidence of the rejection (depending upon the protocol desired), allowing further fraud prevention and forensic security.

4 ACCURACY

After the initial approval of permissioned status for the registration process by Supervisory Authority officials, registrations would be less susceptible to human error. For example, when obtaining priority search certificates,[13] aviation counsel title memos or IR opinions commonly include disclaimers such as:

> *If a registration exists against an airframe or engine which describes that object differently than as noted in the certificate (any discrepancy in the description of the manufacturer, model or serial number including any space, added number or character, or missing number or character) the certificate will produce a false negative search result. Therefore, there may exist registrations against the airframe or engine which are not reflected on the certificate and which would have priority over subsequent registrations on the International Registry.*[14]

This type of potential error (registration against an asset that describes the asset incorrectly potentially creating a duplicated registration overlap, conflicting priority and/or a gap in the chain of interests) is mitigated by a blockchain protocol in which changes to an asset's history or status are either confirmed by the nodes as a valid change in block status via correctly entered syntax, or are rejected and return a failed transaction notification (instead of a false negative as in the disclaimer) to the entity attempting to register. This is because any improper syntax compared to an existing asset registration or attempted overwrite of the history of the asset address would produce a completely different hash value (so the request to update or discharge a registration would not be confirmed) and fail to write to the intended blockchain address.[15] All subsequent registrations for an asset must perfectly match its blockchain address identification values, and searches must match the syntax requirements, or the operation will fail and prompt a correction.

---

13 *Convention*, Regulations at s. 7.2.
14 Example disclaimer drafted by the author.
15 Blockchain Technology Overview at Ch. 2.1.

5 ENSURING UNIQUENESS AND AUTHENTICITY

Utilizing a permissioned fork of the Ethereum blockchain with a non-fungible ERC721[16] standard to 'tokenize' each registered asset, or to assign each asset a unique digital ID and function values to be transacted on the IR blockchain as a 'token' representing that asset, would prevent the aforementioned imposter or syntax error registration issues. Each token is referenced on the blockchain via a unique identification value with accompanying characteristics (e.g. MSN, manufacturer, model, year), and any transferee of the token via a new registration after approval would examine the token's metadata history and identifiers for validation. Thus, each asset on the IR would be represented by a unique and non-replicable token, that may be transferred to user entities or updated as applicable with subsequent registrations.

In the current registry system, a slight discrepancy in information entry for a registration concerning an existing asset on the IR could allow the user entity to mistakenly or intentionally effectuate a new registration (because the existing registration would be undetected) that could cause a gap in the chain of title or in priority. This presents massive potential liability for creditors of these assets if their priority is compromised due to a syntax error. Alternatively, a blockchain registry with tokenized assets would reject an entry or change in priority unless the asset's specific token is affected or if no token with the appropriate characteristics yet exists. New token instances would be subject to approval on the permissioned chain, and if there are duplicate characteristics to an existing token, such approval would be rejected. Thus, an entity that attempts to register against an existing asset by deliberately avoiding the existing token will be unable to tokenize and write to the IR blockchain, because approval will only occur if either the unique token is used or if there is no existing token with matching asset identifiers that would otherwise prevent a new instance. If the proper token is used or there is no existing registration and thus a new token is created, the new entry into the blockchain may then receive approval to write. This process provides top to bottom validation and ensures continuity with the asset's history. Put simply: an asset's one true token as confirmed by its characteristics must be utilized in any registration, and initial tokenization may only occur if no such token exists with matching asset identifiers. If there is a malicious attempt at fraudulent registration via a new, rogue token or if a registration using an existing token is incorrectly entered, the operation fails completely. In the current system, inconsistencies in priority or chain of ownership

[16] The ERC721 token standard defines the functions: name, symbol, totalSupply, balanceOf, ownerOf, approve, takeOwnership, transfer, tokenOfOwnerByIndex, and tokenMetadata; and defines two events: Approval and Transfer.

are simply too easy to effectuate via minor human error in syntax or intentional conflicting registrations.

Creditors of such large value assets as aircraft should not subject their interests to typo contingency or noncontiguous asset history risk, and the decentralized, tamper-proof and transparent nature of a blockchain registry should ensure them that their assets are not subject to surprise encumbrances or vulnerable to security risks common to centralized data servers. If and when aircraft transactions are streamlined and secured by the implementation of smart contracts,[17] the transfer of the aircraft's token to the proper party would become a commonplace condition precedent. The IR asset tokens could also be used in conjunction with the Aviation Working Group's Global Aircraft Trading System (GATS), which aims to reduce the legal complications and operational burdens on airlines, lessors, and financiers in transfers and lease novations by standardizing and implementing electronic transfers of beneficial interests in aircraft trusts, verified via e-signatures and blockchain recordation.[18]

If the consensus in data security, especially those in public owner registries, transitions towards demanding decentralization and immutability in a trustless structure, a blockchain IR may one day become a necessity for the IR's continued legitimacy: while the Registrar is not liable for such errors in *received* registration information[19] and all claims against the Registrar are subject to the defence of contributory negligence,[20] the Registrar may be held liable for losses resulting directly from its errors or omissions in maintaining the IR.[21]

6 CONCLUSION

The front-end user interface of the IR need not be complicated by a transition onto the blockchain. Users and site visitors could still search for assets by various combinations of MSN, name, model, or abbreviations thereof on the current system to find links to matching assets' token addresses, or they could input an

---

17 A smart contract is a collection of code and third party data deployed to a blockchain that executes upon the conditions precedent established in the code. The code, being on the blockchain, can be used (among other purposes) as a trusted third party for financial or other transactions that are more complex than simply sending funds, or to perform calculations, store information, and automatically send funds, tokens or information to other blockchain addresses. *See* Blockchain Technology Overview at Ch. 6; Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* (2013), http://ethereum.org/ethereum.html (accessed 11 Dec. 2018); Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 2(9) First Monday (1997).

18 Aviation Working Group, *Global Aircraft Trading System: Modernizing Aircraft Transfers* (16 May 2018) www.awg.aero/assets/docs/GATS%20modernizing%20aircraft%20transfers.pdf (accessed 11 Dec. 2018).

19 *Convention*, Regulations at s. 28(2).

20 *Ibid.,* s. 28(3).

21 *Ibid.,* s. 28(1).

asset's specific blockchain address to locate the relevant token by which it is represented. When the asset token is found, the blockchain would disclose the asset's current IR status along with its entire transactional history – all confidential information concerning the asset would be available only to permissioned entities, encrypted with the level of privacy and carrying any other attributes or data deemed acceptable by the Supervisory Authority.[22] The asset's blockchain address private key could be dispersed in pieces to the user entities and permissioned existing creditors via a password combination or any additional network security measure to prevent a bad actor taking possession of the key. Further, tokenization opens the door to future integration into smart contracts,[23] in which the tokens may be transacted along with payment directly via blockchain.

Creditors would be assured by their possession of their asset's token and blockchain security that the asset's registration status and thus their priority in interest would be incontrovertible until the next transaction event is validated. Furthermore, the blockchain's encrypted and decentralized method of information storage would provide added security for the IR, as well as reduce overhead, maintenance liabilities, and human error risks. The aerospace industry has embraced cutting-edge technology since its inception – this tradition should be reflected in its IR system.

---

[22] This could also include unregistered interests such as specific default remedies or pre-existing rights covered by declaration, as mentioned in Official Commentary 3rd ed. s. 2.7.

[23] A smart contract is a collection of code and third party data, in many cases deployed to a blockchain, that automatically executes upon the conditions precedent established in the code. The code, immutably preserved on the blockchain, can be used (among other purposes) as a trusted third party for financial or other transactions that are more complex than simply sending funds, or to perform calculations, store information, and automatically send funds or information to other blockchain addresses. *See* Blockchain Technology Overview at Ch. 6; *See generally* Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996), *Smart Contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce (Dec. 2016).