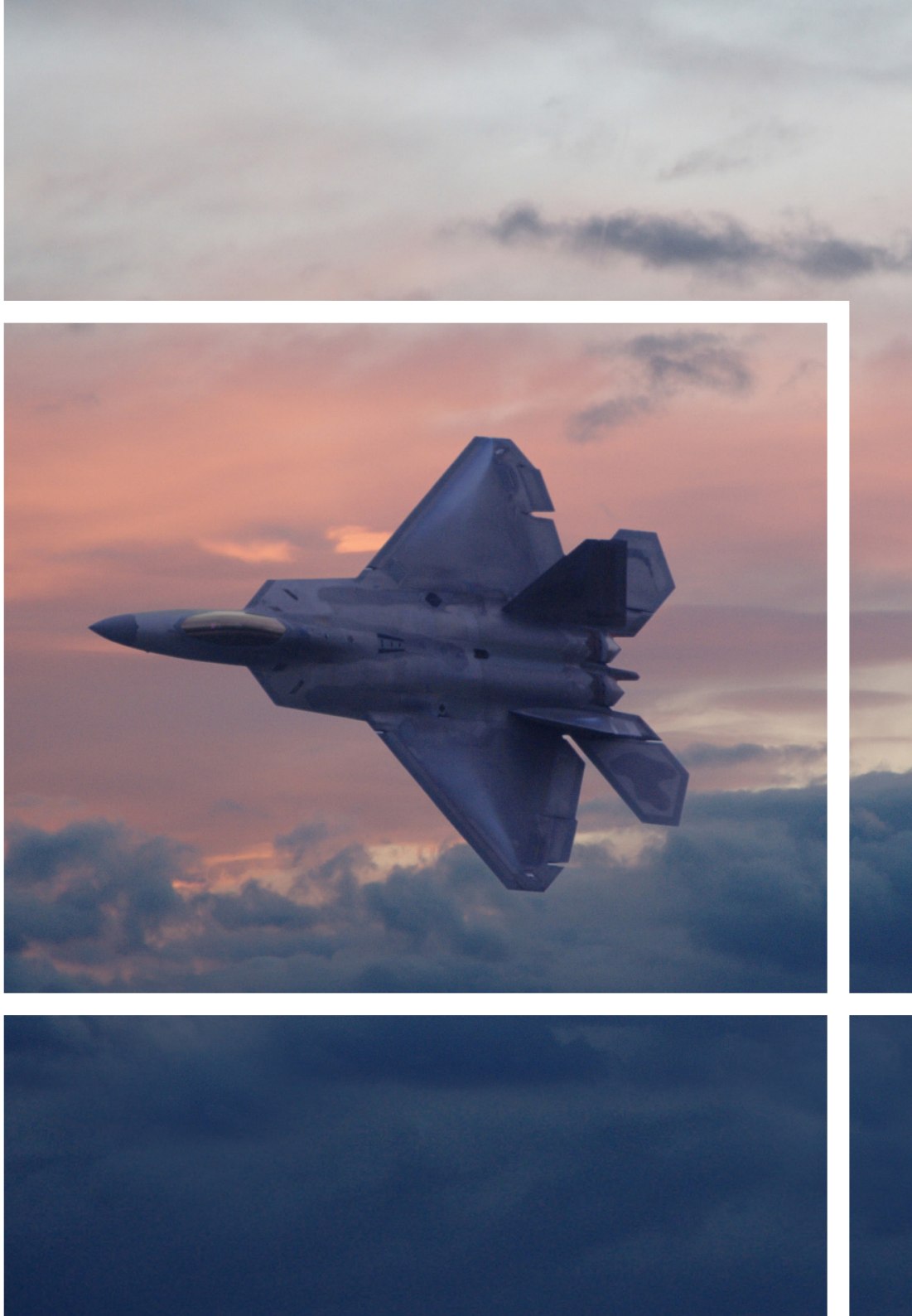
www.pwc.com/blockchain-defence

How blockchain can transform defence assets and give armed forces an advantage on the battlefield

August 2020



pwc

Contents

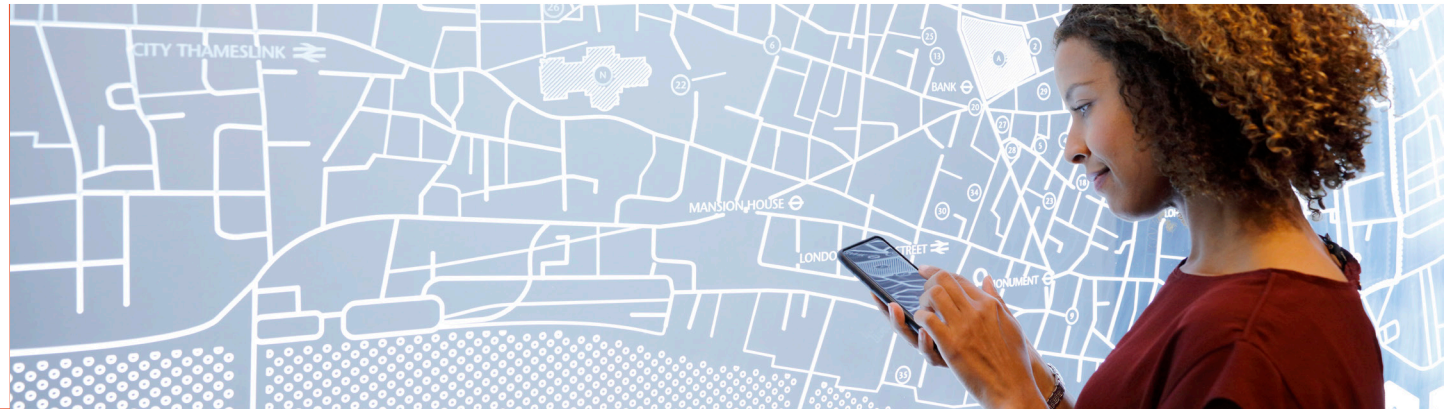
Introduction

Most defence platforms and systems are staggeringly complex. These assets are very mobile (globally) and require collaboration among a number of entities to keep them operational and mission-ready. Technology can help operators, manufacturers and suppliers 'harden' the supply chain and improve operational performance through the entire life cycle, from raw material to retired asset.

Like most weapons systems of the last generation, the F-35, produced by Lockheed Martin, is one of the most advanced weapons platforms in the history of the world. Each F-35 fighter jet has about 300,000 components, manufactured by a worldwide network of more than 1,900 suppliers.[1] Furthermore, Lockheed Martin doesn't just manufacture the F-35; it has also contractually committed to help keep the planes functioning even after the US Department of Defense (DoD) or international ministries of defence accept delivery. The goal is that by 2025, 80% of all F-35s will be operational at any given time, with a cost per flight hour of US$25,000 (which is lower than the cost to operate older, less-advanced platforms). If it falls short of those goals, Lockheed Martin is at risk to absorb the financial cost of closing the gap.

Despite the sophistication of many weapons systems and platforms, their supply chains — both for raw material to finished product and post-production maintenance — are often still managed using traditional, and largely manual, processes. Some government customers have applications to trace and certify parts, but orders, parts status, retrofits and other routine processes have to be coordinated across multiple systems, with each supplier keeping tabs on its own information. Many original equipment manufacturers (OEMs) also have their own centralised systems to coordinate with suppliers for a given programme, but those are proprietary and siloed.

1 Lockheed Martin, *F-35 Lightning II Program Status and Fast Facts,* 1 June 2020, https://www.f35.com/assets/uploads/documents/F35FastFacts5_2020.pdf.



To hit performance metrics, OEMs can use blockchain to improve the way they track parts, inform the analytics that anticipate when repairs will be needed and make maintenance processes far more efficient.

Blockchain holds the potential to significantly improve the way defence contractors manage supply chains, leading to far more efficient processes for the life of the asset — from original manufacturing through retirement and (eventually) parts harvesting. In addition, blockchain offers particular operational performance improvement for assets after they go into service — a component of the life cycle that current technology solutions, including some enterprise resource planning systems, may not support.

This aftermarket capability is critical to sustainment (or 'power by the hour') contracts that are proliferating in defence contracting. In that way, blockchain offers a solution to address the risks that OEMs are taking on when they commit to sustainment contracts with financial penalties. To hit performance metrics, OEMs can use blockchain to improve the way they track parts, inform the analytics that anticipate when repairs will be needed and make maintenance processes far more efficient.

Much has been written about blockchain — essentially a distributed ledger application that allows multiple organisations to track information about a particular object, such as an aircraft tail number or engine number, in a more secure, reliable way (see 'The basics of blockchain'). PwC has analysed the potential for blockchain to improve the performance of commercial aerospace OEMs and suppliers. As that publication put it, "What the aerospace industry doesn't know about its planes is costing it serious money." It also found that efficiency gains from blockchain could increase industry revenue by up to 4% annually, or US$40bn, while cutting maintenance, repair and overhaul costs by about 5%, or US$3.5bn. Yet the technology holds just as much promise in applications for defence manufacturing and operations. In fact, the complexity of US defence contracting and operations, and the massive size of defence budgets, suggests that the financial gains could be even greater — not to mention the potential increase in national security it can bring.

The basics of blockchain

At a high level, blockchain is a distributed electronic ledger. It can be used to track financial transactions, parts histories, employee certifications or any other information where multiple parties need access to reliable, authenticated data.

To understand how it works, it helps to understand what blockchain is not. In a traditional database, a central party controls the information and distributes it to participants. For example, your bank keeps the master file of your transactions and sends you a statement at the end of the month. You can't change the transaction record and have it reflected on the bank's side.

In a blockchain, by contrast, all participants — or nodes — receive validated information contained in the blocks (or information fields) at the same time, resulting in as many encrypted copies of the data as there are nodes. There is no master or subordinate recipient of information. An algorithm uses the data within a given block to generate the key for the next block. If someone tries to change the data in a field without authorisation, it becomes immediately apparent to all participants because the chain breaks.[2] In that way, blockchain technology is more transparent to participants and more secure to outsiders.

Blockchain also enables the use of smart contracts — essentially, a set of pre-existing conditions that, when met, automatically execute a specific step. For example, a company could use a blockchain-enabled smart contract to automate accounts payable. When the company orders a product, everyone on the chain is notified at each step — when the order is placed, shipped, delivered to and accepted by the recipient. At that point, the blockchain could automatically issue a payment, which would again be communicated to all relevant parties at each stage of the transaction.

2 Noor Muhammad Khan, "A Very Brief History Of Blockchain Technology | Blockchain History 2019," Medium, 21 Jan. 2019, https://medium.com/@muhammadnoor/a-very-brief-history-of-blockchain-technology-blockchain-history-2019-3c9f9857e085.

Needed: Supply chain support

Because most weapons systems supply chains are so complex — with some components requiring parts from fourth- or fifth-level suppliers — they are prone to disruptions. For example, the US Government Accountability Office flagged several issues with the F-35 supply chain, including shortages of spare parts, limited repair capabilities, mismatched parts for deploying aircraft and an immature global network to move parts.[3]

In addition to manufacturing the original asset, many contractors struggle in retrofitting and upgrading new versions. The basic M1A1 Abrams tank platform used by the US Army dates back to the 1970s, and it has gone through a dizzying number of variations and upgrades in weapons, armour, drive train and electronics. (The newest, the M1A2C, manufactured by General Dynamics Land Systems, will replace the M1A1 SA, which will be retired by 2025.)[4] Having multiple variants in use by multiple units — not to mention those in use by the armed forces of foreign governments — makes it extremely difficult to ensure that the right part is available to go into the right asset, at the right time in its life cycle. When any one of those elements goes wrong, the result is a production delay, a downed asset, a bad part and an overall reduction in readiness levels.

Another central challenge is that defence supply chains simply don't put enough emphasis on supplier risk management. The development of complex platforms can involve multiple layers of sub-suppliers and vendors, some of which may offer the lowest price for a component but are based in countries that the US would not consider allies. As a result, OEMs and government customers face an unacceptably high level of risk for compromised or counterfeit components, each of which creates vulnerabilities for assets both during development and once they enter their operational service life. Worse, foreign intelligence operatives can hack assets and either reduce their effectiveness or develop countermeasures for their own government's forces.

3 Talal Husseini, "F-35 progress: Three challenges to the F-35 supply chain," *Air Force Technology,* 2 May 2019, https://www.airforce-technology.com/features/f-35-progress-supply-chain/.

4 David Axe, "Here's your first look at the Army's new M1 Abrams variant," *Task & Purpose,* 26 Feb. 2019, https://taskandpurpose.com/military-tech/m1-abrams-tank-m1a2c.

Taming the complexity

Blockchain is a proven means to increase efficiency and transparency throughout industrial value chains. How? By validating data among participants in a way that is simultaneous, encrypted, permissioned and safe. Rather than each node of the supply chain managing its own information, blockchain creates a single source of the truth that links all nodes in real time. Any change made at a single node gets made automatically across every node. No unauthorised changes can be made to the data. As a result, everyone has access to the same permissioned information, and they can trust that the information is current and correct.

In that way, the technology can address a range of manufacturing pain points, including by

- establishing the provenance of raw materials and parts, and helping manufacturers detect counterfeits
- increasing visibility throughout the supplier network (all tiers)
- proactively identifying parts shortages to reduce manufacturing problems, inefficiencies and unnecessary costs
- managing the identities and certifications of people handling parts, assembling components and executing repairs and upgrades
- tracking assets globally
- coordinating quality assurance
- validating multi-jurisdictional regulatory compliance
- improving defence programme management
- reducing fraud, waste and abuse.

Given the potential improvements from blockchain, we believe that ignoring it is a significant missed opportunity. Specifically, we think three applications or use cases should be priorities for defence OEMs and contractors.

Transparency along the supply chain and throughout an asset's operational life

The most intuitive application of blockchain is to increase the transparency of the supply chain, not only during manufacturing but once an asset is in operational use. By using the technology, each part can be tracked from raw materials through assembly to finished component, to its installation in an operational asset and then throughout its service life. The information about that part would travel with it, across its entire life cycle — a concept referred to as a digital thread for that part. OEMs could trust that the part was exactly what the supplier said it was, with no risk of counterfeiting or tampering along the way. (De Beers is now using blockchain to track the provenance of diamonds, from mines through production and into the hands of consumers.)[5] Blockchain can even track the name and certification level of the technician performing a specific repair.

Aggregating the threads for individual parts would allow OEMs to assemble a digital twin for each asset as well, with an intact, current and comprehensive history of every part that went into it, along with all repairs, retrofits and 'supercessions' (or upgrades). For example, each individual fan blade within an engine would have its own recorded history in the blockchain, as would the engine itself and the plane it powers. The result would be a far more systematic means of tracking information on the operational history of an asset, leading to increased reliability and uptime. Taking that logic to the next level, a force could leverage the Internet of Things to develop a digital twin of the battle landscape across all deployed assets: land, air and waterborne. With the convergence of additional emerging tech — specifically AI and machine learning (ML) — a blockchain-based platform could enable the deployment, management and tracking of manned and unmanned vehicles.

5 Nathan Munn, "De Beers Is Embracing Diamond Tracking Based On Blockchain Technology, *Polygon,* https://www.polygon.net/jwl/public/trade-resources/jewelry-insights/de-beers-diamond-tracking-blockchain-en.jsp.

If a part were to fail, OEMs and the DoD would be able to determine immediately which other assets included that part and trace it back upstream to determine what kind of mitigation measures would be needed (along with the potential battlefield implications of an asset being unavailable). Blockchain could quickly identify whether the problem was limited to an individual part or batch, or indicative of a more systemic issue. As a result, it could take steps to prevent the same part from failing elsewhere by identifying which production lots to recall. Blockchain could also be used to allow manufacturers to produce their own parts, at site locations and on demand, using 3-D printing. In that application, blockchain would be used to validate the manufacturing process and then the part itself.

Notably, blockchain technology can support OEMs as they transition from a traditional procurement model to sustainment, or power by the hour, arrangements, in which they no longer sell assets to the DoD but instead sell capabilities. For example, instead of selling airborne fuel tankers, an OEM could sell a specific number of refuelling missions in a given geography and time period. Space commands are also an expanding realm for private contractor operations. These arrangements are gaining momentum, but they shift the operational risk from the military to the OEM that retains control over the asset.

Blockchain provides the transparency and insight needed to link production and operational use, with a single set of data that allows manufacturers to meet not just delivery targets but operational requirements as well. In that way, the technology can help OEMs deliver higher service levels and thus improve their financial performance in these types of contracts.

For example, just about any platform or system used by armed forces has to be periodically inspected — manually — as part of routine maintenance checks. But greater visibility into the condition and usage of each part, distributed to all nodes along the supply chain, could dramatically improve the speed and efficiency with which these checks are completed. Instead, forces could shift from reactive maintenance (after a part fails) to prescriptive maintenance (accurately predicting when it will fail). Powered by AI and ML, the asset itself could link to OEMs and suppliers and call for the required part in advance. That approach would allow maintenance units to retain smaller parts inventories. Moreover, DoD procurers would know that a part ordered from an OEM or supplier is authentic, because it would be validated through the blockchain at every stage of manufacturing and transport to the asset itself.

Validating suppliers

The second major application is validating suppliers. In the past, DoD suppliers essentially had to self-certify that their cyber practices were secure, and the Defense Contract Management Agency would conduct spot audits to ensure compliance. As the battlefield has become digitised, that approach is no longer stringent enough to protect all the data that defence contractors provide and can access.

According to some estimates, up to 70% or more of all defence data resides on contractor networks. Moreover, security breaches cost the US hundreds of billions of dollars a year, nearly equalling the DoD's annual budget. The transition to 5G will increase potential vulnerabilities, and there are indications that many contractors have work to do in order to improve their cybersecurity practices. The National Institute of Standards and Technology (NIST) sets out more than 100 cybersecurity controls, and according to the DoD, only 1% of contractors have implemented them all. In addition, perceived security risks increase with smaller suppliers upstream.

But in late 2020, a new set of security standards will take effect. Called the Cybersecurity Maturity Model Certification (CMMC), the system gives each supplier a rating across five levels, based on a mandatory third-party audit, and that level determines whether a supplier is eligible to win DoD contracts. (For example, if a contract is designated as Level 3, suppliers must have a Level 3 certification or higher by the time the contract is awarded.) The levels are based on NIST frameworks for cybersecurity.

The new standards, though necessary, pose an additional administrative burden on OEMs and Tier 1 suppliers, which must vouch for the certifications of all their sub-suppliers on a given contract. However, this is the type of process — involving certifications across a network of companies collaborating on a project — that blockchain can manage. By linking all suppliers for a given contract on a blockchain, a large supplier or OEM can easily keep track of certification levels and validate those to the DoD when bidding. There are potential benefits for governments as well, in terms of reduced administrative costs and time spent on audits, and — critically — increased security.

Increased cybersecurity

Last, blockchain can help make the supply chains for defence assets — and the assets themselves — more secure. As noted above, cyber threats, either from hackers or foreign states, can attack the supply chains of weapons platforms and systems. They can also attack the underlying intellectual property behind those designs, or the assets themselves. Some estimates hold that a new asset has, at best, a six-month advantage on the battlefield before enemy forces have figured it out and developed countermeasures.

Blockchain is a means to extend that period by protecting supply chains and critical information about an asset, thus giving armed forces an edge in combat. All private blockchains are encrypted in a way that makes them extremely difficult to hack. The baseline version of the technology encrypts the links between each block of data. In addition, however, OEMs and suppliers could encrypt the data itself, adding a second layer of security to the chain. Blockchains such as Bitcoin use SHA-256 encryption, which has as many unique key values as the number of known atoms in the universe. The most powerful quantum computers on the planet are not close to cracking those algorithms, and when they start to get close, the increase in computing power will allow for richer encryption as well. (The next generation of encryption, SHA-512, would square the number of available keys.)

A global application: Managing foreign government offsets

In addition to applications to support the cradle-to-retirement life cycle of US-owned defence platforms and weapons systems, blockchain can also help domestic OEMs work with the foreign governments — particularly in developing markets — that buy their products. For understandable reasons, many of those governments want to evolve beyond mere customers in the acquisition process, and instead build up some of their own local capabilities in manufacturing, research and development, and other areas.

To accomplish that goal, most foreign governments have some type of offset programme in place. Offsets require that the OEM selling its products to a foreign government spend some portion of the total contract value in the foreign country. The value may come through extracting natural resources in that country, buying components from local suppliers or developing talent with the skills needed to maintain the assets purchased through the contract. In 2017, US defence contractors reported more than 500 offset transactions, worth US$4.6bn.[6] OEMs that fall short of offset agreements typically have to pay financial penalties and face a hit to their reputation.

Each country's offset programme is tailored to its own needs, and successful programmes can turbocharge the development of local capabilities. Brazil, Japan and Spain have all successfully applied the concept. But current systems have several challenges, primarily because they add an additional layer of complexity to supply chains that are already highly complex. Some offset programmes suffer from a lack of transparency in terms of the exact contribution of an offset incurred by a supplier. Quality inspections in the local country are often lacking, and the parts produced through these systems may not be reliable. Corruption can be a factor.

Even the math itself can get complex. Different types of activities are assigned a multiple, depending on how valuable they are to the foreign government. For example, extracting natural resources from a purchasing country is typically a low-value activity in offset programmes. But higher-value activities, such as training local employees to code software or use advanced manufacturing technology, get assigned a higher multiple, thus helping OEMs get to the offset amount faster.

Blockchain can help OEMs manage these complexities by integrating all data about the offset programme into a distributed, encrypted, reliable ledger. The chain can keep track of offset data — including percentages and values — and share that with key stakeholders in the purchasing country's government, including ministries of defence and finance.

Benefits come throughout the entire process, from bidding through manufacturing. Offsets typically are negotiated as part of the bidding process, and those aspects can be entered into the chain as part of a smart contract for the OEM that wins the bid. Local suppliers that want to work with an OEM can enter their credentials to establish their legitimacy. During the design process, the OEM can control which suppliers have access to certain categories of data, and for how long, to ensure that local suppliers get the information they need but nothing more. When parts are manufactured by local suppliers, each component can get a unique digital ID stamped onto it, validating that part to the OEM and allowing the chain to track it during its operational life. And the actual value of that component would be determined in a preset way and then entered into the chain, as part of the overall contract.

The bottom line: offsets are an additional application for blockchain that can help increase transparency and reduce complexity for OEMs that sell to foreign governments.

6 US Department of Commerce, Bureau of Industry and Security, Offsets in Defense Trade: Twenty-Third Study, April 2019, https://www.bis.doc.gov/index.php/documents/other-areas/strategic-industries-and-economic-security/offsets-in-defense-trade/2387-twenty-third-report-to-congress-4-19/file.

How to start

OEMs and suppliers that want to capitalise on blockchain need a clear plan of action. Here are three priorities for organisations in the defence industry to focus on:

Start small — but don't start alone

Because blockchain technology represents such a different way of thinking about supply chain and manufacturing issues, many organisations fall prey to institutional inertia. They have so much invested in existing supply chain processes that the thought of starting over with an emerging technology prevents them from taking any action. This is particularly true because the real value of blockchain comes when all participants in a supply chain are integrated on it. In that way, the very problem that blockchain can help solve — the complexity of defence supply chains — becomes a barrier to solving it.

To avoid that impulse, organisations should start small and treat blockchain as a scalable technology. Rather than trying to integrate the entire supply chain for an asset on Day One, they should work on creating a blockchain for a single component and two to three supplier partners that can explore the technology together (with visibility to the DoD). In that way, the organisation can develop some expertise and capabilities in a relatively small-stakes pilot and build from there. Counter to conventional wisdom, blockchain does not require advanced computers or other technology investments; most organisations could start with the IT infrastructure they already have in place.

Build the blockchain with compliance in mind

Second, because DoD procurement is so heavily regulated, OEMs and suppliers should consider the new CMMC regulations — along with any other evolving changes — related to blockchain development. For example, ensure that the metadata for products in the supply chain is incorporated into the chain. This includes data such as CMMC certification specifications, including the supplier's designated level, the date authorised and the organisation that issued the certification. Working with the CMMC Accreditation Body and the Defense Contract Management Agency now on what potential requirements could look like could substantially save costs later from the typical audit activities necessary.

Quantify real-world benefits

In commercial aerospace, suppliers and OEMs have launched notable initiatives to show the value of blockchain. For example, Moog, which offers blockchain-enabled 3-D printing of aerospace components, conducted a real-time test with Air New Zealand to show its capabilities. The airline ordered a part for one of its planes — a component of the in-flight entertainment system — and a digital file for that component was then sent to an approved printer at a hangar in Los Angeles. It was printed on demand, verified as authentic and installed in the plane before its departure.

In defence applications, the mission-critical nature of parts and components means that those kinds of tests are unlikely. But OEMs can still conduct tabletop simulations that allow them to determine the potential advantages of blockchain. The simulation would allow the OEM to bring multiple suppliers and participants together to work through potential scenarios to determine how information and material would flow through a blockchain, how that would increase transparency and reliability, and how it would reduce risk and unnecessary costs. Notably, this kind of simulation would be extremely inexpensive to conduct.

Conclusion

Some defence contractors believe there could be a risk to transitioning to an emerging technology like blockchain. We believe the bigger risk is in not implementing the technology. Blockchain is no longer an untested, novel solution; it has the potential to increase transparency and performance, from the supply chain to the maintenance and management of in-use operational assets. Given that potential, the only question is which OEMs will be bold enough to seize the initiative and begin investing in the necessary capabilities to capitalise on blockchain.

Authors

Rachel Parker Sealy
Industrial Products Technology
Principal, PwC US
+1 314 206 8183
rachel.parker.sealy@pwc.com

Chad Gray
Cybersecurity and Privacy
Principal, PwC US
+1 443 734 4760
chad.gray@pwc.com

Glenn Brady
Global Aerospace and Defence Leader
Partner, PwC US
+1 314 206 8118
glenn.brady@pwc.com

Scott Thompson
US Aerospace and Defence Leader
Partner, PwC US
+1 703 918 1976
scott.thompson@pwc.com

Miguel Denosky-Smart
Aerospace and Defence Strategy and Operations
Principal, PwC US
+1 703 283 7737
miguel.denosky-smart@pwc.com

Matthieu Lemasson
Aerospace and Defence
Partner, PwC France
+33 1 56 57 71 29
matthieu.lemasson@pwc.com

www.pwc.com/blockchain-defence