

EMERGING TECHNOLOGIES FOR FUTURE SKIES: BLOCKCHAIN



SHAPING
OUR
FUTURE
SKIES

canso.org

Acknowledgements

This paper was produced by the CANSO Strategic Technology Workgroup as part of a series examining emerging technologies. CANSO would like to thank the following experts and their organisations for their dedication and commitment in developing this document:

- Luigi Mazzucchelli, ENAV, Italy
- Martin Bowman, Deloitte
- Raam Chandrasekharan, Deloitte
- Chris Reynolds, MITRE
- Connor Freeberg, MITRE

Contents

Introduction

1.1 Blockchain Fundamentals

Blockchain is a technology that makes it possible for groups of people or organisations to collectively agree on and permanently record information without the need of a central third-party authority. By creating trust in distributing data, Blockchain has revolutionised how we share information and carry out transactions in distributed systems.

At its core, Blockchain is a **distributed digital ledger** that lives on a specific network (e.g. the internet) and records transactions and events. The technology relies on well-established **cryptographic** principles and operates as a repository for information, which is recorded and shared through a **peer-to-peer community**. Within the decentralised network, all participants, referred to as nodes, maintain their own copy of the ledger and validate new entries to the chain through the use of a consensus protocol.

This approach was first used for peer-to-peer (P2P) technologies enabled by the internet, such as media file sharing and internet telephony such as Skype. However, internet-based transfers of **asset ownership** are difficult and elusive to achieve, as this requires ensuring that an asset is only transferred by its true owner and ensuring that the asset cannot be transferred more than once by malicious actors, also referred to as the **double-spend problem**. The asset in question could be digital like a currency or tangible like a deed title with a digital representation on which a stakeholder may assign a value.

Historically, the first and most notable effort to structure and formalise the approach was in 2008, in a landmark paper written by Satoshi Nakamoto (pseudonym) “*Bitcoin: A Peer-to-Peer Electronic Cash System*”. The underlying technology for Bitcoin outlined in Nakamoto’s paper was termed **Blockchain**, which refers to a particular way of organising and storing information and transactions that led to the term “**Distributed Ledger Technology**” (DLT) to refer to the broader category of such technologies.

This approach is based on the principle of recording and sharing data across multiple data stores, each of which have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, called **nodes**.

Blockchain, a particular type of DLT, uses cryptographic methods to create and verify a continuously growing, append-only data structure that takes the form of a chain of so called ‘transaction blocks’ – the Blockchain – which serves the function of a ledger, only distributed.

New additions to the (distributed) ledger are initiated by one of the members (nodes), who creates a new “block” of data, for example containing several transaction records. Information about this new data block is then automatically shared across the entire network, containing encrypted data, and other network participants collectively determine the block’s validity according to a pre-defined algorithmic validation method (‘**consensus mechanism**’).

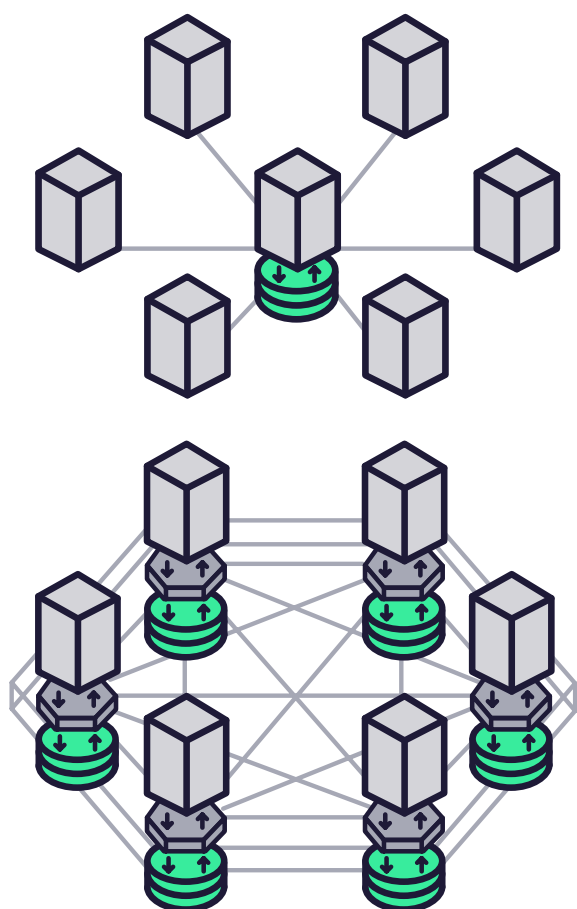


Figure 1 – Centralised model (top) and Distributed Digital Ledger Blockchain model (bottom)

Introduction

1.1 Blockchain Fundamentals (continued)

Only after validation, the new block is added to each participant’s respective copy of the ledger. Through this mechanism each change to the ledger is replicated across the entire network and each network member has a full, identical copy of the entire ledger at any point in time. This approach can be used to record transactions on any asset which can be represented in a digital form.

The distributed ledger is in fact an append-only “database of records”. If a user is to ‘write’ information (a transaction), it must be submitted for verification, validation and finally, insertion, according to the rules of the protocol. By keeping all historic information ever written into the Blockchain nodes, the community can check if the new information is a duplicate. This is a definitive solution to the “double-spend” problem.

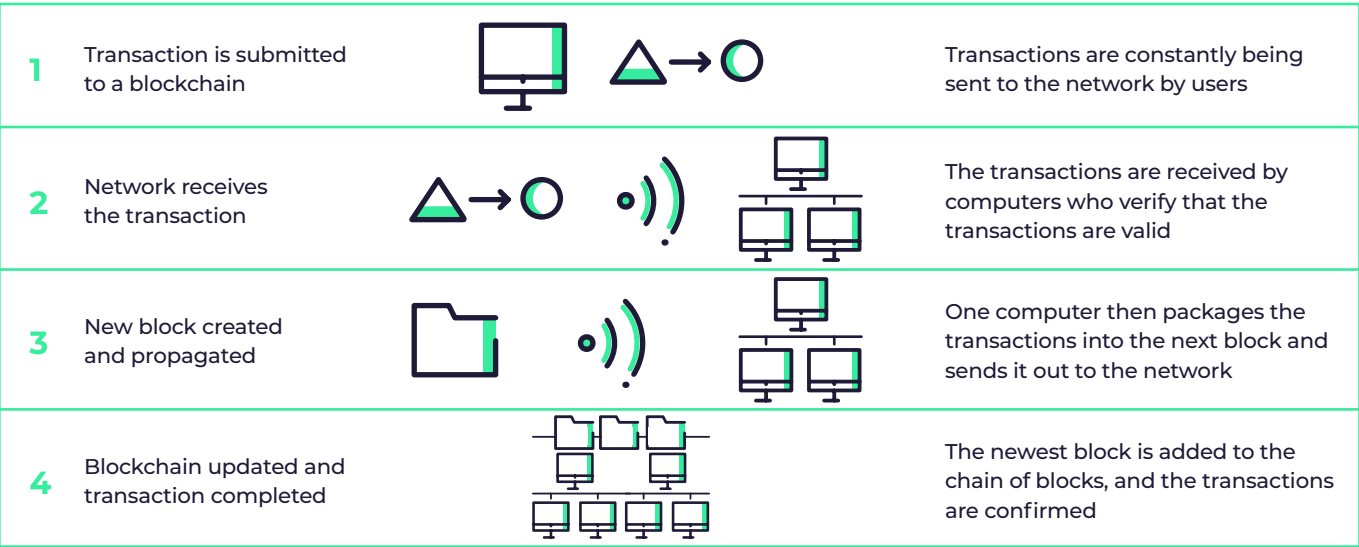


Figure 2 – Blockchain transaction process

The advent of blockchain presents an opportunity for aviation and ATM to rethink information systems and the manner in which a shared and trusted real-time distribution of ATM-related information can pave the way for short, medium and long-term efficiency and rationalisation with the possibility of far-reaching automation and transition to the digital era of ATM.

The goal is to address the issue of decentralisation of the different systems that will bring with it the distribution of data management responsibilities among multiple actors. There is a need to establish requirements that ensure that the data is correctly stored, and that the transmission of data is carried out in a secure and fully traceable manner.

Despite Blockchain being one of the most exciting technology trends over the last couple of years, it often failed to move past hype and struggled to present

tangible use cases that offered more benefits than centralised models. However, while governments and industries are still trying to understand the value of Blockchain, the market now appears to be moving toward actual successful implementations.¹¹

In Europe, the EU believes that when properly used, Blockchain technology can provide significant benefits to industry, the economy, and to society as a whole. For this reason, the European Commission is supporting Blockchain on the policy, legal and regulatory, and funding fronts. It is worth noting the developments of the initiative of the **European Commission “Blockchain Partnership”** (EBP) to cooperate in the establishment of a **European Blockchain Services Infrastructure** (EBSI) that will support the delivery of cross-border digital public services, with the highest standards of security and privacy.

Introduction

1.2 Blockchain Technology

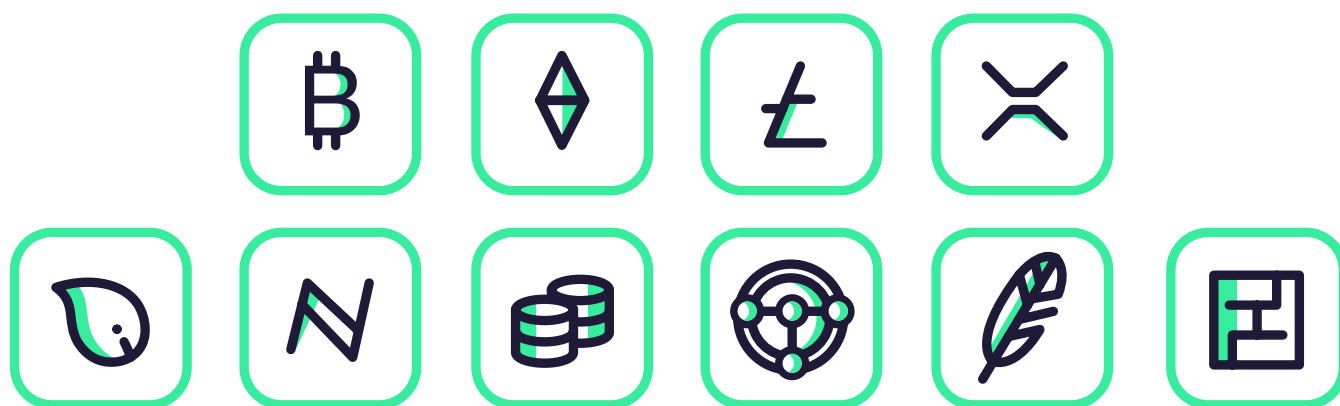
As is introduced above, Blockchain is fundamentally a “database” of transactions between peers. What is revolutionary about this approach is that it replaces a traditional, centralised authority which guarantees the execution of the transaction and maintenance of the integrity of the record, by an ecosystem of peers who engineer and maintain – by a set of rules that permit them to implement the same (decentralised) function with improved **security** and shared trust. This is why Blockchain is often referred to as a ‘trustless network’, since no human intervention is necessary to coordinate transactions.

The disruption is two-fold:

- the data written into the Blockchain becomes immutable, and
- the mechanism of the Blockchain does not require preordained or acquired trust between the participants, thus making it a truly decentralised, fundamental technology.

Blockchain is not a monolithic technology. It is an intricate composite of many cryptographic technologies, economic theories and digital concepts. Some of the key-concepts underlying the technology are the following:

- **Crypto Currencies:** Digital currencies were first introduced in the 1980s as a means to permit two parties to send and receive money directly and safely. However, these systems suffered from: i) centralisation – some sort of “banks” were still needed to control the authentication and issuance of the digital currency that could be digitally exchanged by the transactor; and ii) double-spending digital currency being just a series of numbers was easy to replicate and spend twice. The banks had to step in again as official ledgers guaranteeing one-unit one-spend. With the introduction of cryptographic signing which permitted to adopt the concept of “signing the cheque” to make the transactor uniquely accountable for the transaction, digital currencies had taken a step forward to cryptocurrencies. The extensive use of wide area network (WAN), of public and private clouds leads ANSP to put in place permanent cybersecurity risk assessment and appropriate tools to manage the vulnerabilities. Thus, a dedicated organisation with new systems to detect and handle miscellaneous cases of cyber-attacks has to be considered. At the same time, the virtual centres, based on **increasingly** more standardized interfaces, will benefit from new technologies and COTS (Commercial off-the-Shelf) products, subject to continuous cybersecurity vulnerability vigilance.



² Crypto currencies are just one of the many applications of Blockchain technology

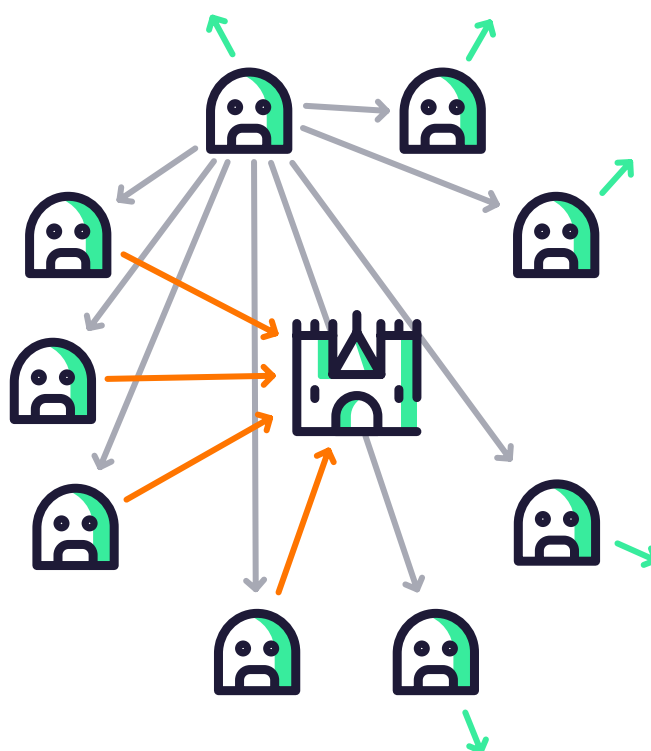
Introduction

1.2 Blockchain Technology (continued)

- **Double-Spending:** is a unique problem to the world of online transactions that allows a malicious actor to duplicate a transaction. Physical or fiat currencies do not have this problem, as they are difficult to reproduce in a short time, and the parties involved in a transaction can verify if they are defrauded with relative ease. Banks guarantee the uniqueness of the transactions by maintaining centralised ledgers. Blockchain communities aim to obviate this dependency for various reasons, the most important of which is to foster P2P interactions without the necessity to centralise trust in the peer. This translates into a need for a new technology that helps prevent double spending in such decentralised environments that are continuously growing in size (the Bitcoin network today spans the globe). This is made possible by the Distributed Ledger Technology.
- **The distributed ledger** is a transactional database which, spread across multiple devices on a P2P network, underpins the philosophy of Blockchain. The idea is, if we need a ledger to check various accounts, and ultimately verify if a cheque received is cashable, instead of asking a Bank, why can't the ledger be distributed to everyone? The information that is inserted into such a ledger is replicated and stored in each of the 'nodes' that actively participate in the network, and anyone with access to the chain (the internet in the case of Public Blockchains) can verify the information against their copy of the ledger. Distributing a ledger to everyone may have been impossible only 30 years ago, but is now possible with the advent of the internet.
- **The Byzantine-General problem:** The propagation of information in a network where **there is no trust** is a problem that was postulated in Microsoft labs in the 70's. In literature, it is popularly dubbed The Byzantine-General problem. The problem refers to the situation wherein only a concerted attack or retreat results in succession to a group of Byzantine generals laying siege to a rebel city, and the only

means at their disposal to execute an orchestrated attack is through a human messenger – a system that introduces multiple vulnerabilities in terms of corruption of the message being carried.

To tackle the Byzantine-General problem, the Blockchain adopts **consensus**.



- **Consensus:** Every transaction must be validated before it is inserted (registered) into the chain. This involves cryptographically linking the latest block of transactions to the previously existing chain (hence the name 'block-chain'). The process of verification, validation and registration of a transaction in this manner is the consensus mechanism whose principal aim is to protect the chain from the risk of having a distributed ledger that is altered by a party (or a group of parties) with malicious intent.

Introduction

1.2 Blockchain Technology (continued)

Many different consensus mechanisms have been conceptualised and implemented to overcome the shortcomings of their predecessors. The consensus scene is one that always incorporates a certain level of game theory in it and is one that is always evolving. All these mechanisms are aiming to resolve the consensus problems by using two levers:

- **Cryptographic protection:** The Bitcoin network contains information regarding all the transactions ever conducted on it since its origin in 2008. All information is cryptographically and chronologically linked, thus making it extremely complex to manipulate (manipulating one piece of information would involve the manipulation of all other information in the chain, implying computational power far exceeding what is currently at the disposal of even the biggest tech conglomerates).
- **Economic incentives:** Incentivising the nodes that maintain the Blockchain network and making it profitable for them to spend resources to adhere to the rules of the game rather than manipulate them. Many Blockchain networks reward the nodes involved in the consensus with the (crypto) currency inherent in the Blockchain (e.g., Bitcoin miners receive Bitcoins). If a node participating in the consensus of a network cheats the community, it puts at risk the rewards it has collected by alienating the user base (since none would subsequently use the currency to transact on a compromised Blockchain) and devaluing the spending power of the cryptocurrency in question. The reward mechanism is often referred to as **tokens**.

Consensus in Blockchain is essential for creating an efficient and secure ledger — just like obeying traffic lights is essential for creating an efficient and secure road. A primary goal of any consensus

approach is to facilitate communication between nodes, especially when it comes to quickly validating new transactions. Just as important is the ability to keep rulebreakers off the Blockchain, adding false blocks of information. The main consensus mechanisms (but not limited to) are the following:

- **Proof of Work:** Proof of Work (PoW) is a decentralised consensus mechanism that requires members of the network to solve an arbitrary (yet defined) mathematical puzzle to prevent anybody from gaming the system.

PoW is the original consensus algorithm in a blockchain network. The algorithm is used to confirm the transaction and create a new block to the chain. In this algorithm, nodes compete against each other to complete the transaction on the network. The process of competing against each other is called mining. As soon as miners successfully create a valid block, they get rewarded.
- **Proof of Stake³:** In a Proof of Stake (PoS) algorithm, a digital signature stands as proof of an ownership stake in the network. The network decides who will announce the consensus based on a lottery. PoS is a consensus algorithm that decides who validates next block, according to how many coins are held, instead of miners cracking cryptographic puzzles using computing power to verify transactions as seen with traditional PoW.

There is a constant competition to build upon or improve consensus protocols and this relates to various factors such as performance and domain. In general terms, POW is more secure and decentralised, while POS is more efficient “and environmentally friendly”. There is also a growing trend towards Proof of Reputation for crowdsourcing data (geo-location, Weather, Comp Resource utilisation) that goes beyond the scope of this paper.

³ This actually describes public proof of stake. Most enterprise blockchains manage consensus through distributed proof of stake or a proof of authority through which organisational nodes get permission to validate blocks. Choosing the consensus mechanism depends on who is participating in the network, whether it is open or closed, scalability requirements, the nature of the data that needs to be recorded, the energy required by the network, among other factors.

Introduction

1.2 Blockchain Technology (continued)

One of the significant evolutions in the world of public Blockchains has been the gradual shift from PoW to PoS and more recently, Pure PoS algorithms. Blockchain technologies based on PoW have some critical issues that may hinder enterprise adoption such as scalability, high transaction fees and energy usage.

In contrast, the latest generation of proof-of-stake solutions such as Pure Proof-of-Stake (PPoS) provides the necessary security, scalability, decentralisation and low transaction fees that make it attractive for enterprise use. The PPoS consensus model is permissionless and it creates full transparency, protection, and speed within a truly decentralised network. With blocks finalised in seconds, the transaction throughput being in line with the stringent requirements of large payment and financial networks.

Some of the main blockchain features are:

- **Smart contracts**, that are programs or collections of rules stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. Such smart contracts can be stateless or stateful, with stateless executing transactional approvals while stateful allows for the building of complex applications. They are flexible, low cost to execute and scalable.
- **Tokenised assets**, that provide a standardised, Layer-1 mechanism to represent any type of digital or physical asset on the Blockchain. These tokens can be fungible or non-fungible, and can be designed to represent utility, a commodity or a security.
- **Mining or Block validation**: Once the transaction is verified via consensus, it is written into a **block** – a set of validated transactions collected by the chain within a certain interval of time (this interval of time is proportional to the complexity of the consensus mechanism; in the case of the Bitcoin network it is 10 minutes). This block is then appended to the chain, creating the Blockchain, which is then replicated across all the participating nodes which result in the distributed ledger.
- The process of creating new blocks of validated transactions is defined as Mining (typically associated with POW) and this encompasses the execution of the consensus and the remuneration with the cryptocurrency for the miners, i.e., those running the consensus process and maintaining the Blockchain network. In the context of the Bitcoin Blockchain, mining is essentially the solving of a cryptographic puzzle related to the transaction (or in some protocols, a block of transactions) through trial-and-error. This is also a reason for having a block every 10 min: to allow time for the miners to solve the puzzle (which has been steadily increasing in complexity – a concept touched upon later).
- Any node can 'mine' on the Blockchain (democratic), and to do so, the nodes (computer hardware) consume energy – electricity. Upon successful mining, the node that succeeds in cracking the puzzle is rewarded (incentivised) – if the node is mining on the Bitcoin network, it is rewarded with Bitcoin. Metaphorically, Blockchain mining has been compared to working in a real mine, where miners invest money and time to dig out gold. This is one reason why Bitcoin is considered the new gold.

Introduction

1.3 Public vs. Private vs. Consortium

Different approaches on how stakeholders are aggregated into the Blockchain are as follows:

- **Public**

For public Blockchains, any stakeholder may access the information, submit transactions that would be effectively confirmed, and participate in the consensus procedures. Public Blockchains integrate economic incentives and encrypted verification through specific methods. The public Blockchain system is open and transparent and is viewed as a public, yet shared and trusted system. The identity of each node may remain anonymous, the anonymity and privacy of the nodes in the system are therefore protected. Regarding the above features, the public Blockchain is considered entirely decentralised. Bitcoin, Ethereum, and Litecoin (examples of cryptocurrencies) are adopting the public Blockchain system.

- **Private**

In this case, a block is managed by the specific stakeholder and the access permission is limited. The private Blockchain typically requires a trustworthy agent to reach the consensus and provides a better solution for organisations (enterprises) that intend to introduce Blockchain since it is managed by a trusted party and the (encrypted) database is shared among participants.

Blockchain Network Types

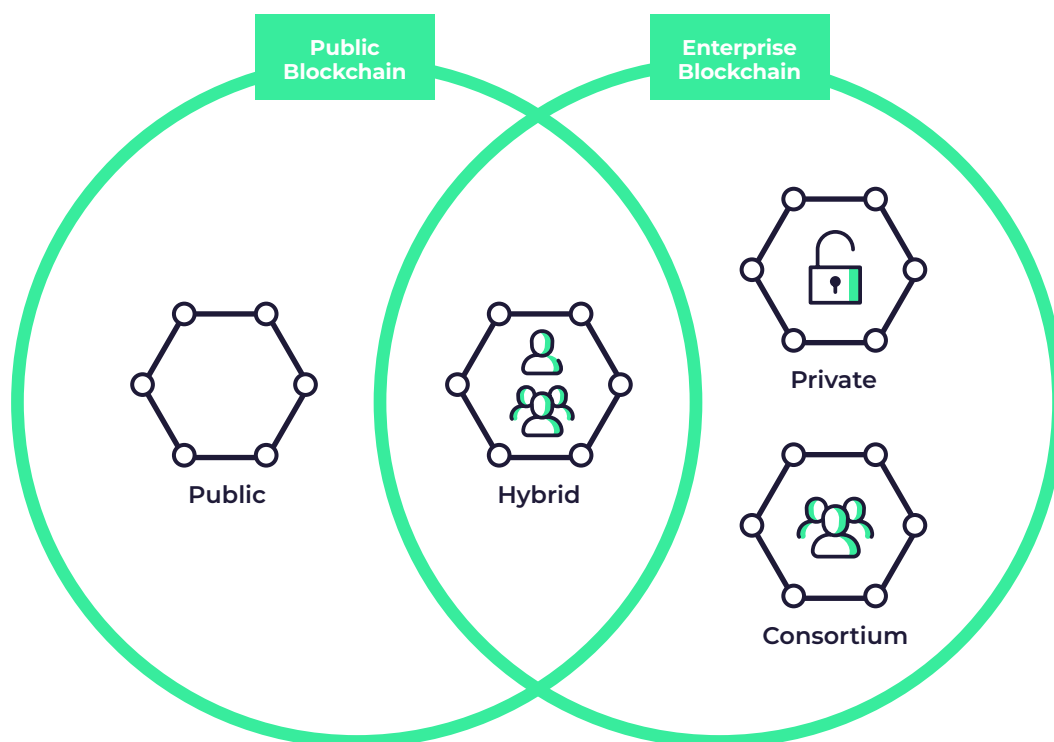


Figure 3 – Blockchain network types

Introduction

1.3 Public vs. Private vs. Consortium (continued)

Federated Blockchain or **consortium Blockchain** is a Blockchain governance structure typically used to manage the process of running a private, permissioned platform, where multiple organisations govern the platform.

In this case, consortium Blockchains help enterprises collaborate with each other. There is not a single authority over the network - all the companies can come together and work on the issues. They can contribute to the network and get credits and features equally. Consortium Blockchains are common in industry settings where multiple stakeholders can benefit from collaborating.

While private and access controlled Blockchains offer access control features, allow for faster transaction cycles, and have lower to nil Blockchain-related operational expenses, private Blockchains lose stride with regards to external trust towards end consumers (since, theoretically, a private Blockchain's immutability is questioned by the centralisation of authority) and cost for setting-up. However, given the limitations that public Blockchains are currently facing, access controlled Blockchains are currently favoured by the Enterprise World to service their needs. As a result of this, Ethereum, a major public Blockchain also offers enterprise (i.e. access controlled versions of its network).

1.4 Maturity Level of the Technology

Blockchains have great potential to build the next generation of the internet but are facing a number of technical challenges related to scalability, decentralisation, trust, security and interoperability.

- **Scalability** takes into account the throughput (also denoted by the number of transactions per second) and confirmation time. Throughput is the number of transactions per second, usually associated with the cost, that the system can sustain. Confirmation time, also known as latency, is the time elapsed between the submission of a transaction, and its definitive acceptance.

The throughput today, in the Bitcoin network, is affected by the 10-minutes (on average) required to mine each new block. This timeframe varies by the network: for instance, it is 15 seconds for the Ethereum network. Limited number of transactions are verified, registered and 'completed' at any given time compared to centralised solutions. Also, the limited number of transactions per unit time results in the cost of a transaction being driven upwards by competition among users, since they are left without choice but to pay more to have their transaction verified before the transactions of other users. Furthermore, the cost, which is paid in fractions of crypto to the miners (to compensate for their consumption of electric power to keep the network up and running) is volatile as it is linked to the market value of the crypto. The cost of the transaction and its volatility currently creates some obstacles to the enterprise adoption of a purely 'public' solution of the technology. Blockchain and blockchain-inspired technologies (such as the IOTA Tangle) are designed with scalability in mind, and often become more efficient with the increase in nodes and transactions.

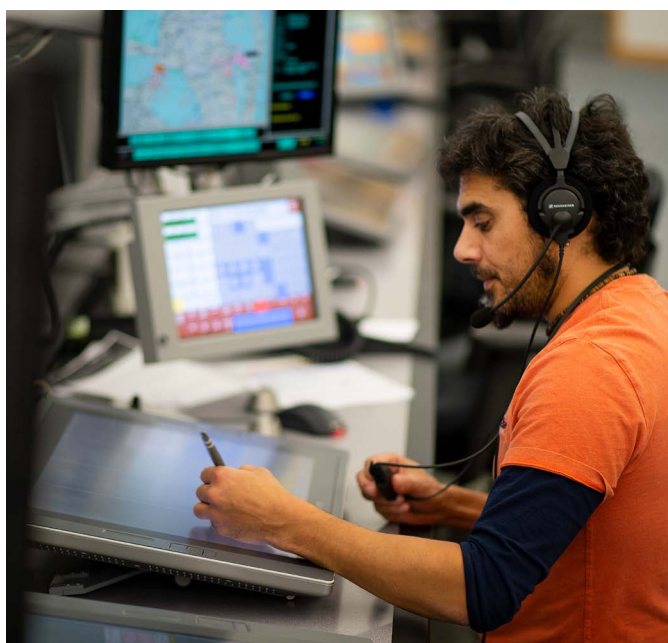
- **Decentralisation** so far has been dealt with in terms of disintermediation of incumbent processes (social and professional) and communal verification and approval of transactions. To a large extent, this philosophy central to Blockchain is also the ability of a Blockchain network (and its underlying consensus mechanism) to resist centralisation, i.e., the concentration of control in the hands of few who could manipulate the network.
- **Trust:** Blockchains have a decentralised architecture and governance structure, meaning there is no one entity that is solely responsible for the state of the ledger and can make changes. A predetermined set of rules dictate which transactions are valid, and how new information is added to the ledger. Because there is no one owner of the system, and all rules are pre-defined, there is a level of trust between unknown parties.

Introduction

1.4 Maturity Level of the Technology (continued)

- **Security** indicates the resistance of the consensus and the possibility to keep the Blockchain and the users' data private and transactions secure. The consensus needs to guarantee that (i) when an honest user has sufficient connectivity and tries to submit a transaction, it will eventually get accepted; (ii) Once nodes confirm a new entry to the transaction log, it will not be changed later; (iii) Once a transaction has been spent it cannot be double-spent and finally; (iv) there is a safety protocol in case of system failure.
- **Interoperability** is the ability of a Blockchain Technology to allow Cross-functional exchange of information with other systems outside of Blockchains (using oracles) and Cross-Chain exchange information with other Blockchains (using bridges). Imagine transactions flowing from Bitcoin Blockchain to Ethereum or vice versa, smart contracts in Ethereum that generate Bitcoin tokens, etc.

In order to tackle the scalability and decentralisation issues the following points are crucial to be addressed: (i) unloading the chain; or ii) evolving the consensus mechanism (maybe the most interesting one from a technical viewpoint).



1.5 Blockchain Initiatives

Blockchain technology was built to enable fast, disintermediated P2P interactions. The exchange of value between peers started out with a monetary flavour, but Blockchain lends itself to transferring value of many different varieties. Land deeds, digital rights, digital identity, asset tracking etc. are some of the popular value-exchanges currently enabled by Blockchain outside the financial space and have become mainly achievable through the use of smart contracts.

Similarly, in the Blockchain world, the definition of peers has evolved with enterprises entering the space. Today, Blockchain is being applied to both Business-to-Consumer (B2C) and Business-to-Business (B2B) exchanges. Start-ups are developing and deploying applications for consumer and commercial utilisation. Enterprises themselves are experimenting with Blockchain technology, developing applications on decentralised networks of both private and public natures. Governments and industries are on the way to implement the value of Blockchain for their respective entities and the market now recognises successful implementations of Blockchain (see Deloitte "Global Blockchain Survey 2020"¹³).

As introduced in the previous section, the decentralised nature of applications like Bitcoin and Ethereum as cryptocurrencies may not match up with business (e.g., dedicated business rules about privacy and asset traceability) and scalability requirements (i.e., number of transactions per unit time) for many industries. These types of requirements are **too** complex to be managed, at least at the start, for major enterprises. This trend, which some believe is temporary, has led to the recent development and popularisation of private permissioned Blockchains as well as consortium Blockchains.

While one of the primary uses of Blockchain is record keeping, Blockchain is much more than an enterprise database. While databases are suitable for recalling ad hoc queries of large volumes of structured and relational data that require complete privacy within a single organisation's parameters, Blockchain is designed to record specific transactions and events that are shared across a network of parties where transparency and collaboration is required.

Introduction

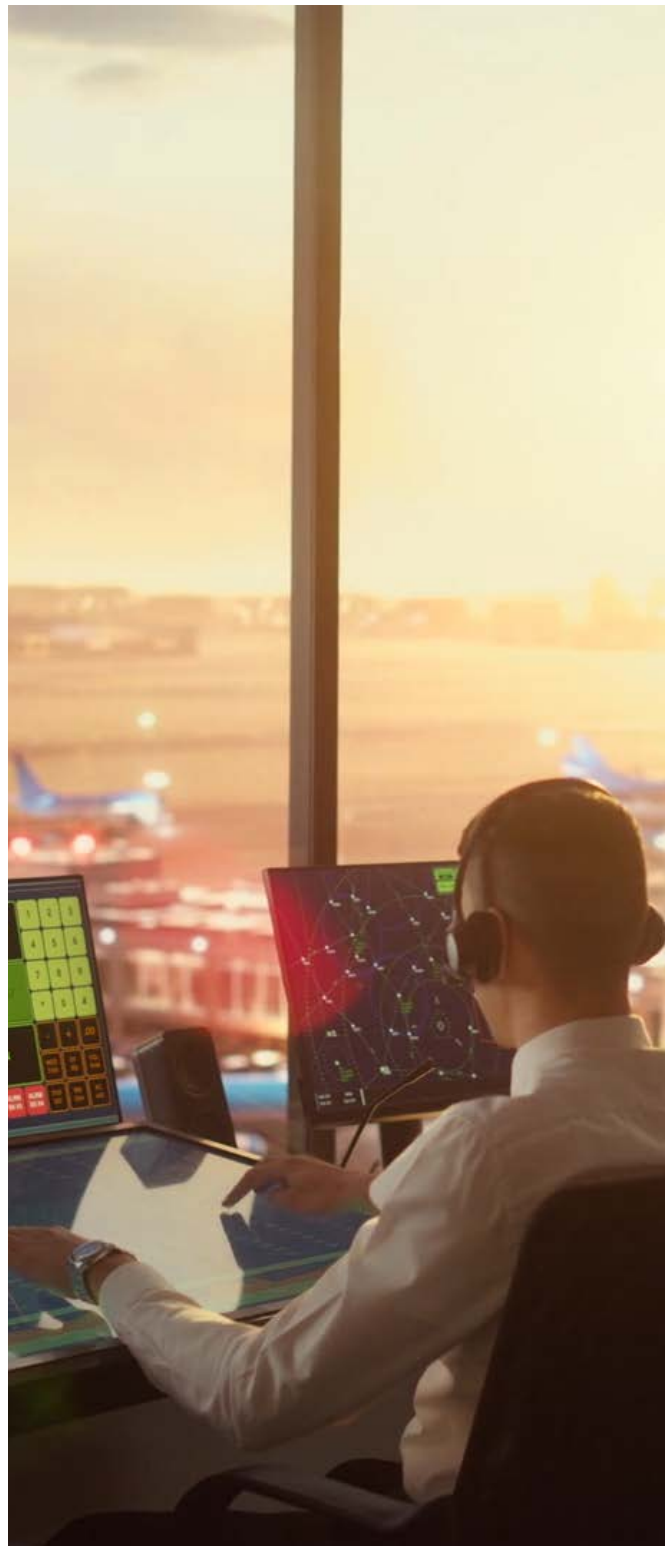
1.5 Blockchain Initiatives (continued)

In a supply chain, a private or permissioned Blockchain may be implemented, dictating users' ability to read and write to the Blockchain. The implementation of Blockchain technology can remediate the supply chain pain points including traceability, compliance, flexibility, and stakeholder management.

Now in its third year, Deloitte's "Global Blockchain Survey 2020" reveals a compelling evolution of Blockchain from an experimental, disruptive technology to a true strategic priority for organisations. Survey respondents indicated increased sentiment, investments, and more strategic talent sourcing and requirements for Blockchain initiatives. The survey also covered the role and evolution of digital assets.

Among the key survey findings:

- 39% of global respondents have already incorporated Blockchain into production. This is a significant increase from 23% of respondents signalling production last year.
- 55% of responding organisations view Blockchain as a top strategic priority, an increase from 53% in 2019 and 43% in 2018.
- Nearly 89% of those surveyed believe that digital assets will be "very" or "somewhat" important to their industries in the next three years.
- 82% percent of respondents said that they are hiring staff with Blockchain expertise or plan to do so within the next 12 months, compared to 73% last year.
- 83% percent of respondents indicated their companies will lose competitive advantage if they don't adopt Blockchain (versus 77% in 2019).
- 70% call the pace of regulatory change for Blockchain and digital asset solutions as "very" or "somewhat" fast.



Fields of Application

2.1 Overview of the domains

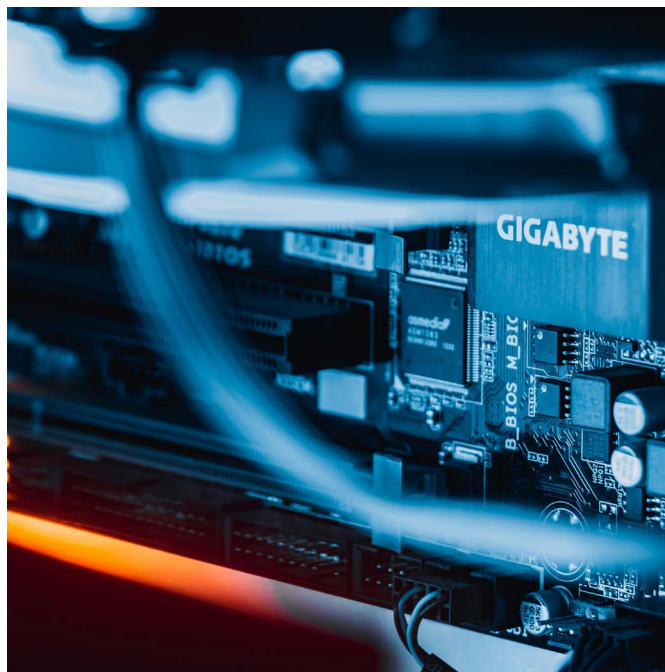
There are thousands of Blockchain-based application systems that have been recently developed to leverage the key features highlighted above. As a review of the key (general) domains that show robust and consolidated use cases for Blockchain applications, the following list highlights potential areas of application across banking and finance, business operations and government:

- **Payments:** Blockchain provides a way to securely and efficiently create a tamper-proof log of sensitive activity. This makes it excellent for payments and money transfers. Decentralised Finance (DeFi) is a growing space that offers users payment solutions (including decentralised exchanges, lending protocols and synthetic derivatives) without the constraints of the conventional banking system currently in place throughout the world. DeFi is expanding into the current banking arena for payment transactions to those who are currently unbanked or hindered by other market constraints.
- **Capital Markets:** Blockchain-based systems also have the potential to improve capital markets and offer solutions to capital markets, some of which include faster clearing and settlement, consolidated audit trail and operational improvements.
- **Trade Finance:** Historic methods of trade financing have been a major pain point for businesses because the slow processes often interrupt business and make liquidity hard to manage. Cross-border trade involves a large number of variables when communicating information – such as country of origin and product details – and transactions generate high volumes of documentation. Blockchain has the ability to streamline trade finance deals and simplify the process across borders. It enables enterprises to more easily transact with each other, beyond regional or geographic boundaries.
- **Insurance:** Arguably the greatest Blockchain application for insurance is through smart contracts. These contracts allow customers and insurers to manage claims in a transparent and secure manner. All contracts and claims can be recorded on the Blockchain and validated by the network, which would eliminate invalid claims, since the Blockchain would reject multiple claims on the same incident.
- **Supply Chain Management:** Blockchain's immutable ledger makes it well suited to tasks such as real-time tracking of goods as they move and change hands throughout the supply chain. Using a Blockchain opens up several options for companies transporting these goods. Entries on a Blockchain can be used to queue up events with a supply chain — allocating goods newly arrived at a port to different shipping containers, for example. Blockchain provides a new and dynamic means of organising, tracking data (adding provenance to it) and putting it to use.
- **Healthcare:** Health data that's suitable for Blockchain includes general information like age, gender, and potentially basic medical data like immunisation history or vital signs. COVID-19 has accelerated the development of blockchain-based healthcare passport applications. On its own, none of this information would be able to specifically identify any particular patient, which is what allows it to be stored on a shared Blockchain that could be accessed by numerous individuals without undue privacy concerns.
- **Real Estate:** The average homeowner sells his or her home every five to seven years, and the average person will move nearly 12 times during their lifetime. With such frequent movement, Blockchain could certainly be of use in the real estate market. It would expedite home sales by quickly verifying finances, reduce fraud thanks to its encryption, and offer transparency throughout the entire selling and purchasing process.

Fields of Application

2.1 Overview of the domains (continued)

- **Media:** Media companies have already started to adopt Blockchain technology to eliminate fraud, reduce costs, and protect Intellectual Property (IP) rights of content – like music records and art. According to MarketWatch, the global market for Blockchain in media and entertainment is estimated to reach \$1.54 billion by 2024. Non-fungible Tokens (NFT's) are currently being explored to enhance the ability to certify and designate ownership of digital property.
- **Energy:** Blockchain technology could be used to execute energy supply transactions, but also to further provide the basis for metering, billing, and clearing processes. Other potential applications include documenting ownership, asset management, origin guarantees, emission allowances, and renewable energy certificates. A reference in this field is the Energy Web Consortium that is building a customer-centric electricity system by enabling any energy asset owned by any customer to participate in any energy market. It develops and deploys open-source decentralised technologies—the Energy Web Decentralised Operating System (EW-DOS)—with a global community of more than 100 energy market participants. It is anchored by the Energy Web Chain, the first open-source, enterprise blockchain platform tailored to the energy sector.
- **Government Record Management:** National, state, and local governments are responsible for maintaining individuals' records such as birth and death dates, marital status, or property transfers. Yet managing this data can be difficult, and to this day some of these records only exist in paper form. Sometimes this necessitates citizens having to physically go to their local government offices to make changes, which is time-consuming, unnecessary, and frustrating. Blockchain technology could simplify this recordkeeping and make the data far more secure.
- **Identity Management:** Proponents of Blockchain technology for identity management claim that Blockchain-based self-sovereign identity platforms would allow people to upload, collect and own their verifiable credentials, and therefore only need to provide the bare minimum (e.g., that they are over 21 years old), to prove their identities when accessing a service (e.g. buying alcohol).
- **Voting:** Blockchain technology has the ability to make the voting process more easily accessible while improving security. Hackers would be no match to Blockchain technology, because even if someone were to access the terminal, they wouldn't be able to affect other nodes. Each vote would be attributed to one ID, and with the ability to create a fake ID being impossible. Governments could automatically tally votes and action outcomes more efficiently, using smart contracts.
- **Taxes:** Blockchain technology could make the cumbersome process of filing taxes, which is prone to human error, much more efficient with enough information stored on the Blockchain.



Fields of Application

2.2 Applications of Blockchain for the Aviation Industry

The aviation industry uses a complex system of interconnected resources, processes, and applications to deliver the safe and secure services. Airline passengers acquire a high-level perspective of the industry; from ticket purchase, check-in, security and immigration, to stepping off their flight at a new destination. From this perspective, the aviation industry seems relatively straightforward and simple, but underneath the surface lies a much more interwoven system-of-systems, comprised of both human and machine interactions. Often overlooked by the average passenger are various stages of checks and procedures that demand a consistent flow of information between typically siloed entities. These information flows and processes are often governed by rules, standards, and established procedures, which serve to ensure the safety, security, and timeliness of any service, such as any given flight positioning itself for takeoff.

Blockchain may enable these entities to efficiently congregate around a common set of governance protocols and eliminate the need for unnecessary intermediaries. For example, the purchase of tickets can be coordinated directly between the consumer and a dedicated Blockchain, without the need for intermediaries such as travel agents, which would significantly lower commission fees in ticket transactions. And, depending on the nature of the transaction protocols built into the Blockchain, the purchase itself could be initiated with any type of accepted fiat currency, digital asset, digital token (such as frequent flyer points), or any other offering deemed acceptable by the Blockchain itself. This payment system would often result in fast settlement of the transaction. Additionally, passengers could securely and directly transfer tickets to other travelers with airlines being able to retain a degree of control of these tickets throughout their lifecycles, by defining the smart contract rules that facilitate these exchanges.

There are many other areas in which Blockchain can provide vast improvements to the aviation industry. In addition to the ticketing and payments infrastructure

described above, the process could be taken a step further by offering a higher-level of assurance that the consumer is, in fact, who they claim to be through cryptographic authentication and verification. Similar types of verification can be applied to aviation personnel who are initially vetted and onboarded during the Registry process. Record-keeping on the Blockchain could serve as a means of ensuring identities remain vetted, protected, and authorised to operate, and could remove the need to re-vet these personnel in the future. Such digital identity initiatives have been accelerated because of the coronavirus pandemic, as we now often need to verify identities, remotely. Specific to the aviation sector, digital healthcare passports will be key to reestablishing confidence in global travel. Such passports allow officials to verify passengers' coronavirus test results or vaccination certificates, while passengers remain in control of their securely stored personal data. By enhancing the trust and efficiency in validating passenger identities - by verifying biometric data, documentation, vaccination certifications, test results and tickets on a Blockchain - passengers could pass through immigration, check-in and boarding with a single QR code or biometric screening, making their journey more seamless and enjoyable.

To add to the customer experience, certain airlines have started using Blockchain technology to distribute tokenised frequent flyer points and smart contracts to automate the reconciliation process - thus streamlining the collection, spending, and accounting of these points - with the ultimate aim of retaining passenger loyalty. Additionally, sustainability pressures have led to a rise in carbon offsetting schemes, the innovation of cleaner fuel and aircraft technologies, and the demand for airlines to be more transparent about their environmental impacts. From allocating tokenised carbon credits, enabling passengers to track how their carbon offsetting contributions are applied, to providing visibility over sustainable and circular practices in supply chains, Blockchain can be used to supplement each of these industry trends.

Fields of Application

2.2 Applications of Blockchain for the Aviation Industry (continued)

Several use concepts have already been applied to various supply chains within different industries. It is both practical and feasible for aviation to leverage these novel capabilities in providing an adequate solution to tracking aircraft authenticity, aircraft lifecycles, aircraft leasing, aircraft parts, and maintenance activities. This would ensure that genuine parts are being used, that the parts from which an aircraft is built can be quickly identified and traced back to the originating manufacturer, and that aircraft are being maintained to high standards. Maintaining a single source of truth and digital audit trail is a significant time and cost saver for stakeholders such as commercial airlines and federal defence agencies that are currently overwhelmed with often paper-based and error-prone data regarding what can be hundreds of aircrafts in their fleet. Similarly, passenger luggage, and essential pieces of cargo can be automatically captured and revealed on the Blockchain, along with their corresponding locations, so that items can be quickly and easily located.

The needs of the aviation community are continuously evolving; the framework that comprises the aviation landscape remains fairly static, despite major leaps in technological advancements. It is inevitable that outdated technologies used today will need to be replaced with modern era capabilities. Meanwhile, new entrant platforms, such as drones, are necessitating the need for innovative solutions to safely and securely operate in existing airspace environments all over the world. This new era is an excellent opportunity to start incorporating innovations such as Blockchain technology. Over time, as Blockchain demonstrates utility, proficiency and gains public trust, the entire airspace infrastructure can further leverage its benefits.

2.3 Applications of Blockchain for ATM and UTM

Digital transformation in ATM will be key to ATM modernisation. New information technologies are expected to change the way the next generation of ATM systems are conceived, designed and implemented. Reduction of time-to-market and costs is no longer negotiable.

For decades, the ATM industry has defined its business strategy mainly with respect to local constraints: cooperation with stakeholders outside the national borders has been kept at an informal subsidiary level, while industries have concentrated on local investments to improve their individual performances.

The lack of a vision focusing on the overall benefits of a fully connected, networked, high-tech eco-system (that for example drove other business domains to be revolutionised in the last ten years) has therefore meant a high fragmentation of the airspace, inevitably leading to a scarce integration and organisation among the actors of the air transport value chain, which resulted in poor delivery of functionality/reliability and poor cost efficiency.

The objective of enhancing the overall ATM capacity, whilst reducing environmental footprint is critical given the traffic growth forecast. ATM configuration is being reviewed with the recognition that the system must be recognised as a cohesive eco-system in which service orientation should play a fundamental role.

Service orientation has an ultimately essential requirement, the information upon which we all trust.

There is a growing realisation that a new generation ATM infrastructure is necessary and cannot be postponed.

The expected increase in aviation capacity demands, economic pressure and attention to the environmental impact are relying even more on accurate and timely information. Such information must be organised and provided through flexible means that support interoperability and secured seamless information access and exchange.

Fields of Application

2.3 Applications of Blockchain for ATM and UTM (continued)

Clearly, system interoperability in aviation/ATM can only be achieved at the service level, through deployment of a Service Oriented Architecture which, in turn, gives all organisations the opportunity to change their local system or maintain what they already have; though, what to relate to will be known through this project by all aviation organisations (a “common denominator”).

Many ANSPs continue to have a fragmented cross-border communications infrastructure relying on bilateral (legacy) connections. For such reasons, the number of services actually exchanged across networks are still very limited, while cross-border operations still rely on bilateral agreements, bespoke dedicated connections between legacy systems, message-based protocols such as OLDI and, in many cases, voice communication over phone or faxes. The same situation is often reflected in between adjacent ACCs within the same national borders. Additionally, the interconnection with non-ANSP stakeholders’ remains complicated and based on ad-hoc setups.

System Wide Information Management (SWIM) and System Interoperability with Air/Ground (A/G) data sharing is therefore crucial to the future of ATM. Building on the best practices from different information communities, the aim of SWIM is to provide information to users with relevant and commonly understandable information. This information should be of the right quality, provided at the right time and delivered to the right place in a secured way, so enabling the concept of net-centric ATM operations.

Automation, artificial intelligence, and sensor technologies have continued to rapidly progress over the past few decades, particularly in the aviation domain. Unmanned Aircraft Systems (UAS), Drones (also referred to as small UAS, or sUAS), Urban Air Mobility (UAM) platforms, and Commercial Space Vehicles (CSV’s) have all demanded access to the established airspace environments. These new platforms require unique solutions, since their operations and distinct operating capabilities don’t easily integrate with the rigid and tightly controlled architecture designed for conventional manned aircraft operations today. Fortunately, these ‘smart’ systems could leverage Blockchain in a manner that provides a more efficient and streamlined approach for exchanging information and adhering to established protocols, without the need for extensive human interaction as found in the manned aviation construct. For example, Blockchain-based identity management could be vital to ensuring the authenticity of UAS and commercial space vehicles. Similarly, concepts involving the Internet of Things (IoT), Device-to-Device Communications (air-to-air & air-to-ground), and standardised policies and procedures can be merged with Blockchain to create interactive environments that cater to the modern-era needs on a decentralised, trustless, secure, distributed ledger system that is both immutable and accessible for historical retrieval and analytics.

Blockchain could therefore be used to create an immutable and shared record of information for the purpose of air traffic management between ANSPs. Like the internet, Blockchains are distributed and ‘always-on’ because they remove single points of failures, like a centralised database.

Fields of Application

2.4 How to choose your Blockchain

The following flowchart provides a general rule-of-thumb to determine if blockchain is a practical solution based on the applied use-cases, and offers a suggested type of blockchain that may be most suitable. It is important to note that this flowchart conveys decisions from a high-level perspective, and additional considerations and concerns may come into play for different scenarios. To gain a general sense of when a blockchain may be beneficial, and the type of blockchain that would most appropriately suffice for the mission need, refer to the flowchart below:

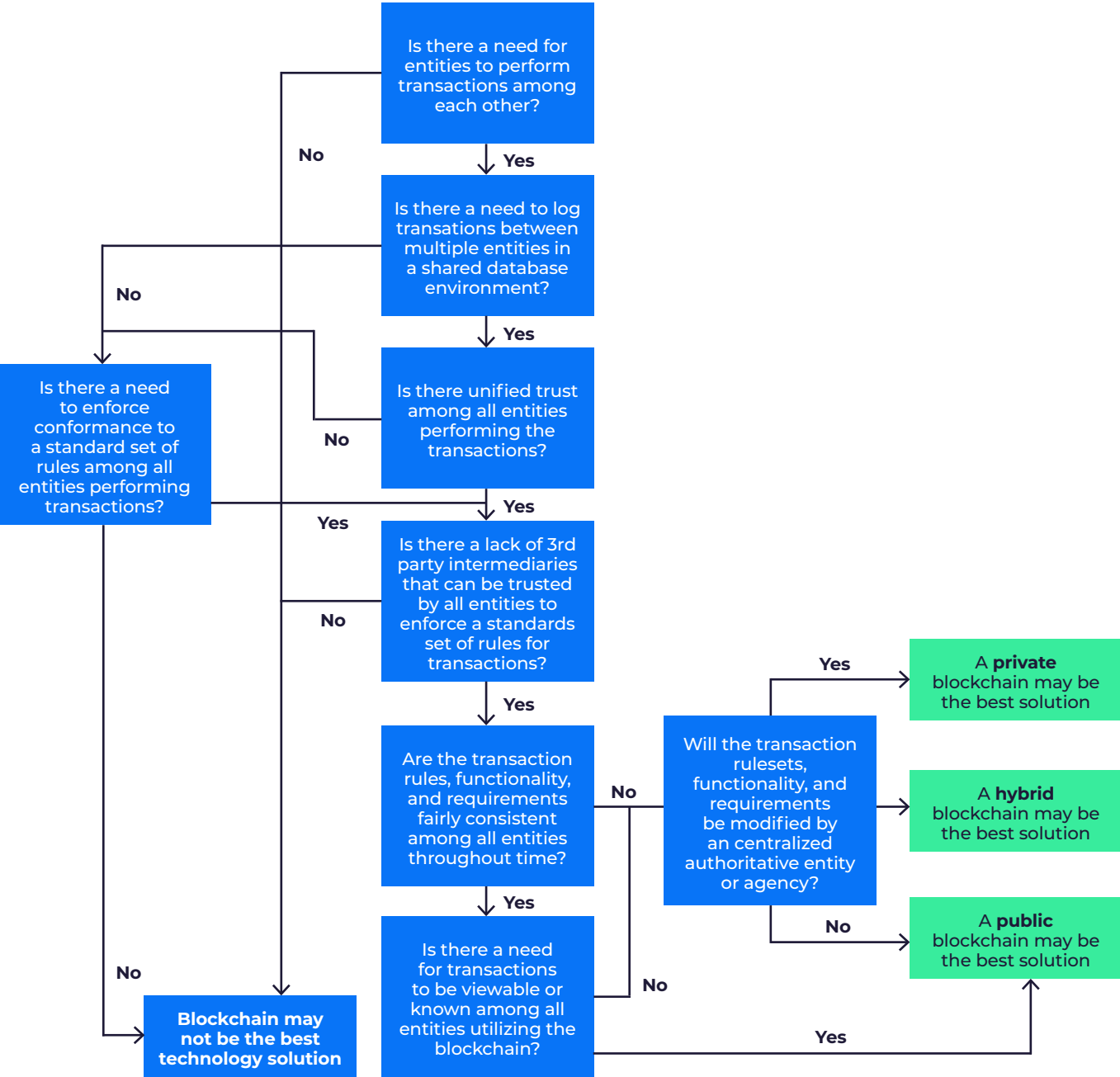


Figure 4 – Determining a Blockchain Solution

Identity Management, Authentication and Privacy

A secure ATM infrastructure involves the ability to accurately identify the key users and service providers who interact within this complex ecosystem. This becomes especially important as digital messages are sent to/from participants, and international operations increasingly take flight around the globe.

In many areas around the world, technologies like the Automatic Dependent Surveillance Broadcast (ADS-B) tend to be useful applications for aircraft identity management, but there remain concerns in the form of authentication, privacy, anonymity, and susceptibility to attacks, particularly with the most advanced form of ADS-B. In the United States, ADS-B has been largely adopted in response to a 2020 mandate to provide a more comprehensive airspace picture of the operating environment. Although verification and validation techniques are applied to both the position reporting and authenticating of the reporting source (specifically for ADS-B), additional security concerns remain. Ronald J. Reisman of NASA Ames Research Center proposes a more secure manner to address ADS-B vulnerabilities using Blockchain and more specifically the public key infrastructure (PKI) on which Blockchain is founded.⁹

The National Institute of Standards and Technology (NIST) also provides a deep dive in this pioneering area of exploring Blockchain utilisation for identification management in its cybersecurity white paper titled, “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems”. (Note: the NIST report indicates a potential use case for Blockchain identification for autonomous vehicles but remains agnostic to the field of aviation as a whole.) The crux of the NIST report explains how Blockchain could provide a leap forward in identify management, authentication, privacy and the exchange of data through secondary layer protocols and smart contracts. In the world of aviation, this not only allows for a safer and more trusted operating environment but allows for the securing of entity identifications and disseminates or conceals information as necessary among aviation stakeholders. The

expansion of airspace users, particularly in the areas of UAS, commercial space vehicles, and other new entrant platforms increases the necessity of a secure, tamper-resistant identity management capability.

3.1 Benefits

To better maintain a safe and secure airspace, it's essential that all participants operating within ATM, UTM, and other developing airspace environments are identifiable by authorities. Blockchain could help provide the foundation for this identification solution. In doing so, it could provide a means for certain entities to remain privately identifiable to specific users, whereas other activities and users may be openly identified to each other and the general public. In a similar manner, air traffic services and data suppliers may also need to be identifiable to help ensure the integrity of the information and services in which they provide. Using public and private keys, Blockchain fundamentally ensures secure authentication and identification, which could also be leveraged to provide substantial benefits, such as smart contract services and other second-layer protocols.

3.2 Impact

Implementing a Blockchain-based system could help to ensure all airspace users and data suppliers are properly identified and authenticated. The Blockchain protocol would eliminate the need for third-party intermediaries to provide these independent checks of validating identification and authenticity. As a result, authorities could monitor, store and analyse airspace users with a high amount of confidence, and grant airspace users' access to a range of additional information and services. It is anticipated that these Blockchain protocols would eventually evolve to become universally standardised and adopted across international borders.

Identity Management, Authentication and Privacy

3.3 Challenges

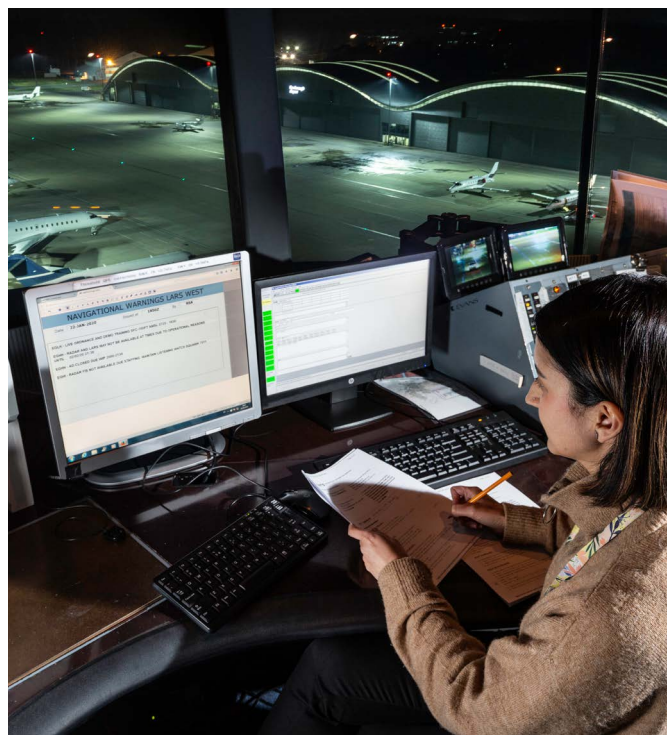
A fundamental challenge for leveraging Blockchain for identity management, authentication, and privacy is the development of a standard set of protocols that is accepted and adhered to by the broadest group of airspace users. Blockchain would likely require a phased-implementation approach to not only garner trust, but also eliminate unintended anomalies within the Blockchain protocols and applications.

Similarly, there are regulatory challenges that cast a shadow on the Blockchain landscape within the realms of identity management, regarding varying data governance and international Blockchain laws. Given the nature of air travel, to bring most value, the technology would typically need to be deployed on a multiparty, cross-border architecture, spanning a number of regulatory regimes. Consequently, governments that already have established regulations pertaining to Blockchain technology will likely encounter varying legislations between them. As many governments still work towards creating legislation on the topic of Blockchain, there is an opportunity for management, regulators, standard-setters, and professional service providers to work together in forging common guidance and establishment of best practices that will lead to the alignment of international Blockchain laws.

Lastly, there is also the small matter of opposing interests and existing contracts in place. Many stakeholders may be bound to using their existing systems, thus preventing them from shifting to a Blockchain based identity management system. This barrier, however, will likely erode with time, as the benefits of such systems are further demonstrated amongst the technologies early adopters.

3.4 Maturity Level

Identity management is key to enabling a new model of systems-of-systems aviation data sharing, which is efficient, scalable and trustworthy. This safe, secure, distributed ledger platform for aviation data exchange between various vehicles operating in a non-segregated airspace will enable high volumes of data exchange. For example, when autonomous airborne vehicles such as drones and air taxis share the sky with conventional aircrafts, the ability to instantaneously share their identities, location and trajectory data with other vehicles will be paramount. Fly2Plan is a current example of how Blockchain is being explored to facilitate aircraft identity management.



Fleet Management, Maintenance and Supply Chain

Supply chain and logistics, like in most industries, are key components of the aviation industry. Given the safety-critical nature of the industry, being certain of the course and quality of the components and materials used in the construction of an aircraft is critical. For companies that manufacture, operate and service aircrafts (e.g., Airbus, Boeing), being able to trace the original source, locate, and monitor the performance of each component in an aircraft is essential. This, however, is a challenging task as the maintenance, repair and operations (MRO) value chain involves numerous stakeholders: manufacturers, component resellers, airlines, service providers, and regulatory authorities, who typically maintain incomplete and inconsistent duplications of this data in disconnected databases or even on paper, leading to costly errors despite the copious manhours spent in trying to coordinate this siloed data management.

Until now, efficiently maintaining aircrafts and their parts requires almost impossible coordination efforts. Prior to the coronavirus pandemic, 25 billion parts were processed, and 3 billion new parts were added annually, while 20,000 suppliers covered 144,000 daily flights.¹⁵ Currently there is no industry-wide system in place, centralised or otherwise, that creates a digital representation of each aircraft component in an end-to-end audit trail. Due to these companies being competitors, and lacking interoperable supply chain systems, there is also a reluctance and inability to efficiently share data on each component. Consequently, having a digitised solution for each component of an aircraft that provides the aircraft's complete configuration and maintenance history could help reduce costs and losses related to downtime and unplanned maintenance, while also maintaining the value of planes as they are sold and leased amongst airlines throughout their lifecycles. Blockchain could be a viable solution to solving this problem, and in doing so, improve the safety and efficiency of the aviation industry through effectively applying Blockchain management to the aircraft manufacturing and maintenance supply chain.

In such instance, the manufacturer stakeholder would register every manufactured component and spare part to the Blockchain. This would ideally include all transaction data (i.e., source, timestamp, etc.), current and future maintenance and repair history, aircraft components configuration, and spare parts provenance. It could also include other inputs like technician identifies and credentials. In addition to using Blockchain to trace components, attaching IoT sensors to the items being traced reaps extra benefits by automatically collecting value-added metadata to provide greater visibility and accuracy of items across the complex ecosystem. For example, sensors could collect information on the condition of items such as temperatures, pressure and sustained impact on items as they are transported and used. This provides transparency on whether aircraft components and cargo are maintained to certain quality standards.

4.1 Benefits

As described above, a complete and transparent digital audit trail of an aircraft's lifecycle; including ownership, configuration, and maintenance history for each sub-component would be revolutionary. It would enable stakeholders to be certain of the origin, quality, and authenticity of the components and materials used in the construction; and subsequently trace, locate, and monitor the performance of each component.

It is anticipated that certain aircrafts parts, especially those with lifecycle limitations, would need to be tracked more than others. By having a Blockchain-based system in place, manufacturers could trace the specific aircrafts in which their parts are being used and subsequently contact the aircraft owner in case a part needs to be recalled, inspected, or replaced. This improved efficiency of the MRO value chain saves time and costs related to downtime and unplanned maintenance, while ensuring that aircrafts are maintained to a high standard. This ultimately helps retain aircrafts' value, as they are sold and leased between airlines throughout their lifecycles.

Fleet Management, Maintenance and Supply Chain

4.1 Benefits (continued)

There could be numerous potential safety benefits for aircraft manufacturers, airlines, MRO services providers, and regulators as well. The transparency of the aircraft manufacturing ledger could help regulatory authorities assign airworthiness scores for each aircraft and maintain a more accurate market value of the aircraft. This also aligns with general improvement in safety, which is the number one concern for ANSPs, as maintenance, repair, and overhaul (MRO) service providers would see a highly accurate digital representation of the aircraft, which inevitably helps identify and respond to component issues in a timely manner. This could also potentially help tracking and tracing of fraudulent and adversarial components, which is a major concern for government customers.

4.2 Impact

One of the challenges for supply chains is removing legacy, and often manual procedures for tracing and storing supply chain data. Using smart contracts, Blockchains can help automate maintenance schedules and remove manual data entry procedures and intermediaries such as brokers who audit and value aircrafts. As mentioned in “Data for the Life of the Aircraft”, having a more comprehensive and accurate picture of an aircraft’s configuration and maintenance history could help reduce costs and improve safety measures. It’s estimated that the impact in, “efficiency gains enabled by Blockchain could increase industry revenue by as much as 4%, or US\$40bn”.¹⁶ Using Blockchain to track aircraft components could save the industry \$3.5 billion - derived from secure document storage, ensuring confidentiality and data privacy, improved insights on repair time and inventory, automated workflows and more efficient record reconciliation.¹⁵

4.3 Challenges

Traceability is one of the key challenges for all supply chains. Often the issue is providing stakeholders financial and operational incentives for investing in the necessary technology, like Blockchain, to improve tracking and tracing. Blockchain is a network-based technology where there is a need for the majority of market participants to join, in order for significant benefits to be realised. A concern for the MRO Blockchain systems would be that a critical mass is not reached, and that the system fails. A recognised solution for this hurdle, stemming from the technology adoption lifecycle theory, is for industry disruptors to start working with a small number of stakeholders and enable value realisation between them. Once adoption gains momentum amongst early adopters, it is expected that larger company executives would commit to reap the benefits of such platforms.

Another similar contributing factor to the supply chain challenge is that manufacturing modern aircrafts involves millions of components, which are supplied by hundreds of different companies of varying sizes around the world. While Blockchain can address many of the technology challenges for supply chain traceability, it does not address the business and governance models needed to agree on what information to store on the Blockchain. This includes agreeing on issues like access rights, data formats, and minimum viable data requirements. It also includes a more difficult problem for international governance models where the varying regulatory frameworks and politics for the countries of business will play in role in how smart contracts are constructed.

Blockchain variance in cross-border data governance and international Blockchain laws create further complications across global supply chains. Given the nature of air travel, to bring most value, the technology would typically need to be deployed on a multiparty, cross-border architecture, spanning countries and their respective regulatory regimes.

Fleet Management, Maintenance and Supply Chain

4.3 Challenges (continued)

Consequently, governments that already have regulations on Blockchain technology in place, may have differing legislations between them. Geographic variability within a Blockchain architecture creates complexities, specifically surrounding the differences in legal frameworks.

Furthermore, the nature of these private or consortium Blockchains leads to a rise in concerns about having to cooperate with competitor airlines, for example. Four areas of concern that business leaders need to address before joining or starting a consortium: 1) decision-making authority, 2) funding and revenue sharing, 3) legal structures and risk, and 4) identification and ownership of intellectual property. Many consortia that begin with good intentions to help its members succeed in their Blockchain-related endeavors often fail because of internal infighting and perceived inequities over issues related to the amount of expenditures and effort that individual members commit; the amount of profit that members receive; and legal considerations that may benefit some members over others. According to Deloitte's "Global Blockchain Survey 2020"¹³, participants' primary challenges to joining consortia were as follows: 'Inability to create fair and balanced governance rules' (41%); 'Inadequate or poorly defined roles and responsibilities of member' (41%); 'Members of consortium as cross purposes' (39%).

The aforementioned survey represents a subset of the non-technical challenges that supply chain initiatives are running into for Blockchain adoption, but as mentioned above these are often bigger hurdles than the technical problems of Blockchain technology. Some of the technical challenges include scalability, computing resources, interoperability, protocol choice, and legacy systems. While some of these issues cause more difficulty than others, depending on the use case, most of them can be mitigated by choosing the proper consensus algorithm to address slow transaction speeds, utilising on-chain solutions or off-chain approaches for storage issues, or choosing the right type of Blockchain, as introduced in Section 1, to address the speed of transactions.

4.4 Maturity Level

This particular use case of Blockchain is arguably the most widely practiced to date out of all the applications of the technology within the air travel industry. In 2017, Lufthansa Industry Solutions launched the Blockchain for Aviation (BC4A) initiative with the aim of enhancing transparency and traceability within aircraft maintenance. Participating members included software developers, aircraft manufacturers, MRO service providers, logistics providers, lessors, and regulators. By registering the serial numbers of installed components in conjunction with the aircrafts being maintained, technicians can trace this information in the event of a malfunction and decide whether to replace or repair the respective component. Additionally, documentation can be seamlessly stored across a distributed yet permissioned network of relevant aviation industry participants, from manufacturers to airlines to service providers, enabling the end-to-end lifecycle of any component to be visible. This is especially beneficial when providing verifiable documentation for any installed component.¹⁸

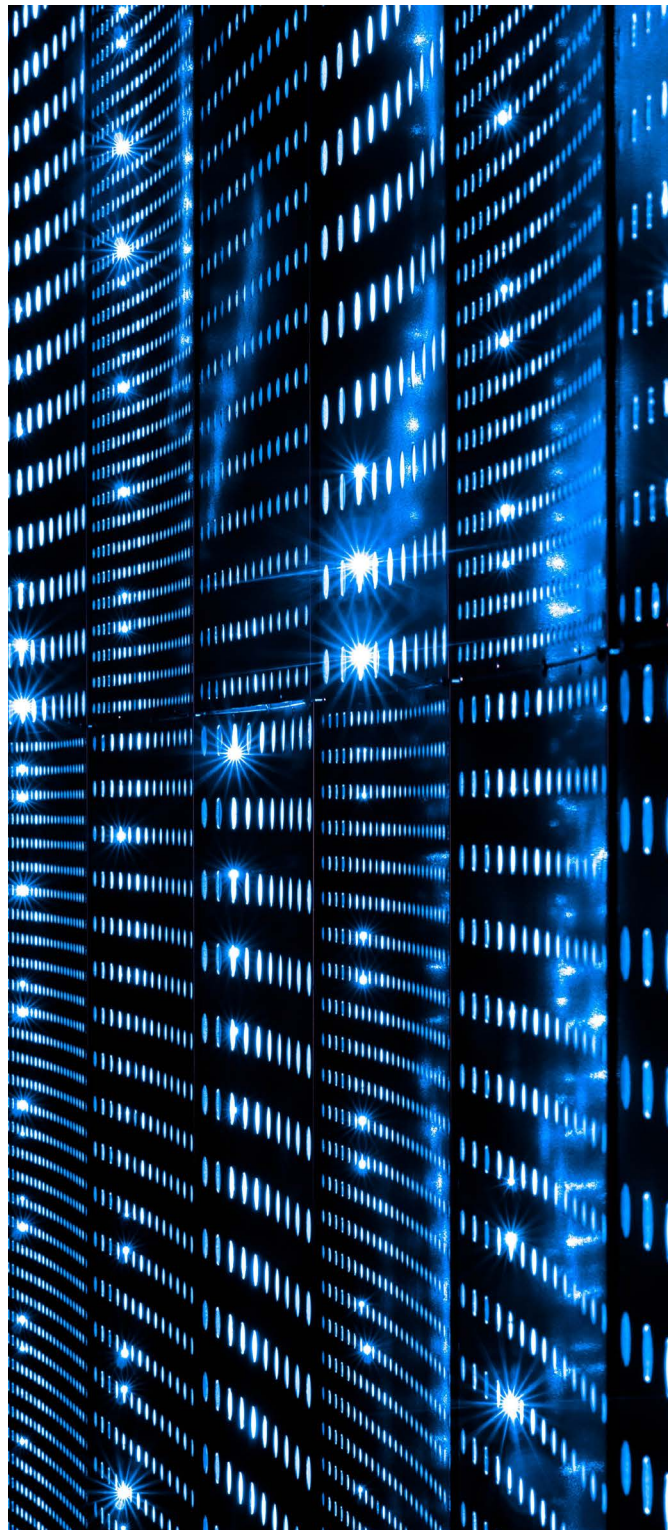
Likewise, as part of SITA's Global Blockchain Alliance, the MRO Blockchain Alliance was launched in February 2020 to explore and standardise the use of Blockchain to track, trace and record aircraft parts. Alliance members include Bolloré Logistics, Cathay Pacific, FLYdocs, HAECO Group, Ramco Systems, SITA, and Willis Lease Finance Corporation. A proof of concept is currently being built to track the chain of custody, maintenance history and quality standards of parts; across airlines, lessors, original equipment manufacturers, logistics suppliers, and maintenance providers. SITA plays the role of the regulating/rule making body in this consortium and is responsible for ensuring that the Blockchain technology components used are compliant with industry standards and are validated with regulators and international standardisation bodies.

Fleet Management, Maintenance and Supply Chain

4.4 Maturity Level (continued)

Similarly, Aerochain, secures aircraft value through maintenance recording and verification and unlocks value in illiquid and disconnected aviation assets and data from aircraft to contracts to human resources to manufacturers. Aerochain is an example of a protocol layer that can be built over, empowering key industry stakeholders to build their own applications on top of Aerochain's protocol without having to worry about the core technology, or privacy, security and cleanliness (and therefore interoperability) of their data. This lowers barriers of entry for this use case to gain industry traction.¹⁴

Lastly, given the efforts to reduce the environmental impact of the airline industry, airlines and aircraft manufacturers could additionally use the transparent and traceable nature of the technology to highlight their efforts to embed circular economic practices as well as sustainably source the necessary raw materials required to build aircraft components. Circular is a Blockchain company currently exploring this niche Blockchain space.

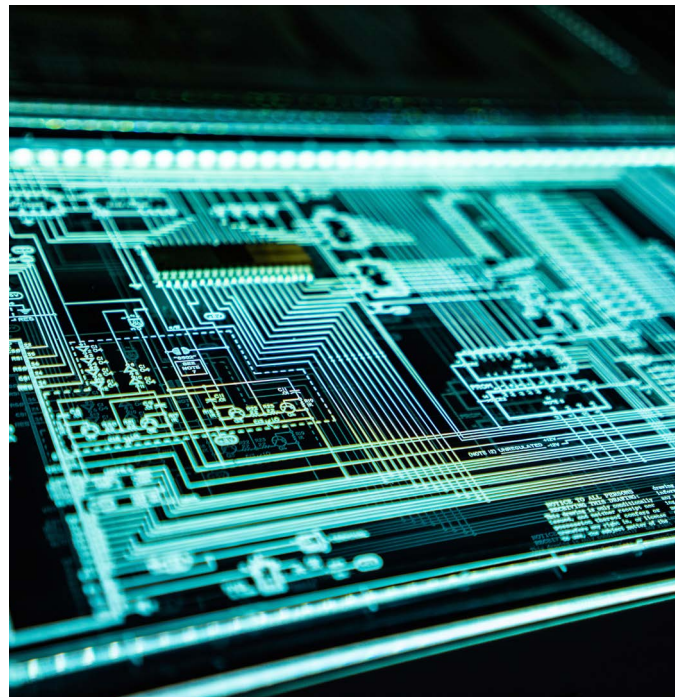


Airspace Management and Flight Planning

The importance of real-time, accurate, and accessible flight object data has been discussed since the early 2000's. Described as “a collection of common information elements describing an individual flight and available electronically for use by both the National Airspace System (NAS) users and the Air Traffic Management (ATM) service providers”, flight-object is an essential concept to many future ATM applications. One such concept, trajectory-based operation (TBO), relies heavily on the functionality of flight object because for TBO to be fully enabled it relies on current and accurate information. As such it is one of the cornerstones of global and European initiatives, such as ICAO's Global Air Traffic Management Concept, NextGen and SESAR.³⁴ Yet despite its obvious importance, flight object has never been implemented on an international level.

The primary objective of flight object is to enable interoperability between ATM systems. Historically these systems are often “monolithic” and developed uniquely to fit the requirements of a respective country's ATM system. This means ATS messages sent by an international flight will need to communicate with multiple ANSPs and will be dependent on the constraints of each ANSP's legacy system capability, which can often mean the information is transferred by voice or requires human interpretation. While work is being done to improve international flight information sharing, like Flight and Flow-Information for a Collaborative Environment (FF-ICE), they still don't address the problem of how this data will be shared among different systems. There are also concerns that as the data becomes more dynamic and complex for concepts like TBO, these systems will not be able to handle the interactions, even with new concepts like FF-ICE.

Part of the reason this flight object problem has not been resolved is the international component. It would seem that a centralised database housing all the flight object data would be a viable solution. However, it requires a central entity that controls and operates the database. Such an entity would need the technical capability to run an operational system critical to the efficient operation of international aviation. It would need a source of funding, and it would need to be trusted and accepted globally by ANSPs and airspace users. This is not to say a centralised database solution is impossible. However, a more likely solution, which would allow for ANSPs, airspace users, and other international aviation stakeholders to have control over their own flight object instance could be to utilise Blockchain technology.



Airspace Management and Flight Planning

5.1 Benefits

As introduced above, with a Blockchain-based solution, the international flight information sharing would be achieved by storing the set of flight objects on a distributed ledger. The Blockchain would assure airspace users accessing the data that the ledger is complete and accurate, leading to improved operational efficiency and support for dispute resolution. The Blockchain would also remove the need for a centralised authority and would not require each of the participating stakeholders to trust one another. In addition, securely storing real-time flight data on a distributed network increases the accessibility and availability of the data. Lastly, the scalability of these new models of systems for aviation data will enable copious volumes of data exchange that today's ATM systems are unable to deal with, thus enabling the future scenarios of unmanned aircrafts roaming the sky.

By streamlining the ground operations and departures aspects of air traffic management - enabled by capturing real-time data and tracking tasks against detailed flight checklists, Blockchain can help airlines coordinate the activities of all the crew members and service providers that are essential for timely departures.

Further benefits are unleashed when the technology is deployed in conjunction with other cutting-edge technologies. For example, the combination of AI, distributed ledgers and smart contracts will ensure that operational decisions made by humans or machines will be safe, logical and transparent. This will allow autonomy to be integrated into systems in the future, as pulling data from a common network can avoid issues of conflicting or missing data. Users and programmers will trust a rigorous governance

process where traceability, training and competence records extend into the autonomy software as well as the licensed human operators.

Modernising the data exchange ecosystem that has stood for over three quarters of a century is possible with Blockchain. It is a technology that can finally allow traditional aviation operators to exploit the internet and benefit from better resilience and lower costs – costs that can ultimately be passed on as savings for passengers and consumers, as well as welcoming new pioneers to the sky.

5.2 Impact

A Blockchain-based flight object capability could potentially change how ANSPs share flight information. In a report titled, "Flight Object Sharing Capability Using Blockchain"²², the authors provide both a concept and a prototype that illustrate a Blockchain-based solution can resolve many of the issues plaguing flight information sharing today. Unlike some of the other aviation Blockchain concepts described in this paper, this idea has proven it is not only possible to provide a complete flight object solution using Blockchain technology, but that their solution offers additional benefits like strong integrity guarantees and role-based update permissions enforcement.

To provide a scale of the economic impact of such initiatives, it is expected that the implementation of Fly2Plan, would add up to \$42 billion to the UK economy by 2030. Additionally, such an infrastructure for data exchange would disrupt the global airport IT market, worth \$50 billion per year, by preventing 60% of delays due to a more resilient IT infrastructure.¹²

Airspace Management and Flight Planning

5.3 Challenges

Similar to any international problem, getting buy-in and agreement from every participating party is difficult and often results in Blockchain initiatives not moving beyond the pilot phase. In the flight object example, the challenge would be getting a Blockchain based solution through the ICAO standards process. Another challenge would be getting countries, like those in Europe, and the respective companies working on solutions, like iTec and CoFlight, to abandon their current flight object solutions after years of working on a solution. Due to the lack of suppliers, many of these countries have spent millions of dollars on these projects and it would be difficult to imagine them completely retiring these solutions for a Blockchain-based solution.

As described above, there are contrasting regulations around Blockchain technology and data governance across geographies. Given the nature of air travel, this poses a barrier to deploying a distributed record of air traffic management data across a network of participants that may reside across the globe. Consequently, governments that do already have regulations on Blockchain technology in place, may have varying legislations between them. For example, in countries where cryptocurrencies remain illegal, there is skepticism over how multiparty, cross-border Blockchain configurations will affect their control over business and government data. This reemphasises that private and permissioned Blockchains, in which governance decisions and system changes are easier to deploy, are likely to lead the way for enterprise adoption. Furthermore, as many governments still work towards creating legislation on the topic of Blockchain, there is an opportunity for management, regulators, standard-setters, and professional service providers to work together in forging common guidance and establishment of best practices that will lead to the alignment of international Blockchain laws.

5.4 Maturity Level

SITA's FlightChain protocol enables airlines, airports, air traffic control and airport ecosystem partners to achieve consensus, by providing a single source of truth on flight data on a distributed network that includes these stakeholders. This solves the flight information sharing problem where multiple copies of subsets of flight status data may exist which are not easily accessible by all stakeholders when required. SITA has demonstrated the solution benefits with IAG, Heathrow Airport, Geneva Airport, Miami Airport, Beijing Capital Airport, Shanghai Airport, Air China, and China Eastern.

Similarly, TEKTower's Fly2Plan initiative, which is using SITA's FlightChain protocol to scale its operations, is developing a decentralised communication infrastructure, working alongside Heathrow, NATS, IAG and other consortium partners. This initiative is enabling a new model of systems-of-systems for aviation data, which is efficient, scalable, and trustworthy. This safe, secure, distributed ledger platform for aviation data exchange between various vehicles operating in a non-segregated airspace; will enable copious volumes of data exchange that today's ATM systems are unable to cope with. For example, when autonomous airborne vehicles such as drones and air taxis share the sky with conventional aircrafts, the ability to instantaneously share location and trajectory data with other vehicles will be paramount. In addition, the project will demonstrate system-wide analytics and process automation through smart contracts.¹²

Integration of UAS and other New Entrants

The integration of Unmanned Aircraft Systems (UAS) and other new entrants into the airspace provide a great opportunity to leverage cutting-edge technologies like Blockchain into a newly conceptualised airspace ecosystem. Not only do new entrant devices have the potential to be “smarter” than conventional aircrafts, by leveraging cutting-edge technologies more rapidly, but the envisioned support infrastructure to manage these flights are intended to be highly automated, federated, and interoperable; yet collectively adhering to a distinct set of rules. The foundation of the support infrastructure is built on a network of interconnected UAS Service Suppliers, which rely heavily on the dissemination of information among a wide variety of networked entities. Much of the data exchange involves state information relevant to both the aircraft and airspace environments in which these aircraft transit.

6.1 Benefits

In response to an ICAO request regarding the safe integration of UTM and the ATM system, Air Market drafted a detailed report titled, “A Decentralised Solution for Integrating Large-Scale UAS Operations in Future Aviation System”.³⁴ This report constructively summarises many of the benefits that Blockchain can provide in the proposed UTM construct. The security and encryption capability of Blockchain can enhance the integrity of UAS Registration, Identification, and Remote Tracking. The inherent functionality of Blockchain protocols can enable the P2P communications and data exchange in a secure, authenticated, and cohesive manner. Similarly, the supporting UTM infrastructure can leverage Blockchain in a manner that designates and communicates when various segments of airspace are accessible, and to whom. Over the long-term, UTM service suppliers and supplemental data providers could benefit from Blockchain, by providing services and products over the Blockchain in exchange for instant payment settlements.

6.2 Impact

The emergence of highly automated technologies, such as drones, new entrants, and the supporting infrastructure, go hand-in-hand with the innovative functionality that Blockchain provides. By leveraging Blockchain early-on in the development process of the UTM framework, stakeholders can reap many benefits of a safe and secure operating environment. Early implementation would allow both Blockchain and drone technologies to evolve cohesively and resolve any inevitable, yet unintended, anomalies while the consequential risk to life and concept reputation is relatively low. As benefits are realised and Blockchain functionality becomes more trusted and reliable, Blockchain concepts can merge directly into the manned airspace environments, where risk is inherently greater.

6.3 Challenges

One of the biggest challenges of integrating Blockchain into the UTM and new entrant domain space is overcoming the lack of understanding by decision makers. Blockchain has little history and demonstrated capability in this specific field, rendering any benefits derived from the functionality questionable, at best. Additionally, it is well understood, that with any novel technology, there will be unintended consequences and unforeseen malfunctions that arise. In a historically risk-averse domain foundational to the world of aviation, applying new and rather complicated functionality such as Blockchain can introduce substantial amounts of risk (whether substantial or perceived), simply due to unfamiliarity with the underlying technology.

Integration of UAS and other New Entrants

6.4 Maturity Level

Both industry and government agencies around the world are adamantly exploring the innovative technology of Blockchain to gain insight into the benefits that can be introduced into the world of air traffic management. The feasibility of Blockchain in its current form remains uncertain, but the rapid pace of Blockchain innovation is promising. Several of the examples discussed above pose innovative use cases that can lead to a breakthrough paradigm shift, resulting in a complete alteration of the existing airspace construct as we know it today.

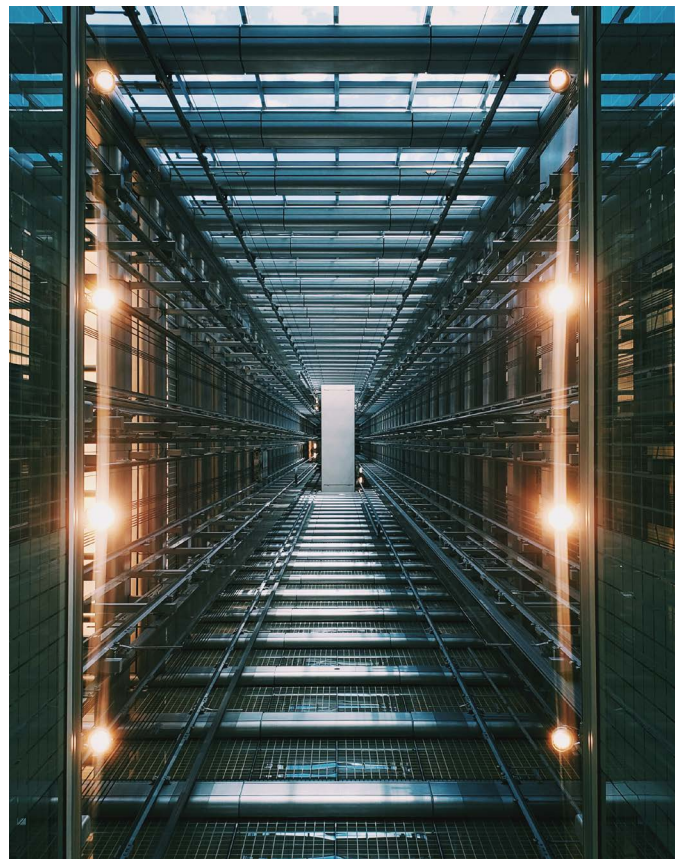
To exploit new opportunities in this domain space, several Blockchain companies around the globe are advancing concepts on how to best leverage Blockchain technologies in a manner that solves several UTM challenges in an efficient and effective manner.

In many cases, companies have partnered with large industry partners, like Boeing, to develop effective solutions in airspace management for drones and new entrants. For example, SkyGrid, founded in 2018, is the result of Boeing teaming up with SparkCognition, a Blockchain and Artificial Intelligence company, to produce a platform geared towards airspace awareness, flight operations, and fleet management capabilities. They intend to use Blockchain as a means of providing audit trails and powering the common operating picture of the flight environment to its many users.²⁸

Other examples include Distributed Sky and Skyy Network, who are both developing Blockchain solutions to build the foundation for a safe and secure traffic management system for new entrant aircrafts, particularly in the UTM environments. This becomes especially important where information sharing is critical in a more autonomous environment.²⁹ Distributed Sky advocates that Blockchain is ideal for executing smart contracts between autonomous entities, such as the drones themselves or interactively with the service providers, on an as-needed basis. Whereas Skyy Network is focused on leveraging

the cryptography benefits of the Blockchain for ensuring time-stamped and immutable information is exchanged between properly authenticated entities. Furthermore, Red Cat and GoChain have partnered up to build a scalable Blockchain solution that enables the capturing, dissemination, storage, and analytics of UAS flight traffic data, in a manner that offers transparency and a high amount of integrity.³³ Non-aviation startups, such as FOAM and Helium, are looking to enable the storage of environmental information, such as terrain and location data that can be captured on the Blockchain and disseminated to other users within the network.

Over the course of the UTM exploratory phase, there have been numerous proposals for utilising Blockchain to help advance and secure the functionality that the UTM solution may bring to the aviation domain.



Registration and Recordation of Airmen and Passenger Identities

The coronavirus pandemic has led to an increase in the need for remote and digital identification and verification of individuals, with direct implications for the aviation industry with regards to consumer digital identity services (such as healthcare and travel passports), as well as to the onboarding and vetting of aviation personnel. As a result of the pandemic, travel bodies have requested internationally recognised and mutually agreed standards for a pre-flight testing regime to prove that passengers are vaccinated or have produced negative COVID-19 test results. For customers of airlines such as Lufthansa, Qatar Airways and Singapore Airlines - digital healthcare passports have already become a pre-boarding requirement for certain routes. These mobile app-based passports have quickly gained traction across the industry to safely restore the public's confidence in the connectivity of air travel, as they enable travelers to match their travel itineraries and validate that they comply with their destination's coronavirus health requirements.

Similar to health passports, the concept of digital travel passports also falls in the wider realm of decentralised digital identities, which confirm through cryptographic authentication and verification of one's credentials, that a traveler is in fact who they claim to be, while subsequently improving process efficiencies. By verifying biometric data, travel documentation, flight tickets and additional user attributes through decentralised identifiers (DIDs) on a Blockchain network; passengers could pass through immigration, check-in and boarding by scanning a single QR code or a biometric feature to prove who they are and their eligibility to travel. This would significantly reduce airport queues by automating and removing human error of an otherwise manual document verification and data entry process.

Similar types of verification can be applied to the process of employing aviation personnel (e.g., flight crew, air traffic controllers and airport employees) who are initially vetted and onboarded during the registry process. Record-keeping on the Blockchain could serve as a means of ensuring that identities remain vetted, protected, and authorised to operate; and could remove the need to re-vet these employees in the future.

7.1 Benefits

On a basic level, the use of digital identities from the start of the flight booking process, enhances accuracy of passenger data collection into the Advanced Passenger Information (API) system – which collects passenger data before they board to reinforce information required at country borders. Currently, approximately half of all passengers make errors when submitting their information to airlines before their flights, often requiring manual data corrections at the airport by airline staff. Furthermore, a \$0.50 fine is applied to the airline for each case of incorrect API data. Digital identities would therefore lead to reduced fines from incorrect data input, real-time confirmation of validated passenger information based on their identity attributes, reduced airport waiting time and a frictionless passenger experience by removing multiple identity verification check points in the current passenger airport experience.

The foundation of digital health passports and digital identities revolves around the concept of Self-sovereign identity (SSI), in which individuals are in complete ownership of their identities and encompassing data, as well as in control over how their data is used and shared. This helps minimise the personally identifiable information that airlines need to hold on their customers, thus reducing the impact of potential data breaches. In the context of sensitive biometric, healthcare data and personal information - there is an even greater necessity for individuals to be able to consent to sharing specific pieces of their data with airlines and border controls, and only share the minimum amount of personal information required (often in an anonymous or pseudonymous manner) to board a flight. The shift to decentralised identity makes it more difficult for companies to manipulate sensitive user data for monetary and marketing purposes. Instead, by being put in control of their own data, users will start being compensated when they allow for their data to be used for such purposes.

Registration and Recordation or Airmen and Passenger Identities

7.1 Benefits (continued)

As the technology can guarantee trust between entities that may not necessarily trust each other, stakeholders such as governments do not have to worry about whether they trust the information coming from a certain country or not. Government officials and airlines can request, verify, and trust data relating to passengers – in a way that respects individual privacy while keeping data secure. They can subsequently be confident that passenger COVID-19 tests and vaccine certifications are valid, that they meet the local destination's requirements and that passengers are in fact who they claim to be; while passengers can be confident that the testing or vaccination certificate assigned to their digital identity, as well as additional travel credentials, are accurate and sufficient for their destination country. Blockchain based digital health passports would also prevent anyone from being able to fake vaccination certification or test result documentation, which is commonly seen with equivalent paper-based health passport such as the World Health Organisation's Yellow Card booklet for yellow fever vaccinations.

For aviation personnel and their employers, digital identity improves the onboarding experience, reduces the time taken for pre-employment checks, increases onboarding efficiency and reduces fraud and cost. These savings come from optimised right-to-work checks, sharing of verifiable professional qualifications, and using verified identity attributes for background checks. There are subsequent productivity gains from not needing to make any trips to provide physical documentation for in-person identity verification. Lastly, as a result of reduced onboarding time, aviation personnel can be deployed faster to meet industry demands.

7.2 Impact

As mentioned above the digitisation of identities will facilitate the move towards contactless and seamless travel. This is increasingly important given forecasted growth rates. It therefore paramount that governments, airports and airlines use innovations

in digital identity to automatically establish trust in passengers' identities, to subsequently be able to rapidly and safely process passengers in places where space and resources are limited. Employees of the global travel industry currently spend the equivalent of 10,000 years annually on processing and verifying identities.⁷ According to the World Economic Forum, digital identity solutions that enable documentation-free travel, could save up to \$150 billion in the global aviation industry while "creating up to \$305 billion worth of value for the industry through increased profitability."⁸ Similarly, according to analysis by Deloitte, the adoption of digital identity can bring annual economic benefits of £214.2m through the automated identity verification; and up £95m through reduced data breaches and a reduction in the time that is lost in transit. To reap these benefits, digital identity must be reimaged collaboratively by all parties in the air travel ecosystem.

7.3 Challenges

Despite the recent accelerations in the field of digital identity in the aviation sector, spearheaded by demand led innovation in digital health passports; the concept of a global digital identity needs to gain further acceptance from the general public, who understandably have concerns about the safety and unauthorised dissemination of their valuable, personal data, as well as skepticism about Blockchain technology itself. It is therefore imperative that end users can trust and have confidence in the digital identity systems of the future and understand the benefits of moving from the centralised and federated identity landscapes to the decentralised digital identity landscape.

Recent policy frameworks led by government, such as the 'UK Digital Identity and Attributes Trust Framework' and the 'Pan-Canadian Trust Framework'; and governance schemes led by industry bodies, such as World Wide Web Consortium (W3C), the OpenID Foundation, and the COVID-19 Credentials Initiative

Registration and Recordation or Airmen and Passenger Identities

7.3 Challenges (continued)

(CCI) will be catalyst in creating interoperable standards as well as an understanding between those using digital identity services (e.g. passengers), the organisations relying on the services (e.g. airlines, authorities and laboratories), the identity service providers (e.g. technology providers creating identity wallets), attribute service providers (e.g. third party organisations and governmental agencies), and orchestration service providers (e.g. distributed ledger technology providers that make sure data can be securely shared between the aforementioned parties). Such frameworks will mold the guidelines which illustrate what 'good' digital identities look like, enabling businesses to innovate whilst being aligned to frameworks, and allowing customers to be confident that the products and services being accessed will safeguard their personal data. It is important that international governmental bodies work hand-in-hand in developing these frameworks, to ensure that standards are interoperable between organisations, stakeholders in the aviation sector and schemes across the globe - so that digital identities can be used internationally, seamlessly. For example, by building open-source standards such as W3C's verifiable credentials, services can be extended beyond health credentials to any identity credential, enabling passengers to securely share any digital travel documents across the travel experience.

Additionally, due to the immutable nature of data stored on a Blockchain, there needs to be clarity on how well such digital identity initiatives adhere to data governance and privacy regulations such as GDPR. For example, the GDPR states that businesses must disclose the duration of data retention, the country where the processing occurs; and that international companies that collect or process EU citizens' personal data, are subject to the same requirements and penalties as companies in the EU. Because requesting or retaining healthcare, biometric, personal and professional data has GDPR implications, it is desirable that such records are held by the passenger or employee in personal wallets and shared via explicit consent when necessary, which is

the case with SSI (which instead of storing sensitive information on the ledger, stores the corresponding verifiable decentralised identifiers (DIDs) representing these credentials).

7.4 Maturity Level

The COVID-19 pandemic has spurred multiple initiatives to develop digital travel and vaccine passports. IATA's Travel Pass is using blockchain in a digital health application that allows labs to securely send test results and vaccination certificates to passengers' digital wallets. For airlines and officials it allows secure verification of test results, certificates and respective passenger identities.⁶ The app boasts additional functionalities in which passengers can choose what data to share and with whom, without being forced to do so, and for passengers to check the vaccination and/ or testing requirements at their travel destination. Besides using decentralised ledger technology to put passengers in control of their data, Travel Pass also minimises the risk of data theft as a result of decentralised data storage. Lastly, the application is designed modularly, to enable interoperability with other digital solutions that are being trialed.³⁵

The Sovrin Foundation and AOKPass have also built Blockchain-based digital passports, giving passengers control of who to share their data with, which data to share, and how it is used; while American Airlines and British Airways have also built their own 'Verify Health Passport'.⁶ Similarly, IBM's Digital Health Pass and Zaka's NewNorm, enable the issuance of verifiable health credentials, while prioritising the privacy of user data.^{10,11} Lastly, Zamna is a blockchain-powered SSI verification platform, focusing more on improving airport security whilst providing a seamless passenger experience. It achieves this by providing the infrastructure to verify, manage, and control accurate identity data which allows the automation of airport security checks by enabling officials and airlines to be able to trust passenger data.⁴¹

Tokenisation of the Aviation Ecosystem

Tokenisation refers to the representation of digital or real-world objects or assets. Blockchain provides the technology needed to facilitate exchange, ownership and trust of these tokens amongst participants of the network. In the aviation ecosystem tokens can be used to represent flight tickets, frequent flyer points, carbon credits, as well as to track aircrafts and aircraft parts as described in Section 4.

There are multiple intermediaries and stakeholders that are currently involved in the ticket purchasing process. These include Global Distribution Systems (GDSs), travel agents, airlines and online ticketing companies; between whom booking data and a web of revenues must be distributed. Today, IATA acts as an intermediating payment clearinghouse between relevant stakeholders and sets industry standards. Airlines have thus become dependent on third parties that control much of the industry's decision-making power and charge high commissions for their services. Today, the top three GDSs dominate 99 percent of the market for indirect ticket sales, while travel agents still register the majority of airline bookings. Enabling the purchase of flight tickets on a Blockchain network would disintermediate such third parties, therefore lowering commission fees and increasing revenues among network members, leading to the reallocation industry value. In addition, representing a ticket as a Blockchain based token, would enable the traceability of ownership of a ticket. For example, as currently seen in the application of Blockchain ticketing for events, travelers could securely and directly resell/transfer tickets to other travelers, between whom trust may not typically exist, by using smart contracts. These smart contracts' rules can be defined by the airlines selling the ticket in order to prevent customers from creating a black market and/or profiting from reselling tickets. Such passenger-to-passenger systems would also eliminate the risk of ticket overbooking and eliminate the typically manual methods of ticket reissuances, while increasing accuracy and efficiency in the process.

Most airlines have loyalty and rewards programs that enable customers to collect frequent flyer points which can be redeemed to make discounted purchases with airlines or limited affiliated partners. However, because of the use of segmented systems amongst different loyalty scheme providers, consumers are often unable to use rewards across different airlines and associated retail merchants, limiting cross-marketing potential as well as revenue opportunities for the businesses involved. As Blockchain technology can enable different providers to establish trust in the collection and sharing of a digital asset via tokens, it can be used to facilitate loyalty schemes between multiple stakeholders. In addition, reconciling these points is often an error-prone and time-consuming process, so 'tokenising' points and using smart contracts to automate the reconciliation process can streamline the collection, spending and accounting of points, leading to greater overall customer satisfaction.

Continuing on the notion of customer satisfaction, passengers are becoming increasingly environmentally conscious thus pushing airlines and industry bodies to become more sustainable. This has led to a rise in carbon offsetting schemes, the innovation of cleaner fuel and aircraft technologies, and the demand for airlines to be more transparent about their environmental impacts. From allocating tokenised carbon credits, enabling passengers to track how their carbon offsetting contributions are applied, to providing visibility over sustainable and circular practices in supply chains; Blockchain can be used to supplement each of these industry trends.

Tokenisation of the Aviation Ecosystem

8.1 Benefits

In a competitive cost-cutting environment with low margins, keeping passengers loyal is increasingly difficult as benefits are reduced and customers flock to the cheapest fare. Blockchain technology can improve the efficiency of rewards programs, because it helps loyalty scheme operators reduce costs relating to accounts reconciliation and payment management.

Additionally, as a network technology, Blockchain can help the creation of ecosystems and deliver network effects that will engage customers. By increasing member engagement, airlines who opt to tokenise their loyalty solutions can provide a greater range of personalised promotions and offers with almost real-time insights into passenger behavior, while sharing this data with network members in a secure manner.

8.2 Impact

Developing a blockchain-based payments infrastructure between the aviation industry and its customers provide for a seamless, documented, and efficient payment system, while reducing the need for payment processing and collection services. In essence, this reduces the man-in-the middle, and allows for direct payments from customer to service provider, without the need for intermediaries.

Additionally, a blockchain-based payments infrastructure within the aviation industry offers the ability for goods and services to be provided when payments are rendered, oftentimes with instant settlement. In aviation, goods and services may vary a great deal, and range from aircraft fuel and parts to gate fees. With near instant settlements that several digital assets provide, price-points could be established in real-time and adhere to true free-market laws of supply-and-demand, thereby driving down prices to the lowest acceptable levels throughout the industry. Furthermore, costs could be reduced even further by eliminating intermediaries, since the blockchain-inspired solution would enforce any of the necessary payment protocols and rules permissible by industry stakeholders. Additional

impacts would involve the ability to store, maintain, and analyse a historical log of on-chain transactions, which may provide ample opportunity for supply-chain management solutions.

8.3 Challenges

Given the current market hype around NFTs, there is a concern that many of the associated risks are being overlooked. For example, there's a lot of debate regarding the rights management of whatever is being tokenised, because it is commonly misconceived that a token is the same as what the object represents. In actual fact, a token is simply a small data file, while the object it represents may not reside on a blockchain at all. Therefore, it is unclear whether the owner of a token owns the rights to the object being tokenised, especially as these rights are interpreted differently across jurisdictions.

Similarly, most tokens are distributed and managed on the Ethereum blockchain as it has the most developed smart contract ecosystem. Because of the increased demand for Ethereum and the applications built on top of it, there is a substantial gas fee and energy consumption associated with transferring and minting tokens, ultimately due to the POW consensus mechanism which the Ethereum blockchain still runs on. In April 2021, gas fees for minting an NFT on Ethereum network cost approximately \$80, while gas fees for a transaction on the network costs approximately \$25 (based on figures in May 2021).⁴² However, as Ethereum and other token supporting blockchain network transition to POS, these fees are expected to decline substantially.

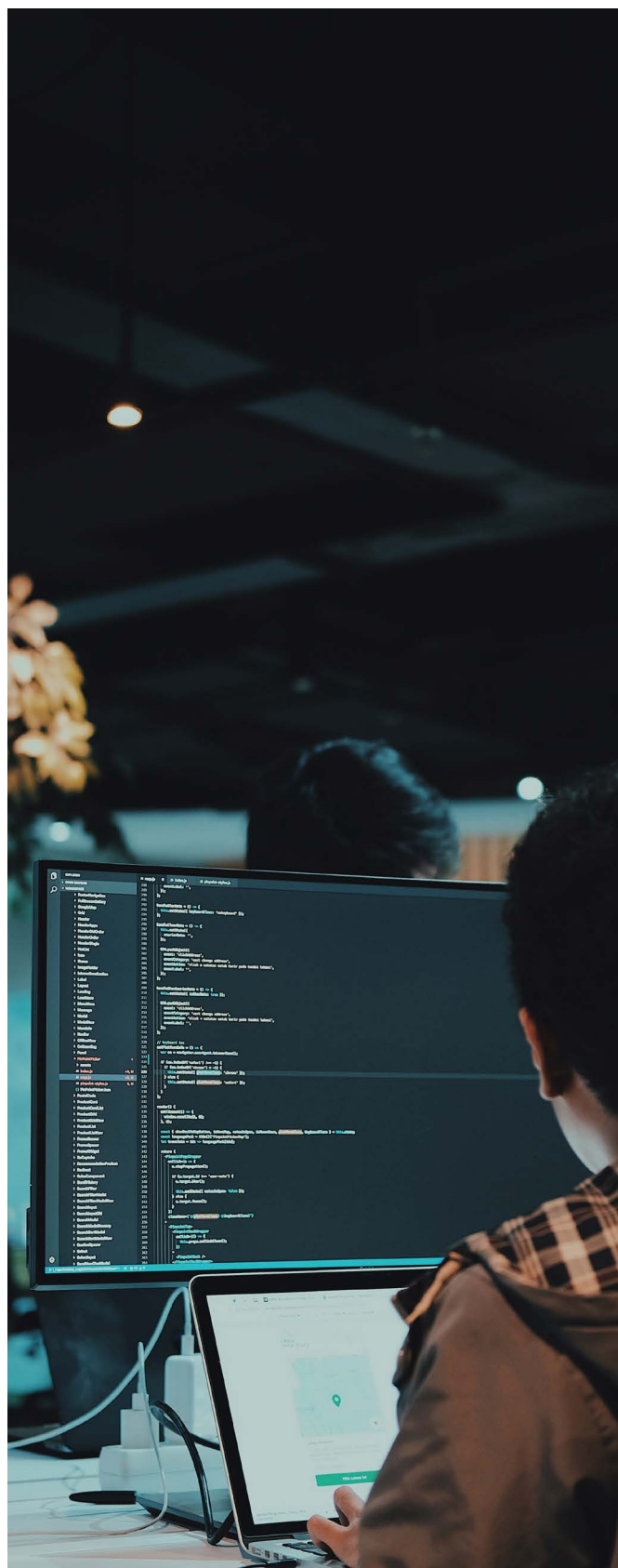
Lastly, there is the argument that loyalty systems are closed ecosystem and airlines wouldn't necessarily want their loyalty points to be exchanged with loyalty points from other airlines, limiting the likelihood of adoption. However, in order to remain attractive to customers, airlines may be left with little other choice.

Tokenisation of the Aviation Ecosystem

8.4 Maturity Level

KLM, Etihad Airways, Air France, Swiss Air, Lufthansa, Air Canada and Hahn Air have all partnered with the open-source travel distribution platform Winding Tree to issue flight tickets via the technology. The Winding Tree enables airlines to list their inventories, manage reservation requests and receive payments via fiat or cryptocurrency. Hahn Air was the first airline to do so, flying passengers with Blockchain powered tickets between Dusseldorf and Luxembourg in November 2019.³⁷

Certain airlines with loyalty schemes have begun distributing tokenised frequent flyer points using Blockchain technology. Since 2018, KrisPay, an extension of Singapore Airlines' KrisFlyer loyalty program uses a distributed ledger to account for digital currency units that customers can spend from their digital wallets, in the KrisFlyer merchant ecosystem.³⁸ Similarly, Cathay Pacific has a Blockchain-based loyalty app that lets customers spend their points in real time.² Other players in the wider Blockchain ecosystem have also been working on similar initiatives. Loyyal, a company using Blockchain to reinvent how customer incentives are created, rewarded, and managed; has been working with airlines such as Emirates, to bring transparency, efficiency and cost savings to existing loyalty and rewards programmes.



Conclusions and Recommendations

Beyond the general understanding that Blockchain is a synonym of Bitcoin, its goal is to address the issue of decentralisation of different systems in managing data distribution among multiple actors in a secure, trusted and immutable manner. Blockchain technology was born to enable fast, disintermediated P2P interactions.

In the Blockchain world, the definition of peers has evolved ever since enterprises entered the space. Today, Blockchain is being applied in both the B2C and the B2B spaces. Start-ups are increasingly developing and deploying applications for consumer and commercial utilisation. Enterprises themselves are experimenting with Blockchain technology, developing applications on decentralised networks of both private and public natures. Governments and industries are on the way to implement the value of Blockchain for their respective entities and the market now recognises successful implementations of Blockchain. Among others, secure payments with cryptocurrencies, supply chain, healthcare and identity management are notable cases of application.

In the aviation and ATM domain – that involves a complex system of interconnected resources, processes, and applications to deliver the safe and secure services of interwoven system-of-systems, comprised of both human and machine interactions – the Blockchain applications are several and of a key importance in the field. In this paper we have chosen to focus on the key aspects of identity management, fleet management, maintenance and supply chain, airspace management & flight planning, integration of UAS and other new entrants, the registration and recordation of airmen and passenger identities and tokenisation among others.

Many of the blockchain-based concept/use cases presented would impact safety, albeit indirectly. For many of the use cases examined (e.g., aircraft parts tracking) safety may be enhanced through the implementation of blockchain. However, it should be noted that this report was not drafted from a safety standpoint. Full safety risk analysis would need to be undertaken for any use case.

The needs of the aviation community are continuously evolving; the framework that comprises the aviation landscape remains fairly static, despite major leaps in technological advancements. It is inevitable that outdated technologies used today will need to be replaced with modern era capabilities. This new era is an excellent opportunity to start incorporating innovative technologies and among them Blockchain. Over time, as Blockchain demonstrates proficiency and gains public trust, the entire airspace infrastructure can further leverage its benefits. Organisations will need to conduct upfront financial, regulatory, and cultural evaluations of their current information systems to compare the true value added of embracing a Blockchain-based solution.

Blockchain is therefore a great opportunity for all the domain members of Aviation and ATM to rethink their information systems in which a shared-trusted real-time distribution of ATM-related information can pave the way for short/medium and long-term efficiency and rationalisation with the possibility of far-reaching automation and transition to the digital era of ATM.

References

1	<u>Blockchain in Aviation: Exploring the Fundamentals, Use Cases, and Industry Initiatives, IATA White Paper, Oct. 2018</u>
2	<u>What Could Blockchain Do for Airlines?, BCG, Mar. 2019</u>
3	<u>The Use of Blockchain in Aviation, GTG Advocates, Oct. 2019</u>
4	<u>Blockchain – a game changer in aircraft leasing?, Deloitte, 2018</u>
5	<u>Everything You Need to Know About Health Passports, Simply Flying, Feb. 2021</u>
6	<u>New health and other apps may make travel easier, The Economist, Feb. 2021</u>
7	<u>Digital Identity, Raconteur, Feb. 2021</u>
8	<u>The promise of self-sovereign identity and its impact across industries, Sovrin, Mar. 2020</u>
9	<u>“Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy,” NASA Ames Research Center, Moffett Field, California, 2019.</u>
10	<u>IBM Digital Health Pass, IBM</u>
11	<u>NewNorm, The Reality of Blockchain, Gartner, 2022</u>
12	<u>Future Flight – TEKToWr, TEKToWr, Nov. 2020</u>
13	<u>Deloitte's 2020 Global Blockchain Survey, Deloitte, Mar. 2020</u>
14	<u>Anthony Shook - Founder and CEO of AeroChain Discusses Blockchain in Aviation, Crypto on the Block Radio Show, Jul. 2018</u>
15	<u>SITA and key industry partners launch MRO blockchain alliance, SITA, Feb. 2020</u>
16	<u>Data for the life of the aircraft, PWC, Apr. 2019</u>
17	<u>The Role of Blockchain Technology in Aviation Industry, IEEE Aerospace and Electronic System magazine, Oct. 2020</u>
18	<u>Generating more transparency in aviation with blockchain technology, Lufthansa Industry Solutions</u>
19	<u>Blockchain in the Aviation Industry, BBN Times, Aug. 2019</u>
20	<u>Governance and structuring considerations in blockchain consortia, Deloitte, 2020</u>
21	<u>Blockchain-enabled supply chain: analysis, challenges, and future directions, Sohail Jabbar et al., Nov. 2020</u>
22	<u>Flight Object Sharing Capability Using Blockchain, The MITRE Corporation, Apr. 2020</u>
23	<u>Meet the Global Blockchain Alliance, SITA, 2019</u>
24	<u>U-Space Concept of Operations Volume 1 & 2</u>
25	<u>Unmanned Aircraft System Traffic Management (UTM) Concept of Operations v.2.0</u>
26	<u>Blockchain for Unmanned Aircraft Systems, Volpe center, April 2020</u>



Click on the links above to read more.

References

27	<u>US Dept of Transport Explores Blockchain for Drones, Air Traffic Management, Ledger Insights</u>
28	<u>SkyGrid</u>
29	<u>Distributed Sky</u>
30	<u>SkyyNetwork</u>
31	<u>AnraTech</u>
32	<u>Helium</u>
33	<u>Red Cat & GoChain: “Red Cat Partners with GoChain for Blockchain Based Drone Data Storage, Analytics, and Services Platform</u>
34	<u>Air Market: “A Decentralised Solution for Integrating Large-Scale UAS Operations in Future Aviation System”</u>
35	<u>Covid: Airline industry travel pass ready ‘within weeks’, BBC, Feb. 2021</u>
36	<u>The Eight User Rights Under the GDPR, Privacy Policies, Jan. 2021</u>
37	<u>A Practical Application of Blockchain for the Travel Industry, Winding Tree</u>
38	<u>KrisFlyer Launches Innovative Miles-Based Digital Wallet, KrisPay, Singapore Airlines, Jul. 2018</u>
39	<u>Accelerating Profitable Partnerships Through a Blockchain Loyalty Platform, Loyyal</u>
40	<u>The UK digital identity and attributes trust framework, DCMS, Feb. 2021</u>
41	<u>Zamna</u>
42	<u>Ethereum Gas Limit Hits 15M as ETH Price Soars, Coinbase, Apr.</u>



[Click on the links above to read more.](#)

This report was written based on our knowledge and research up to and including the summer of 2021. Even though the technology and industry in the Blockchain domain have progressed significantly since then, the key findings and themes of the report remain valid.

In this report we have included reference to certain projects to illustrate use case concepts within the aviation and ATM industry and highlight how these relate to the use of Blockchain technology. Those projects are not directly supported or recommended but serve as examples of blockchain use.

