

AREA42

WHITE PAPER TRADETECH

Cyber-Physical Systems x Blockchain for Trade

Research led by Roy Nahum

White paper outline and coordination
by Florent Bardy, Innovation Lab Lead

MARCH 2022

Table of contents

Meet the authors	P02	CPS and Blockchain use cases	P20	Challenges/What would it take to win	P33
Introduction	P04	Insurance / financing - Consumer	P21	Relevant established groups and Consortia	P34
Definition and assessment of level of maturity and standardisation	P05	Pay per use - Financing and insurance	P22	Trade Blockchain consortia	P35
Cyber-Physical Systems (CPS)	P06	Supply chain	P25	Potential partners: CPS providers	P38
Blockchain	P08	Logistics	P26	Appendix	P40
Benefits of Blockchain in CPS	P10	Agriculture	P27	Developing common standards	P40
CPS/Blockchain products and service ecosystem	P11	Data sharing	P28	About AREA42	P42
Assessment of maturity and standardisation	P13	Identity Wallets for individuals and equipment	P28	Interviews with	P43
Summary - Maturity	P14	Facilities management	P29	References	P43
Breakdown - Maturity elements considered	P15	Energy	P29		
		Infrastructure	P29		
		Key issues in opportunity assessment for CPS+BC in Trade	P30		
		Participation incentive	P31		
		Leading with size	P32		
		Building the ecosystem	P32		



01

Meet the authors

Roy Nahum has a background in multiple industries (Entrepreneurial, Online, Trading, FMCG, Retail, B2B). Most of his work focuses on Management Consulting particularly performance improvement using analysis and technology.

He started his career journey by starting a small export sales business in Shanghai, where he developed first-hand experience in dealing with manufacturers of all capability levels, freight forwarders, and trade finance. There he learned about the many possible inefficiencies within those systems. More recently, during his time in Supply Chain Planning and Operational Excellence roles for BP's Castrol / Trading & Supply businesses he has experienced more advanced supply chains. In between, most of Roy's experience was in Management Consulting, internally at BP, then later at McKinsey.

He worked as part of BP's Performance Improvement team, and was heavily focused on data analysis to determine performance gaps and identifying opportunities to revise processes, improve capabilities, or introduce new software and tools. At McKinsey, he was part of the Sales and Marketing practice, focusing on performing rapid client diagnostics and implementing McKinsey's sales and marketing Software-as-a-Service (SaaS) solutions.

Roy has built websites, managed multiple system implementation projects, and has worked in Product Owner roles on Agile product development teams. He has also made his home a Smart Home with many devices now routinely powered by his voice. Despite this experience, Roy doesn't code. His expertise lies in how business can benefit from using technology to improve operational inefficiencies.



Florent Bardy is a Senior Innovation Strategist with expertise in business trade venture building.

He holds a Master degree in business administration from Audencia Nantes Management School with a specialisation in Finance. Florent has accumulated over a decade of trade credit expertise from top tier financial institutions in Singapore, Paris and London. Florent is credited with taking part in the creation of the financial institutions department of the French Credit Insurer Coface in Western Europe.

In 2018 he decided to move from the traditional trade credit business to take a more digital and entrepreneurial journey.

He first collaborated with the B2B Venture Builder Alpine style before taking part in the foundation of the first trade innovation ecosystem, AREA42, backed by Belgian Credit Insurer Credendo.

AREA42 brings together innovators from across the world to discuss frictions in B2B trade and ideate on how to leverage technology to make trade more fluid in a changing world.

As Innovation Lab lead, Florent co-designed and co-managed the AREA42 innovation funnel to gather relevant ideas, turn them into experiments and build MVPs to bring innovative TradeTech products to the ecosystem.

Florent has since then taken new responsibilities as Product Manager of one of our new upcoming ventures.

02

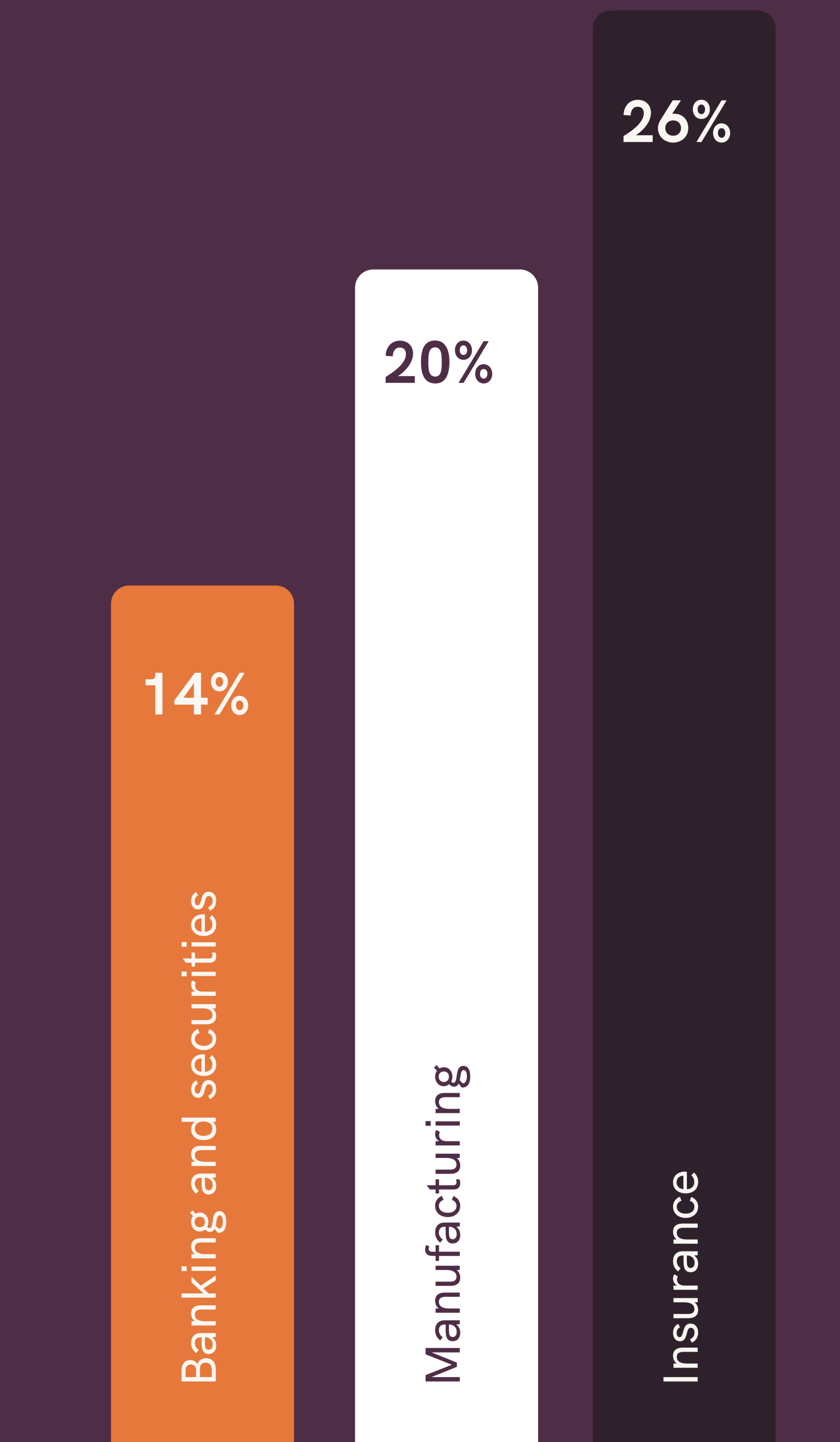
Introduction

The Internet of Things (IoT) is gaining popularity in industry, government and consumer realms. The variety of tools, manufacturing technologies, and legacy systems inherent in industry has resulted in a truly enormous range of devices that can be connected together to provide real time insight and action.

The increasing number of devices connected together also means that there are also now multiple entry points for malicious actors. Once vulnerabilities in IoT devices are exploited to

cause harm, confidence in IoT may shatter (think self-driving cars, plants handling dangerous materials, or healthcare devices), particularly if these devices are integrated across companies. Security is paramount and using Blockchain can help to ensure that trust is maintained when data starts being shared across companies.

Accenture Strategy estimates that the industries that will capture the most value from IoT are **insurance (26%)**, **manufacturing (20%)**, and **banking and securities (14%)**. The race is on to provide targeted IoT—and IIoT—services for each of these industries. IIoT offers a wide scope for solution innovation.

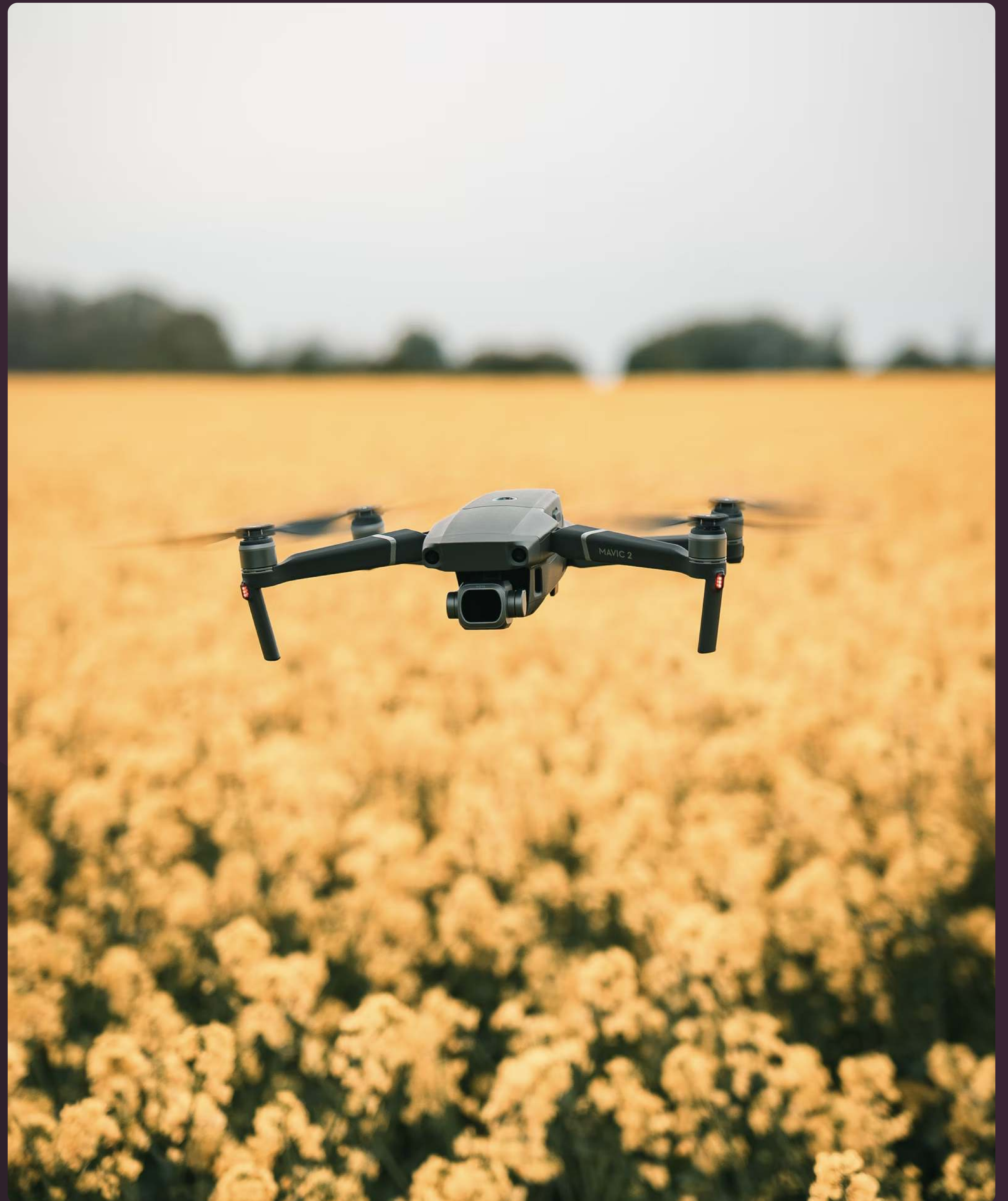


Accenture Strategy estimation of the industries that will capture the most value from IoT

03

Definition and assessment of level of maturity and standardisation

Cyber-Physical Systems	06
Blockchain	08
Benefits of Blockchain in CPS	10
CPS / Blockchain products and service ecosystem	11



Cyber-Physical Systems

DEFINITION

The basic definition of IoT Technology is any device that can connect to the internet so that it can either relay sensing information that it has gathered, or execute an action identified for it.

In the consumer domain, common examples of these are: health trackers (Fitbit); security (doorbell cams, smart locks, nanny cams); smart devices (smart plugs to turn on/off any device, washing machines that signal when maintenance is needed); which are often linked into a smart home (Google Home, Alexa) or mobile device. Most of these can either be activated automatically or remotely, or collect and send data automatically.

The Industrial Internet of Things (IIoT) is similar to IoT which consists of mainly consumer products, but with a few key characteristics:

- Potentially massive data being transferred (e.g. turbines collecting more than 500gb of data per day).
- Far more precise sensors are often required.
- More urgent emergencies: system failures can have significant downtime cost, as well as the potential risk to human life.
- Smart factories are typically composed of multiple systems working together (a “System of Systems” SoS)
 - “IO” level (Device level - Sensor “Input” / Actuator “Output”).
 - Device controller level.
 - SCADA (Supervisory Control and Data Acquisition) level.
 - MES, Manufacturing Execution Systems to plan and execute.
 - ERP (SAP etc.).

A Cyber-Physical System (CPS) is an interacting network of physical and computational components, where devices are controlled or monitored by computer-based algorithms. These are sometimes referred to as “embedded systems” under the Internet of Things (IoT) umbrella.

CPS focuses more on the coordination between a larger number of physical and computational elements, usually with a larger network of connected devices. A CPS can be a single device, or multiple devices or systems, forming a “System of Systems” (SoS). Other terms commonly used in this space include Internet of Things, Industrial Internet, Smart Cities, Smart Grid, Machine to Machine (M2M), “Smart” anything (devices, cars, buildings, homes, manufacturing, hospitals). CPS are a core component of Industry 4.0. There is enormous overlap in these fields so, for simplicity, this report will use them all under the CPS umbrella, within the realm of Trade.

THE FOUR INDUSTRIAL REVOLUTIONS

- 01 **Industry 1.0**
Mechanization and the introduction of steam and water power.
- 02 **Industry 2.0**
Mass production assembly lines using electrical power.
- 03 **Industry 3.0**
Automated production, computers, IT-systems and robotics.
- 04 **Industry 4.0**
The Smart Factory. Autonomous systems, IoT, machine learning.

BENEFITS OF CPS

Monitoring

Traditionally, plant operators would walk the plant on a regular basis, reading devices (such as pressure gauges) and noting it manually on a piece of paper. This obviously meant that urgent safety events could not be responded to in real time.

Modern plants not only have automatic sensors that track this information and relay it to a central control room, but also have safety systems that make actuators shut off critical processes when a potential emergency is detected – responding much faster than humans can.

Automation

Removal of manual processes and replacing them with combinations of sensors and actuators that understand commands (e.g. from planning tools) and execute.

The Mini Cooper plant in the UK receives online orders, and combinations of robots and sensors then build 90% of each car to order.

Only the final touches like in speaker cable wiring (requiring more dexterous hands) is done manually. This plant which used to operate with 2000 people now operates with 40.

Maintenance

Maintenance has often been “reactive” in nature – waiting for items to break down before they need replacing. At best, this results in unplanned downtime (risking customer satisfaction). At worst, these events can be catastrophic in nature, destroying plants and potentially human lives. Most factories have moved to “preventative maintenance” – understanding the lifespan of an item (e.g. a bolt holding two sections of piping together; or a machine in a production line) and replacing it when it is expected to fail (based on historical averages).

“Smart” factories are moving to “predictive maintenance”, whereby IoT sensors monitor item conditions (e.g. through vibrations in the case of the bolt, or internal temperature sensors in the case of the production line machine), and identify a likelihood of failure. Both allow for plants to better anticipate failures, and plan their maintenance scheduling and purchasing more effectively. If failures do occur, information can be used for root cause analysis (e.g. in cases of catastrophic failure such as an explosion, where there is no asset to analyse anymore).

This concept is not limited to plants, it is also widely used for machines such as planes, trucks and ships – to identify when spare parts or maintenance are likely needed (e.g. pressure sensors in tyres), to save on call-out costs.



Sales and Operations Planning (S&OP)

The core concept of S&OP is that having better visibility and integration of sales forecasts ensures that production can be planned more effectively, resulting in better batch scheduling, better raw materials ordering and delivery, and reducing inventory (working capital).

More advanced companies in this area are going a step further, sharing their forecast demand with upstream suppliers – enabling these suppliers to in turn optimise their production and reduce Cost of Goods Sold (COGS). Furthermore, they can also track status and location of their orders in real time, updating estimated delivery schedules in real time, reducing the need for “buffer stock”.

Blockchain

DEFINITION

Blockchain is a distributed ledger of transactions and assets. It provides a trusted view of who did what, who paid whom, and who owns what.

It is a computer technology comprising distributed data storage, point-to-point transmissions, consensus mechanisms, and encryption. Transactions are given a unique ID based on the ID of the transaction before it and the transaction after it, which forms a chain. If a malicious actor tries to insert a different ledger it will not fit within the chain and will be rejected.

Instead of the traditional, single-entity-owned infrastructure that has the responsibility to own and manage the data (and be trusted for doing so), data in Blockchain is decentralised across multiple machines called nodes. Transactions are created and confirmed across multiple nodes, all of which have copies of the same transaction record or ledger. If a malicious actor tries to alter the ledger, then this alteration will not match the ledgers in the other nodes, and the transaction will be rejected.

Blockchain technology has gained fame through currencies such as Bitcoin, Ethereum, Dogecoin etc. initially to help human to human transactions. There is also the introduction of Smart Contracts where transactions can occur automatically once programmable conditions are met, enabling machine-to-machine transactions to take place. This can be linked with IoT devices. A high-level initial review of the legality of this suggests that IoT devices or blockchains can be allowed to transact, and suggests that the smart contract logic can also be captured in any legal contracts.

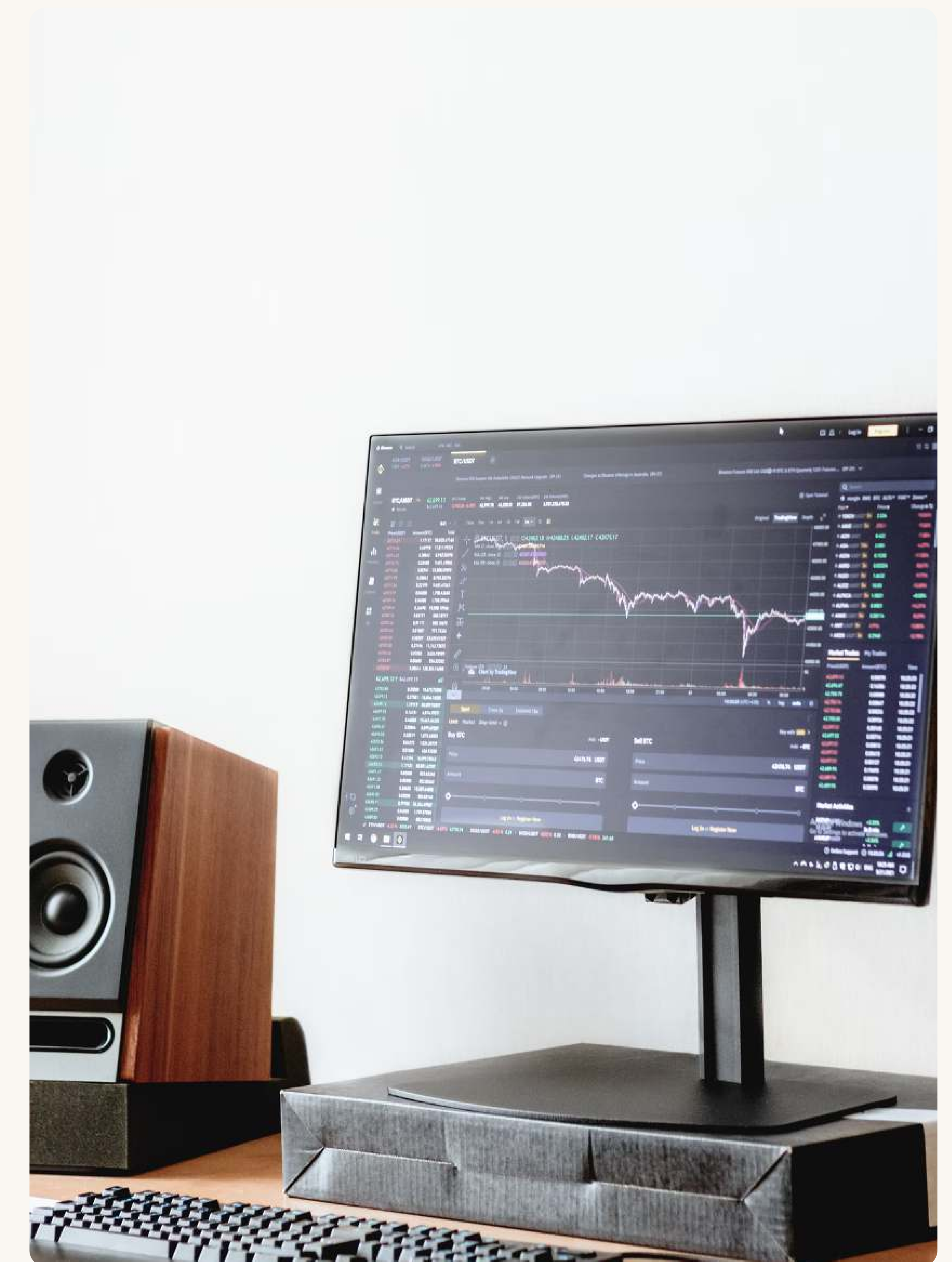
Blockchain can also be used to secure flows of data within a system, or system of multiple systems, enabling selected data to be shared safely and securely across parties.

WHERE SHOULD BLOCKCHAIN BE USED?

Despite all the recent hype around Blockchain, it is not the ideal solution for every scenario. Blockchain is useful when working in an ecosystem where trust is an issue and where it is expensive to manage checks and balances. It is less useful when you trust your partner or working with a high-performing intermediary.

Blockchain however is still growing in terms of speed – even bitcoin commonly handles only five to ten transactions per second.

Some parts of the network can still be secured using traditional methods. Blockchain is likely to be overkill for many applications especially where there are significant numbers of transactions with massive data storage requirements. Realistically, IoT devices will not be based entirely on Blockchain anytime soon, but instead will be hybrids of traditional systems that share selected information to the platform.



BENEFITS

Ownership clarity:

Having a robust shared ledger of transactions enables visibility across the supply chain. Transfer of assets from party to party can be tracked, for example, proving that a vendor really does have what they are selling.

This creates a shared single source of truth for applications in real estate transactions, education (e.g. credential fraud), supply chain (proof of provenance, anti-counterfeiting, delivery tracking, condition monitoring).



Smart Contracts

These can help ensure that once deal parameters are met (e.g. volume, delivery location, timing etc.) payment can occur automatically, building buyer/supplier confidence in the process and each other. Similarly, they can enforce penalties automatically such as penalties for late delivery. Smart Contracts reduce the human admin overhead of matching and verifying (e.g. purchase orders to payments).

Sharing of data

Permissioned-blockchains allow businesses to securely share selected data through the chain without sharing it with the entirety.

An example of this are details of products in a container moving from supplier > freight > port > customs > ship > customs > port > freight > customer, can be selectively shared with various parties, including financiers, without sharing with non-participants.

Increased trust

The difficulty of tampering with the chain makes transactions hard to falsify which helps users trust the network, reducing the need for trusted middlemen. The open nature of public blockchains takes ethical responsibility away from corporations who traditionally own single databases.



Performance history

This can potentially be shared across networks. This would allow HR to access a candidate's permanent record, security clearance etc., or a vendor's track record could be shared without disclosing important or sensitive information.

Benefits of Blockchain in CPS

Security

One of the most important benefits of Blockchain in CPS is secure transactions.

- Ensuring only approved devices can access your network. Authentication of new devices only possible through approved nodes.
- Reduces risk of malicious actors in highly safety critical activities (think self-driving cars, or actuators on highly flammable petrochemical plants).
- Sharing data privately across platforms, not in one single data centre, reduces risk of downtime from an attack.

Traceability

Transaction records can also be linked to sensors in the logistics industry. GPS coordinates can track item location to prevent re-routing to unplanned destinations, preventing things like swapping real items with counterfeit items.

Covid-19 vaccine packages are fitted with temperature monitoring devices to ensure spoiled items are not administered. Warehouses have sensors to monitor temperature at different points in the journey.

Smart Contracts

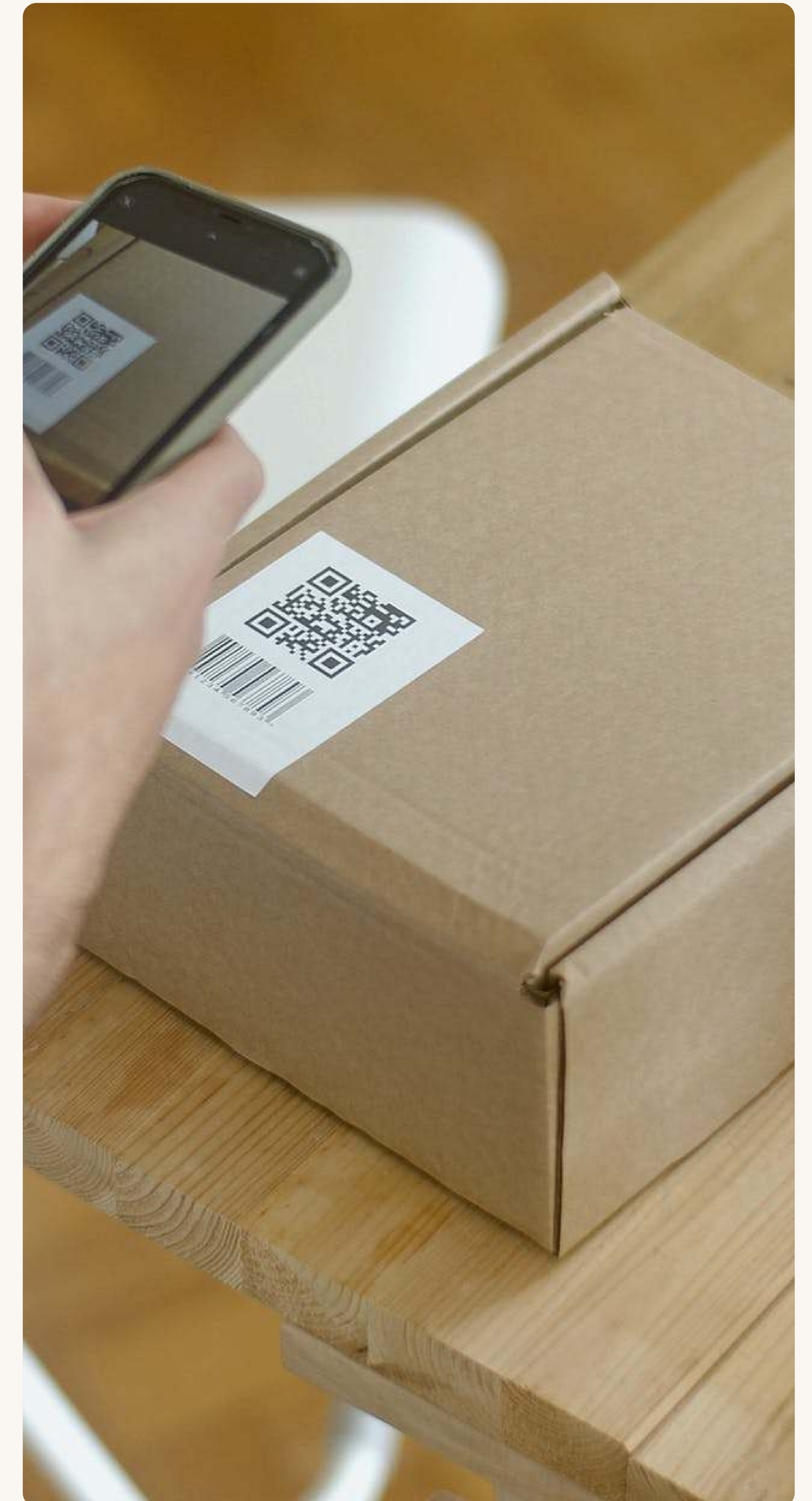
These can be paired with IoT devices to automatically execute when conditions are met. For example, a ship and port are both fitted with IoT sensors that confirm docking, automatically exchanging documents. Or vaccines arrive at their destination with full logistics and temperature history from their origin.

Data sharing

Sourcing data from multiple suppliers, such as multiple factories into a shared data pool, ensures data can't be manipulated. (E.g., trade pricing reporting). Role-based security in a Blockchain ensures that only approved participants have access to the data.

Identification

Vendors and products can be assigned unique IDs, confirming their credibility, provenance, history, performance and the like.



CPS/Blockchain products and service ecosystem

Cyber-Physical Systems are a combination of many types and layers of technologies. This section is not intended to be a deep dive into every area involved, but instead serves to illustrate some of the complexity that this industry faces.

HARDWARE

Common Sensors used in CPS

Temperature	Machinery, Crops, Cold Chain	Levels	Water in Tank
Humidity	Aircons, Heating, Weather	Accelerometers	Fitbit, Driving Fleets, Antitheft Devices
Pressure/Flow	Leak testing, Water Systems	Speed	Leak testing, Water Systems
Speed	Vehicle safety	Rotation	Fans, Turbines, Wheels
Weight	Freight contents	Altitude	Planes, Drones
RFID	Item tracking	GPS/Cell location	Traffic monitoring, Vehicle Location, Person Tracking
Image	License plate tracking	Motion sensing	Confirm worker presence
Smoke/Gas	Firefighting/safety		
Proximity	Parking lots, Warehouse Storage		

Sensors:

CPS are combinations of the mentioned hardware and more. Sensors relay information across the network. Devices are increasingly being fitted with these from the beginning, or being retrofitted with them.

Mobile phones:

These are readily available and have many of these sensors built in already making them highly suited for integration with CPS because of their touch screen / cameras / GPS chips / speakers / mics / light sensors / proximity sensors / bluetooth / NFC / wifi / 4G.

Networking technology:

MESH solutions which boost connectivity in hard to reach areas. KNL (recently acquired by Telenor) aims to create a mesh network across ships using radio waves. MIST solutions, where the sensor has some processing power built in, or FOG – or so called edge devices which process some information locally.

Security solutions:

These range from Blockchain to traditional encryption methods.

SOFTWARE PRODUCTS

Digital Twins/Cyber-Models:

This is a term common in IIoT. It refers to having a digital version of a physical item. Imagine a washing machine, for example, that has sensors that identify drum rotation speed, internal temperatures, water flow, resistance etc. These sensors are woven together to form a virtual washing machine that can be used to notify users of issues, such as adding too much soap, and remotely diagnosing problems, or anticipating servicing requirements. This concept can be applied to any machinery, or combination such as production plants.

Remote monitoring:

These are systems set up to monitor real time sensors. Plants often have control rooms to monitor sensors in real time. Trucks can be set up with tyre pressure sensors that would relay information back to a central tracking tool that would flag to the driver the need to inflate.

Connectivity management:

This helps to find ways to connect IoT devices. Local factory level wired and wifi solutions obviously exist, but range is extending to harder to reach places. 5G networks will massively boost device connectivity, and many are moving to eSIM technology. Products also include items that can create a solar-powered mesh across a whole farm or development of low-bandwidth ship-to-ship mesh networks.

Device management and tracking:

Identifying location of assets in real time requires GPS technology and tracking options.

Applications:

Multiple, usually custom, applications exist to connect and manage the various sensors or actuators to information gathering components to wired/wifi/mesh/networking to a central or cloud storage for data analysis and finally to action execution.

Data repositories:

Various options are employed depending on storage, connectivity, and processing requirements. Combinations of local/offsite/cloud storage are commonplace, but often storage and processing are done in the “fog”/“mist” where data is extensive, connectivity requires that processing is needed semi-locally before sending elsewhere.

Analytics:

These are highly-customised offerings ranging from Tableau or PowerBI dashboards to custom-developed software. Data is pulled from the various data storage options to be analysed.

LABELS, TAGS, RFID, NFC

RFID long distance labels:

Moving items around can make them hard to locate. Items such as raw materials or finished goods can be fitted with sensors to help with tracking through the warehouse or supply chain. These can be read at a longer distance like once it passes an entryway. This technology is used in Singapore in cars to help them pay for tolls using a reader with a top-up card.

Labels/tags:

Not all items can be “smart”. Most finished products are not electrical in nature, so have no opportunity for sensors to be built in. Imagine tracking the provenance of mangoes or rice. Mangoes may have a QR code that identifies their farm of origin, the part of the farm they were harvested from, the date they were picked and other information.

Label printers:

Printing unique labels, encrypted labels, nfc tags and the like requires printing technology to generate and print the required unique ID.

04

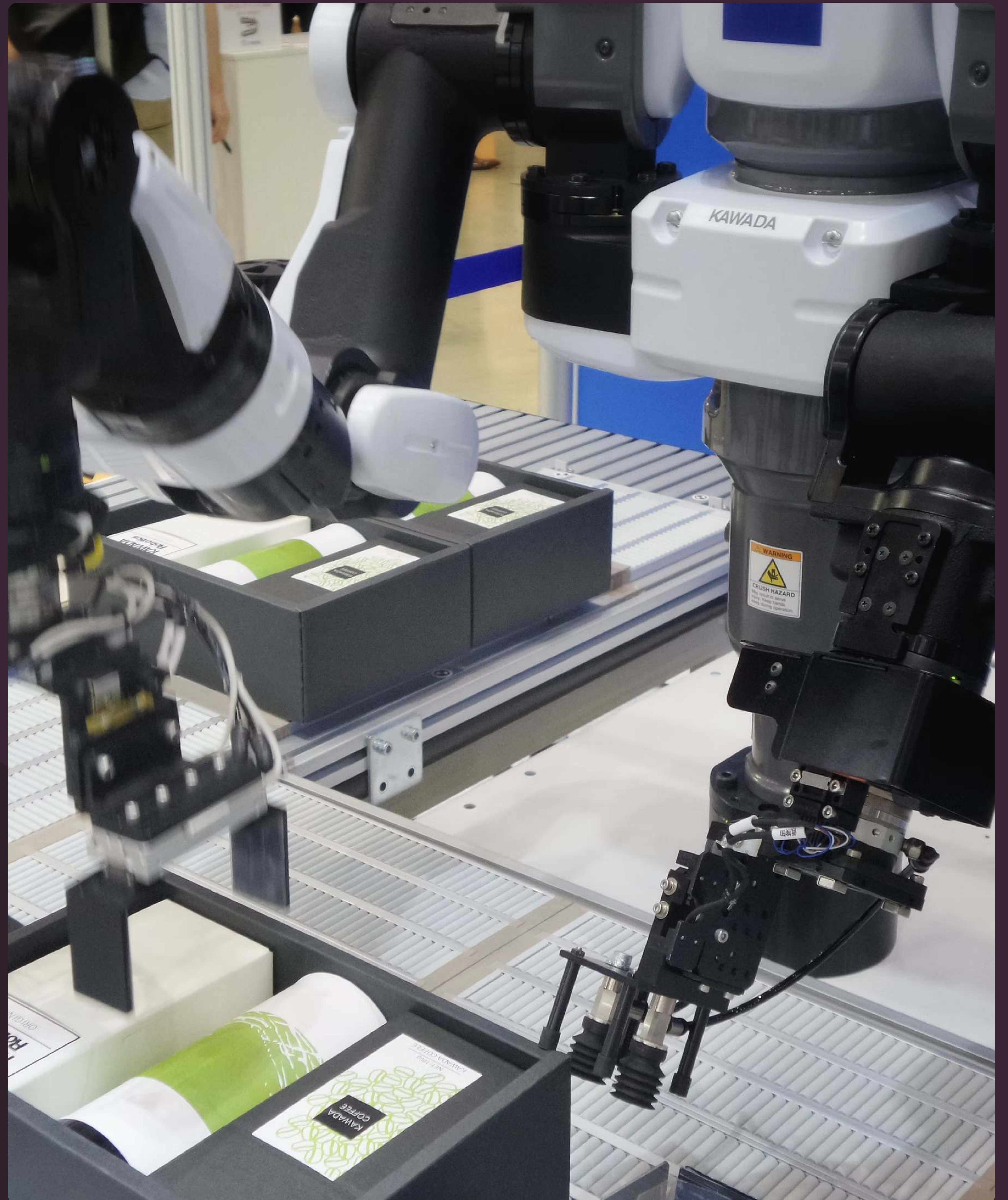
Assessment of maturity and standardisation

Summary - Maturity

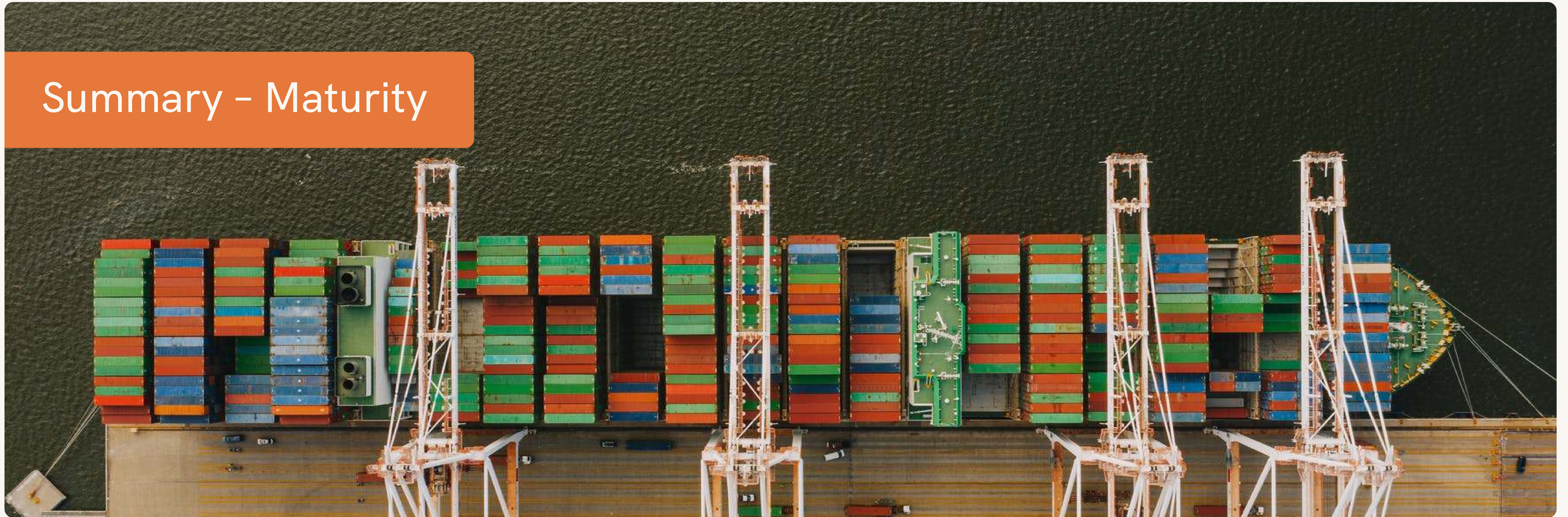
14

Breakdown - Maturity elements considered

15

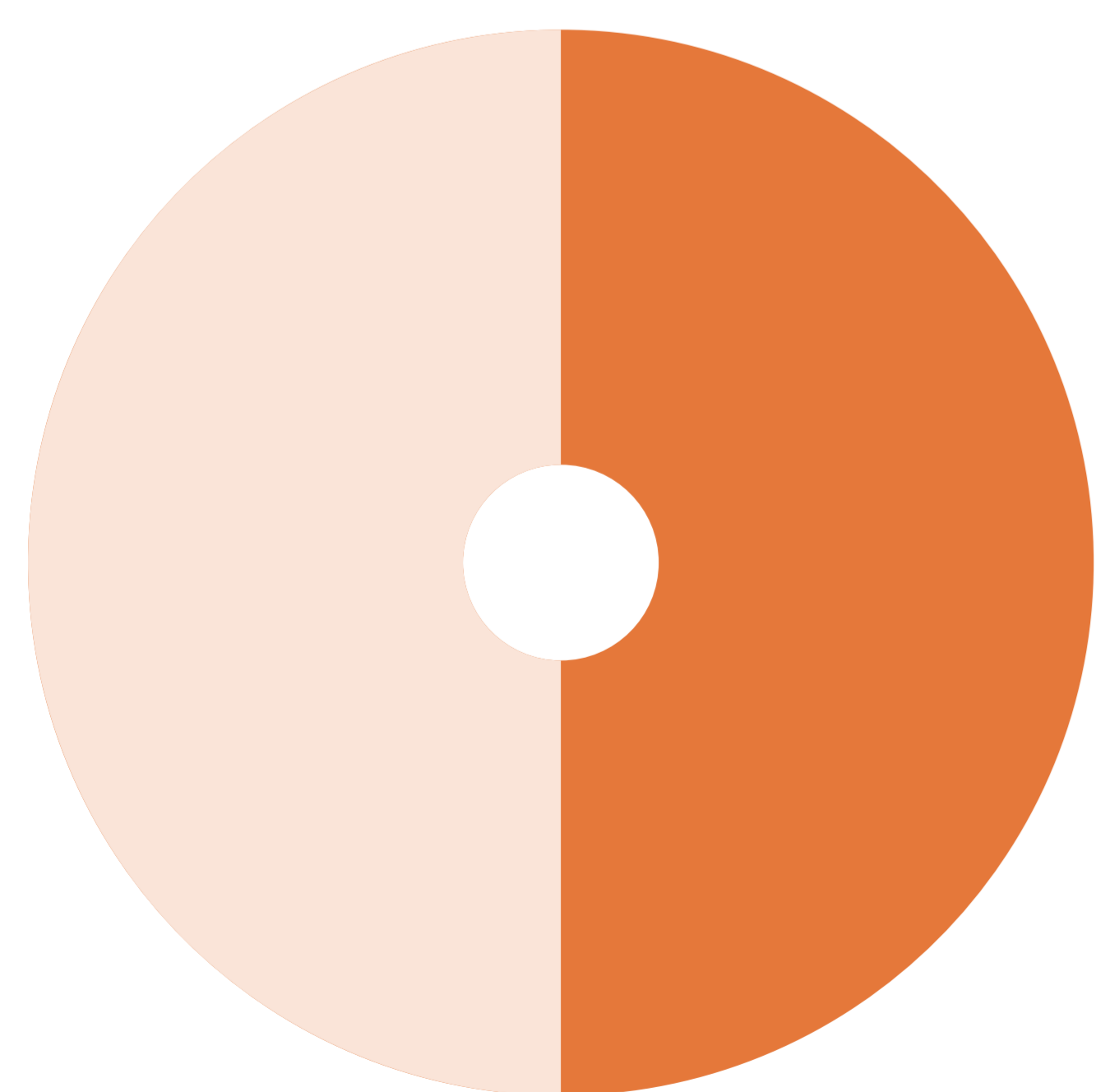


Summary - Maturity



COMMENTARY

Overall assessment



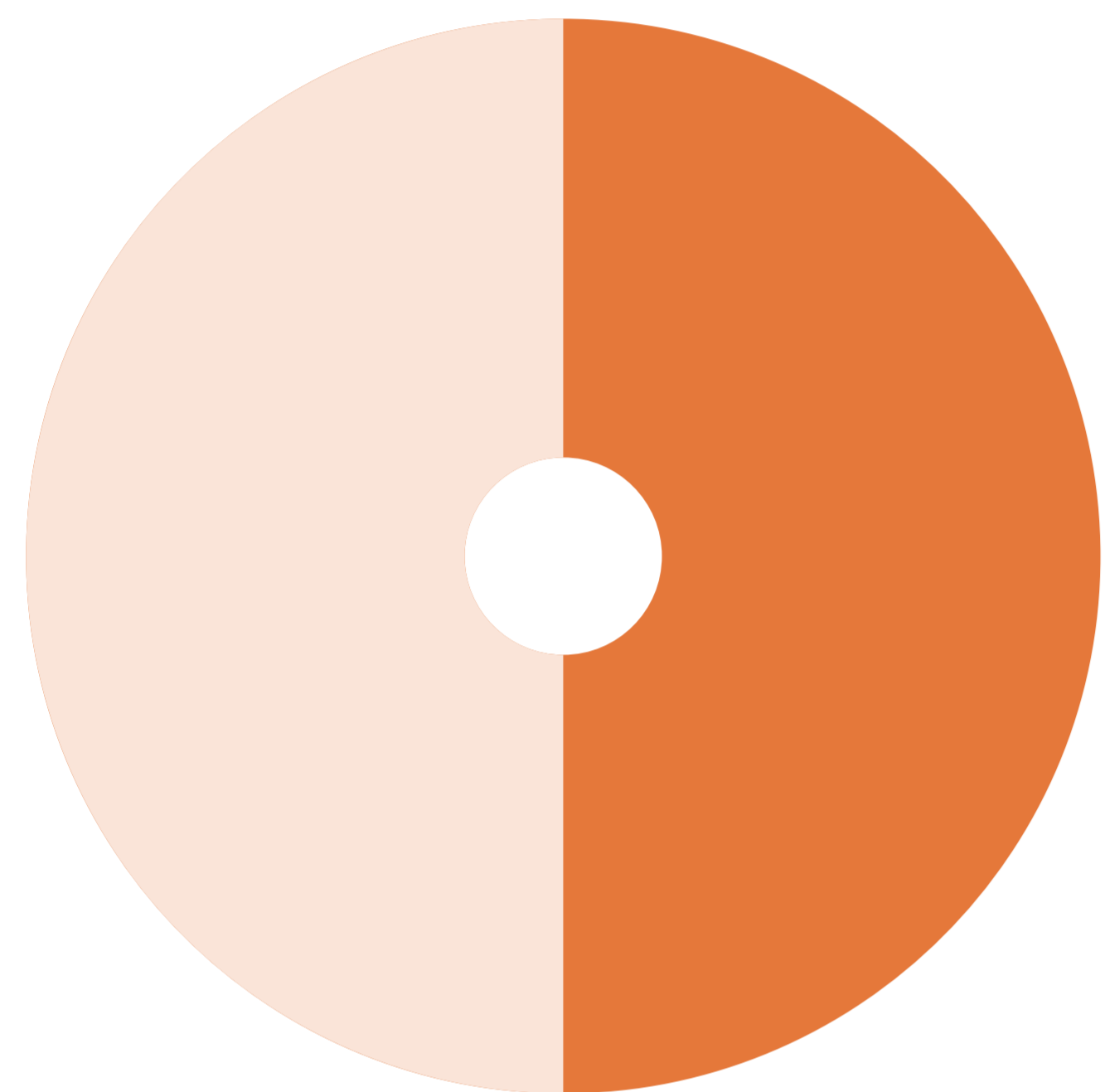
COMMENTARY

- The combination of CPS and Blockchain technologies is still somewhat in its infancy. There have been several successful implementations of both independently, but to fully leverage the benefits of them in combination will take time, as these often require significant network effects for them to be successful. Networks are forming and converging, but this will take significant investment to reap the benefits. This is also a crucial time in this evolution and is gaining critical mass in a network ecosystem that can mean it becomes a winner-takes-all scenario. In general, the combination is still in early stages with no clear standards yet established.
- Logical progression suggests that a dominant Blockchain needs to be established first, and then the process of fully integrating CPS data into it can occur. It is too risky for factories to do so otherwise.
- Trade however is slightly ahead of the curve, as data processes and roles are very clearly defined, and has enabled some major players (Maersk, IBM, Walmart) to define a way forward as they build their own Blockchain networks. These standards are paving a path for IoT integration, developing some common standards for paper processes, a critical step towards integrating CPS.

Breakdown – Maturity elements considered

ELEMENT

Ecosystem buy-in

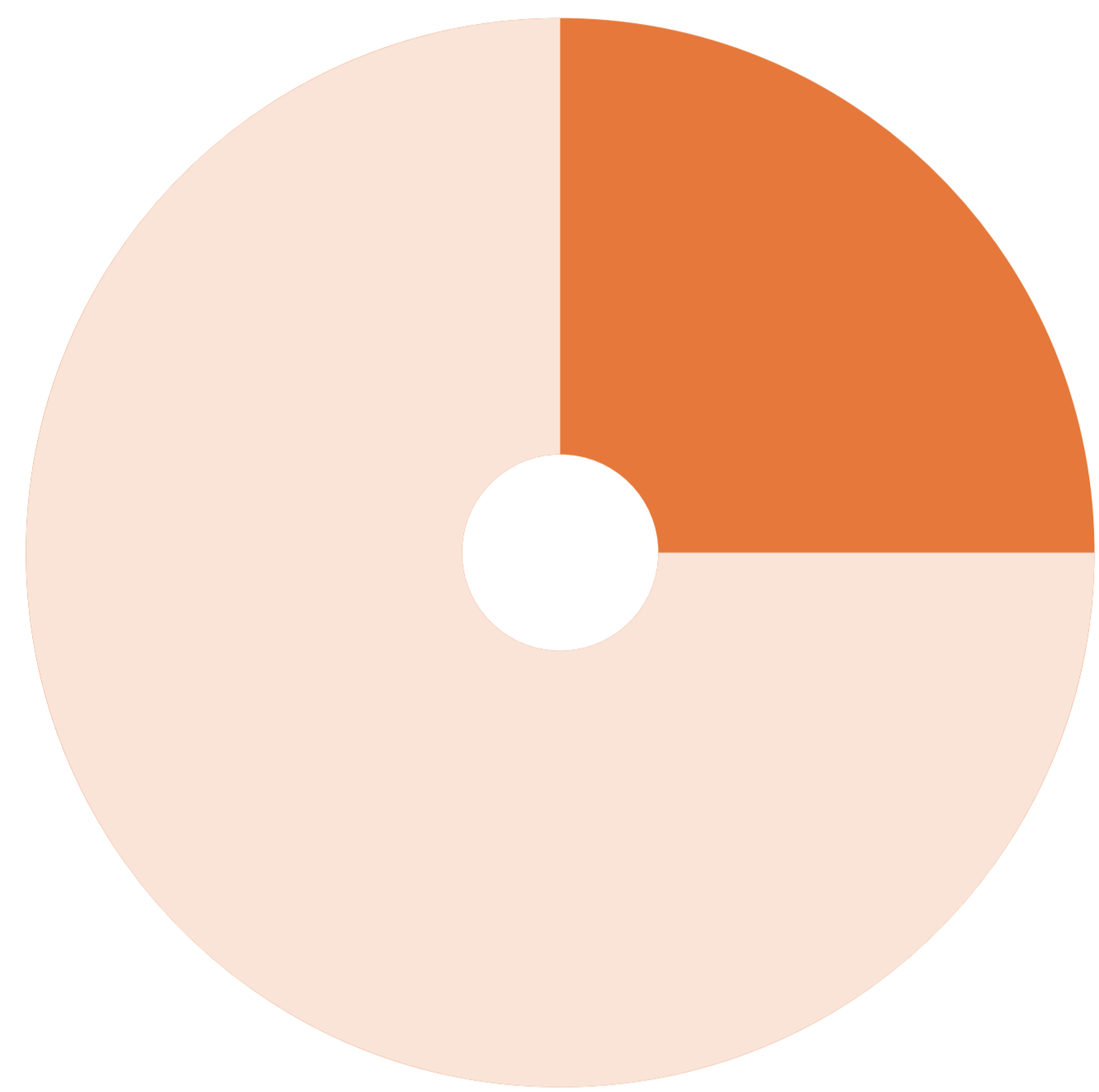


COMMENTARY

- IoT standards are still developing, and most suppliers are still not as smart as they could be. Most of the opportunity is still in building lean capabilities before they go for full IIoT. Most factories are not sharing their data externally in an integrated fashion. For example, sales forecasts are commonly shared manually.
- Blockchains are subject to significant network effects which need to be surmounted before the costly and complex process of integrating layers of CPS. Diversity of technologies and standards, and integration challenges, means that investing in connecting their IoT devices to an emerging Blockchain can be risky unless a significant number of useful participants have already joined.
- The challenge further exists that building a Blockchain would require investment, typically by organisations. Participants become concerned about the ecosystem's autonomy when it is in the hands of private institutions and are reluctant to join. This was seen with Tradelens, started by IBM and Maersk, who found it hard to get participants to join until they made it into a partnership.
- Global Trade, led by shipping, is in a slightly better position here than most other industries. The logistics and shipping process is somewhat standardised globally and has several major players that dominate. This has enabled Maersk to rally the industry and has spearheaded IoT standardisation initiatives through the DCSA and Blockchain adoption through TradeLens.
- Likely, initial successes in this space will be government initiatives which can implement nationwide standards. Kenya's customs and border management is a good example of this. Players with significant power to influence the market such as IBM Food Trust, with Walmart can also assist with establishing these standards.

ELEMENT

Ease of implementation

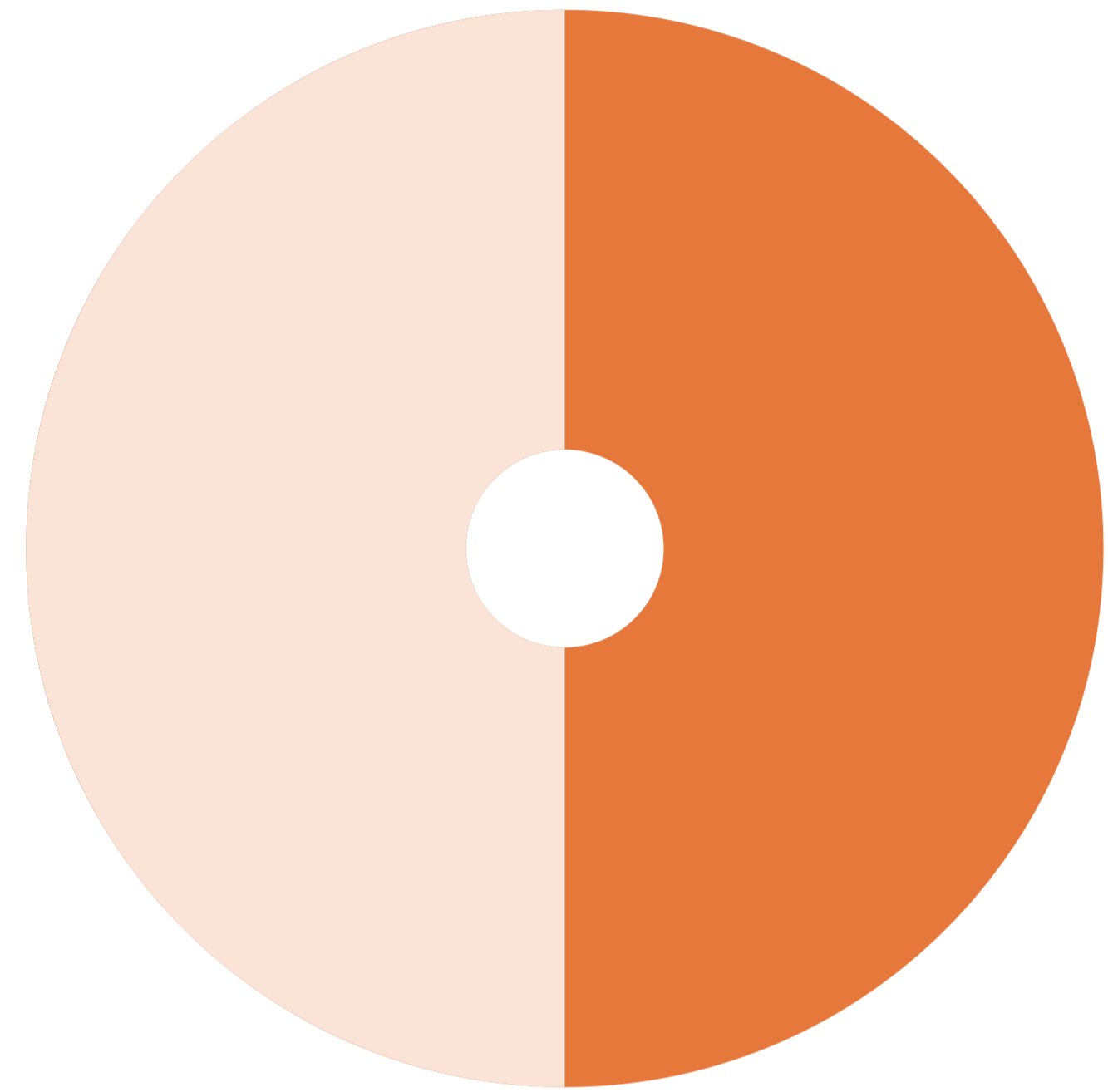


COMMENTARY

- Multiple disciplines involved have no standard language throughout. Diversity of data capture methods such as simple things like a timestamp format or sync frequency have yet to be established. Control schemes could be local, distributed, federated, centralised. Single and multiple source data and implementations that involve integration with multiple layers of legacy systems, ERP tools etc. can be hugely complex system integration projects. Implementations are often recognised tech experts running custom projects such as Accenture, IBM, Deloitte and others.
- Simplifying CPS integration complexity requires a new approach that allows different disciplines to work together without forcing each of them to learn the technology of the other. Some efforts are being made here (see Appendix for some of the many efforts to develop common standards). Industries where some success is being seen are where major players have weighed in to drive development and adoption of standards. Maersk, IBM, Walmart again are leading the way here. So far, no dominant technologies or protocols exist for fully-integrated CPS solutions.
- IoT standards are still developing, and most suppliers are still not as smart as they could be. Most of the opportunity is still in building lean capabilities before they go for full IIoT. Most factories are not sharing their data externally in an integrated fashion. For example, sales forecasts are commonly shared manually.
- Blockchains are subject to significant network effects which need to be surmounted before the costly and complex process of integrating layers of CPS. Diversity of technologies and standards, and integration challenges, means that investing in connecting their IoT devices to an emerging Blockchain can be risky unless a significant number of useful participants have already joined.
- The challenge further exists that building a Blockchain would require investment, typically by organisations. Participants become concerned about the ecosystem's autonomy when it is in the hands of private institutions and are reluctant to join. This was seen with Tradelens, started by IBM and Maersk, who found it hard to get participants to join until they made it into a partnership.
- Global Trade, led by shipping, is in a slightly better position here than most other industries. The logistics and shipping process is somewhat standardised globally and has several major players that dominate. This has enabled Maersk to rally the industry and has spearheaded IoT standardisation initiatives through the DCSA and Blockchain adoption through TradeLens.
- Likely, initial successes in this space will be government initiatives which can implement nationwide standards. Kenya's customs and border management is a good example of this. Players with significant power to influence the market such as IBM Food Trust, with Walmart can also assist with establishing these standards.

ELEMENT

Security

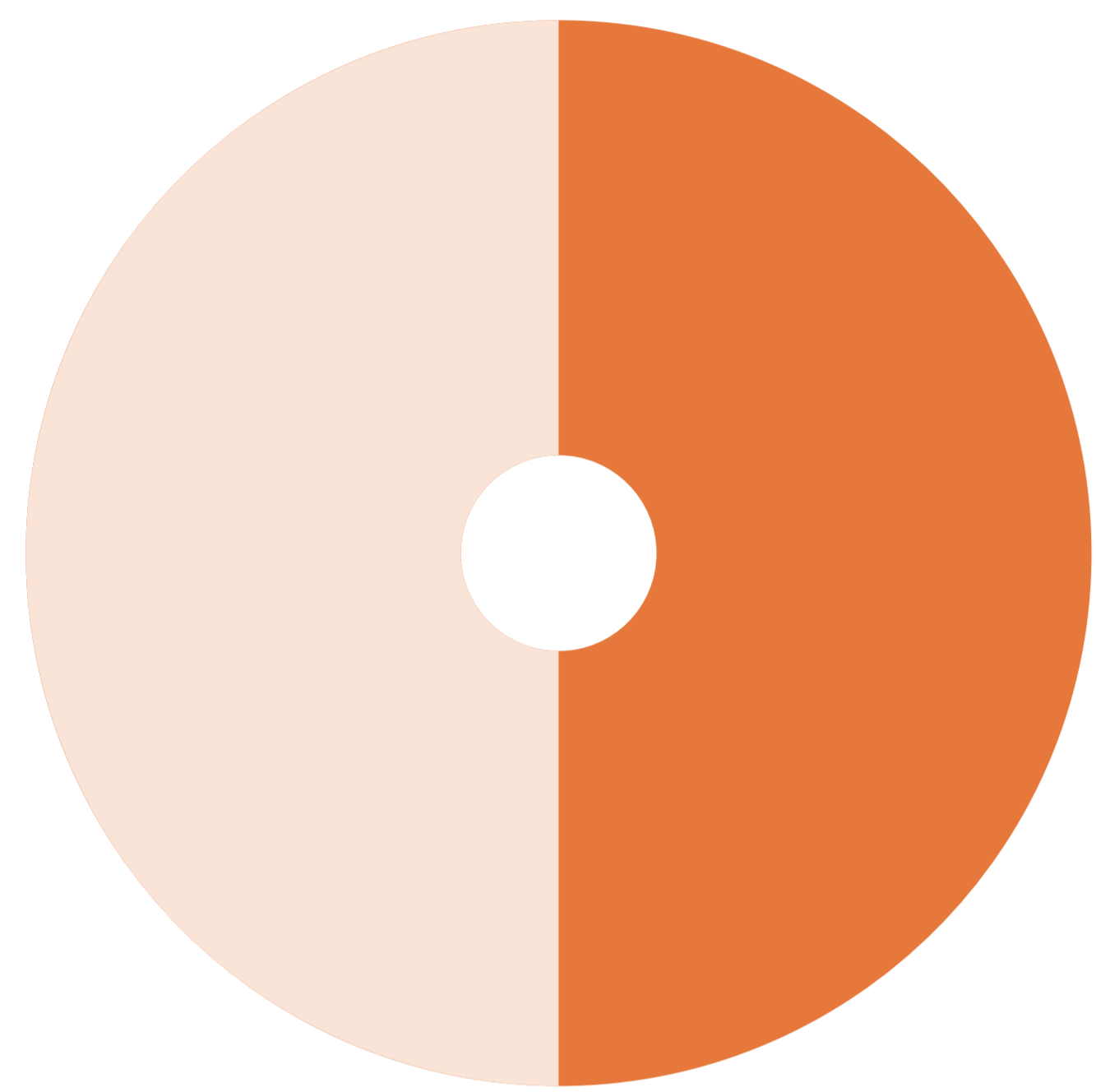


COMMENTARY

- The key security challenge here is that IoT devices are, by design, very simple devices. They are not designed with any innate security features. While they can be built to include blockchain-compatible security, the lack of dominant blockchains or IIoT standards makes it hard to justify for device producers.
- Increasing number of IIoT devices creates an increased number of points of vulnerability. Blockchain, while very secure, is still potentially vulnerable. To alter the chain, a malicious actor would need to control 51 percent of the nodes, within ten minutes (for bitcoin).
- Vitalik Buterin, co-founder of Ethereum, discusses the Scalability Trilemma in which only two of the three properties of decentralisation, security, and scalability can be achieved. The higher the number of transfers means the higher the amount of data stored. As this stored data increases, nodes will reach capacity, and so only a few larger nodes will be able to store transactions which reduces the number of required nodes a malicious actor would need to compromise. Private blockchains don't face this trilemma.
- GDPR legislation means that data on individuals can not be stored on a blockchain. The laws require that individuals have the Right to be Forgotten which means it can't be on a ledger that can't be changed. That data on EU individuals cannot leave the EU which means it can't be stored on a network of globally distributed nodes. This means that it must be stored on a traditional database. Imagine KYC processes and documents being stored, like documents with reference to an unapproved status. This status could be hacked, then changed to approved and transactions can occur. There are potential solutions to this provided data is encrypted correctly.
- Hackers are finding creative ways to cheat. The Selfish Miner approach aims to keep other nodes busy solving already solved crypto puzzles, while the hacker adds new transactions to nodes of which they have already taken control. An Eclipse Attack involves taking control of the communications connecting the nodes by either wasting their time or feeding them fake transactions without the ability to corroborate. A Double Spend attack leverages the time it takes to fully confirm a transaction, which took 40 minutes in 2018, and spends coins twice.
- Implementing blockchain correctly is critical to ensure security especially when considering a mixed network such as IIoT devices on a traditional network that relays information to a blockchain. Even when developers use tried-and-tested cryptographic tools, it is easy to put them together in ways that are not secure.
- IoT devices are, by design, very simple. There is no standard security platform for them to align, instead they rely on their implementation. They are highly vulnerable to DDOS attacks which isolate them from the network of nodes and alter the network's view of their status. Failures tend to take place wherever blockchains connect with the real world such as software clients and third-party applications.
- In the 2018 500-million-dollar Coincheck hack, Hot Wallets exploited internet-connected applications stored in traditional databases used for storing cryptographic keys that crypto-currency owners needed to spend money.
- Smart Contracts that provide the ability to build programmable logic into blockchain transactions led to the theft of 80 million dollars of Ether from the Decentralized Autonomous Organization (DAO) fund. Hackers can intercept the software programmed logic by rerouting funds among other tactics, and still mark the blockchain transaction as successfully completed.
- Addressing these challenges with IoT devices becomes harder. IoT devices tend to have limited capabilities. The transactional cost of verifying every data entry may limit the interactions needed to capture the data correctly.

ELEMENT

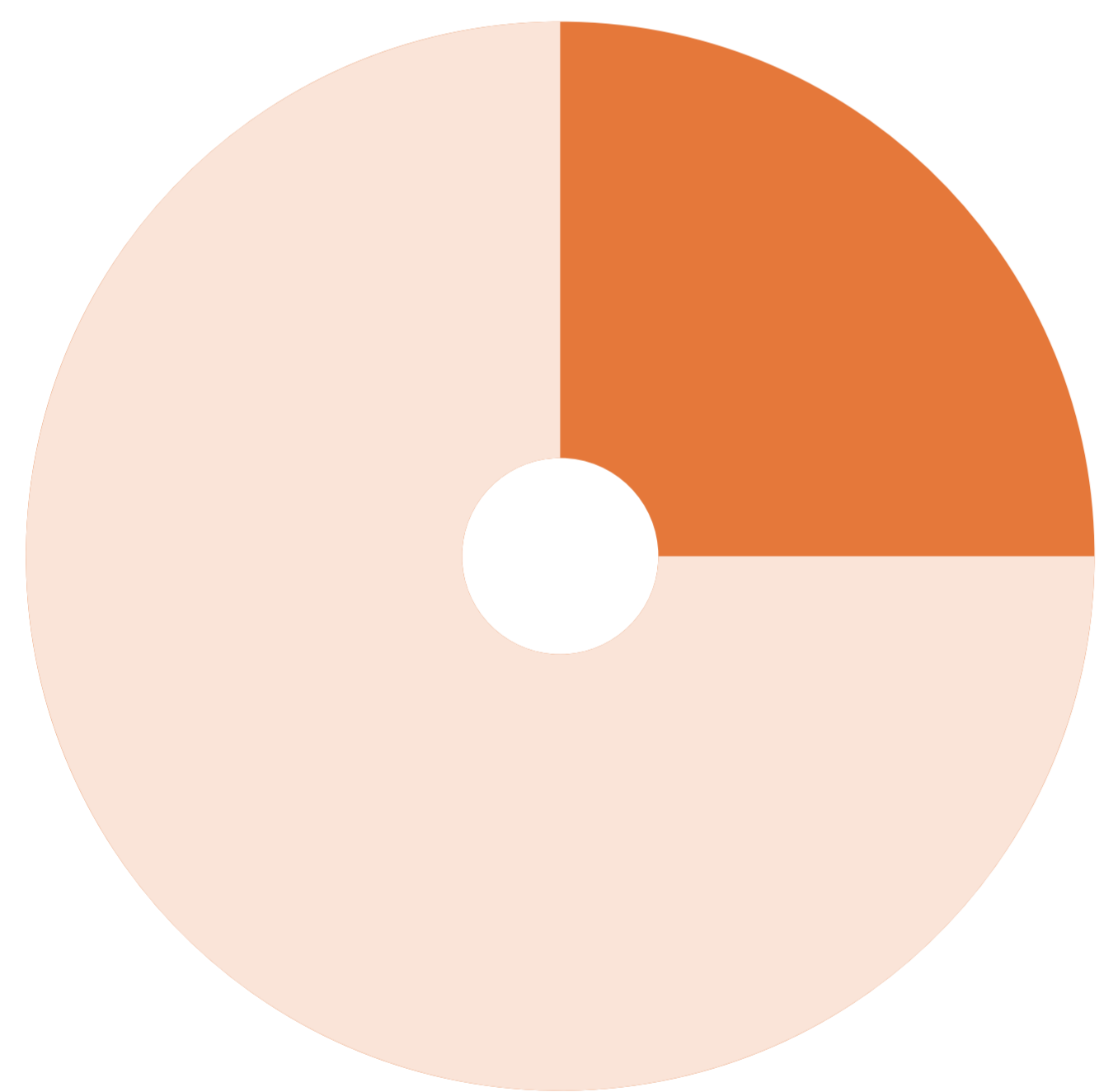
Efficiencies







COMMENTARY

- Benefits case for CPS is clear (5-15 percent according to McKinsey). CPS and Blockchain combinations are highly dependent on the network effects needed for ecosystem buy-in. The efficiency case for CPS is clear. Better integrated systems result in less manual labour, fewer mistakes, safer processes and more. Industry 4.0 is under way, but still with plenty of room to improve. Legacy equipment often still not informatised – setting machinery up to capture information is costly. Building Digital Twins, otherwise known as virtual versions of a physical machine, need a clear vision of desired analysis before embarking on or capturing it.
- The CPS/Blockchain benefits make sense for industry. But much work is needed before they can be fully integrated. In the case of trade financing, for example, much of the effort is currently in the digitalisation of manual processes – a requirement before CPS devices can really maximise the impact through the chain. Some markets are moving in this direction, especially with logistics and shipping, and there are opportunities to enhance those that have already digitised their financing.
- Payments can be automated through Smart Contracts and IoT devices, but need an adopted Blockchain.

Trust



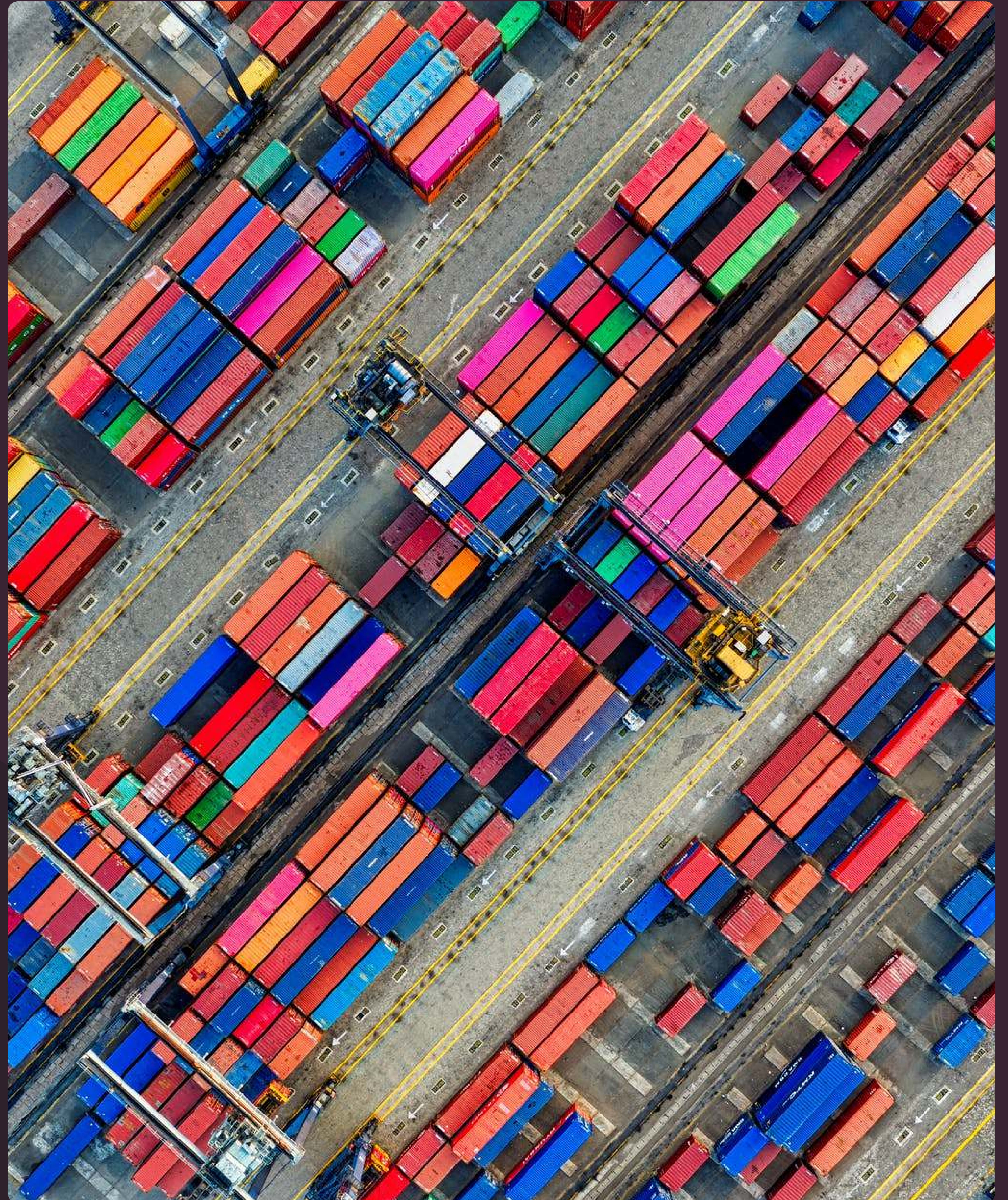
- People have become used to trusting platforms with their data even with increasing privacy concerns. Organisations still have some way to go before they easily share their data with others.
- Blockchain can indeed help keep data secure, it can still be exploited if not implemented correctly. For companies to share their data with others there needs to be clear benefits to doing so, which might not be apparent to the data providers.
- In many cases, the need for Blockchain may also not be evident, when there are other platforms already doing similar activities.
- Security is critical in manufacturing, where breakdowns can cause significant financial and safety damage if hacked. A good example of this is a mini-manufacturing plant or flammable BP assets.
- Connected cameras and sensors are connected to form Digital Twins of the equipment which is sensitive IP if it falls in the hands of the competition. Information brokers within the chain need to be robust.
- Anticounterfeiting measures are not online all the time. How do we know that just because supplier B bought from supplier A , that supplier B isn't selling the counterfeit on Blockchain and reselling the original elsewhere?
- Permissioned Blockchains enable the ability to reveal only certain specified fields to the chain and to certain users.
- For individual identity related Blockchains, General Data Protection Regulation (GDPR)-style legislation requires that users have the Right to Erasure, or the right for their data to be forgotten which works against any individual performance records use cases.

ELEMENT	COMMENTARY
<p>Cost of devices</p> 	<ul style="list-style-type: none"> • The cost of sensors is decreasing for both consumers and businesses, but the sheer variety of options is making it harder to gain economies of scale. Applying some form of standard components and designs can help to achieve this. This has been commonplace in China for decades before IoT, with the government sharing certain core designs. • The average price of an IoT sensor has declined from \$1.30 in 2004 to \$0.44 in 2018, according to Microsoft's "2019 Manufacturing Trends" report.
<p>Suitable human interfaces</p> 	<ul style="list-style-type: none"> • Sufficient technologies exist to create suitable interfaces to view or control sensors. • Plenty of data visualisation tools exist that can interpret captured data. Businesses often lack the ability to really track correct metrics that would maximise value. Controlling actuators can happen, even based on sensor data. Implementations tend to be highly customised and therefore expensive, and often miss useful data to track and are then expensive to customise post-implementation.
<p>Operating costs</p> 	<ul style="list-style-type: none"> • Once established, additional running costs can be low. The main expense is in the supplier's maintenance or upgrades of the system. Sensors are low cost. As with any IT implementation, if not fully scoped or defined it can be expensive to customise later.
<p>Connectivity</p> 	<ul style="list-style-type: none"> • Traditional CPS networks within the factory fence involve centralised data centres. Instead of having dumb sensors that connect to the cloud, some processing can be done in the sensor itself, or using Fog or Mist networks to process on the edge of the local network before syncing to the cloud which reduces bandwidth requirements. • IPv6 is now commonplace and is more suitable to handle more devices and 5G is rolling out. These will be pivotal to enabling IoT connectivity. Certain applications make connectivity harder, like sea vessels, or remote agriculture fields, however there are many mesh applications being developed to extend connectivity. Blockchain applications however require reliable, accessible storage nodes. Reliable farms are evolving to meet this need. • Multitude of mesh/Mist/Fog. Blockchain speed is still an issue for many implementations, but can be controlled by a private Blockchain at the risk of Trust.

05

CPS and blockchain use cases

Insurance/financing - Consumer	P21
Pay per use - Financing and insurance	P22
Supply chain	P25
Logistics	P26
Agriculture	P27
Data sharing	P28
Identity Wallets for individuals and equipment	P28
Facilities management	P29
Energy	P29
Infrastructure	P29



Insurance/ financing - Consumer

MYBIT: SHARED OWNERSHIP OF E.G. CARS

Plans to build an ecosystem of services where IoT assets, from drones to cars, are owned by a group of people and the revenues are shared.

A new financing model and investment opportunity open to anyone. Ethereum Smart Contracts are used to automate processes: when the IoT devices generate revenue the investors automatically receive a share of the profits proportionate to their ownership stake. A central Smart Contract is responsible for the control, maintenance and updating of the platform. The platform defines different asset types, and IoT devices are linked to assets, once installed they send and request information through an API. Oracles are used to connect devices to the network.

CAMBRIDGE MOBILE TELEMATICS - USAGE BASED INSURANCE

Metromile / Cambridge Mobile Telematics have pay per mile car insurance policies in association with American Family pay per use insurance / Liberty / Admiral

American Family Insurance has partnered with Cambridge Mobile Telematics (CMT), a smartphone telematics company, to create the MilesMyWay auto insurance program that rewards drivers for driving less. Customers fix a CMT sensor in their car, and an app on your phone tracks mileage/driving behaviour – offering discounts up to 25% per month. No penalties, only rewards (however data could potentially be used to calculate next year's premium).

They have a software development kit to help insurers build apps tailored to their offering. Options include a crash detector for real time crash alerts. They also have fleet insurance offerings, to track driver performance. Reuters previously estimated that around 50m US drivers have experienced IoT related insurance.

BEAM DIGITAL: SMART TOOTHBRUSH DENTAL INSURANCE

Beam Digital provides a smart toothbrush to every customer and monitors their oral health, as well as using this information to support a dental insurance plan. Beam sends the customer notices and encouragement if their brushing habits are falling short of the required standard, and hopes this will result in improved dental hygiene — and reduced premiums. The company's insurance plan gives away a toothbrush to each member, and hopes to reduce the cost of premiums by up to 25 percent.

HOMESERVE LABS

HomeServe Labs has formed partnerships with insurers such as RSA, Aviva and Legal & General, who provide its connected water leak detector, LeakBot, to customers to help them identify and fix small water leaks before they become major loss events. German appliance manufacturer, Grohe, has taken the concept a step further with a smart water controller that can automatically cut off the water supply if a leak or burst pipe is detected.



JOHN HANCOCK – LIFE INSURANCE BASED ON FITBIT USAGE

Interactive life insurance, pioneered by John Hancock’s partner the Vitality Group, is already well-established in South Africa and Britain and is becoming more widespread in the United States.

Policyholders score premium discounts for hitting exercise targets tracked on wearable devices such as a Fitbit or Apple Watch and get gift cards for retail stores and other perks by logging their workouts and healthy food purchases in an app.

In theory, everybody wins, as policyholders are incentivized to adopt healthy habits and insurance companies collect more premiums and pay less in claims if customers live longer.

Privacy and consumer advocates have raised questions about whether insurers may eventually use data to select the most profitable customers, while hiking rates for those who do not participate. The insurance industry has said that it is heavily regulated and must justify, in actuarial terms, its reasons for any rate increases or policy changes.

LIBERTY MUTUAL + GOOGLE NEST

Liberty Mutual has partnered with Google’s Nest to implement connected smoke alarms in the home, enabling customers to reduce the risk of a fire, and in turn reduce their home insurance premiums.



Nest tells the customer where there’s smoke or carbon monoxide, gives alerts on their phone, while the Split-Spectrum sensor looks for fast and slow-burning fires.

Liberty sends these \$99 Nests out to customers free of charge, and will take up to five percent off customer insurance premiums once installed. This is a great example of IoT in insurance pushing insurers to increasingly become lifestyle companies or advisers.

Pay per use – Financing and insurance

PARSYL – TECHNOLOGY ENABLED CARGO INSURANCE

April 2020: Parsyl, a US-based supply chain data platform, raised \$15m in Series A (led by Ascot Group/Lloyds) for the launch of ColdCover by Parsyl Insurance, a suite of connected cargo insurance products for perishable goods powered by its IoT data platform.

“

As the only integrated supply chain visibility and cargo insurance solution, Parsyl has created a data-driven insurance offering that is simple, transparent, and fast, including the industry’s first and only parametric spoilage policy, protecting against losses due to temperature.”

Parsyl’s cargo insurance suite gives shippers of perishable goods the coverage, predictability, and protection they need for their products’ most significant risks

Several device types listed – “Trek” devices track temperature, humidity, light, impact and GPS. Parsyl claims they have unmatched accuracy and operating range, with a multiyear battery life. Web platform integrates package location and weather data to understand events in real time.

Devices can stay there all the way from their origin. “Tracktab” device (\$10) has a “status” button which, when pressed, flashes green or red. There’s an option to review data by scanning the code, or throwing device in a “Smart Bin” which reads it automatically and uploads to a platform. Web platform shows temperature throughout the journey.

The ColdCover product suite includes:

- ColdCover Parametric: Single Peril transit cover for spoilage due to temperature. Parametric policy: entirely driven by sensor. Define custom “catastrophic” events and provide options for immediate payout, or provide visibility of number of shelf days lost (delays etc.).
- ColdCover Buyback: Deductible Buyback for All Risk transit and STP policies.
- ColdCover Transit: All Perils cargo policy for theft, loss or damage to products in transit.
- ColdCover Stock + Transit All Perils cover for theft, loss or damage to products in transit and/or stored in inventory.

They are licensed to offer cargo insurance products in Alaska, California, Colorado, Louisiana, Maine, Massachusetts, Oregon, Texas, Virginia, Washington and the United Kingdom.

Currently they are also exploring ways to offer cover for vaccine delivery with Lloyds of London.

RELAYR: MUNICHRE AND TRUMPF

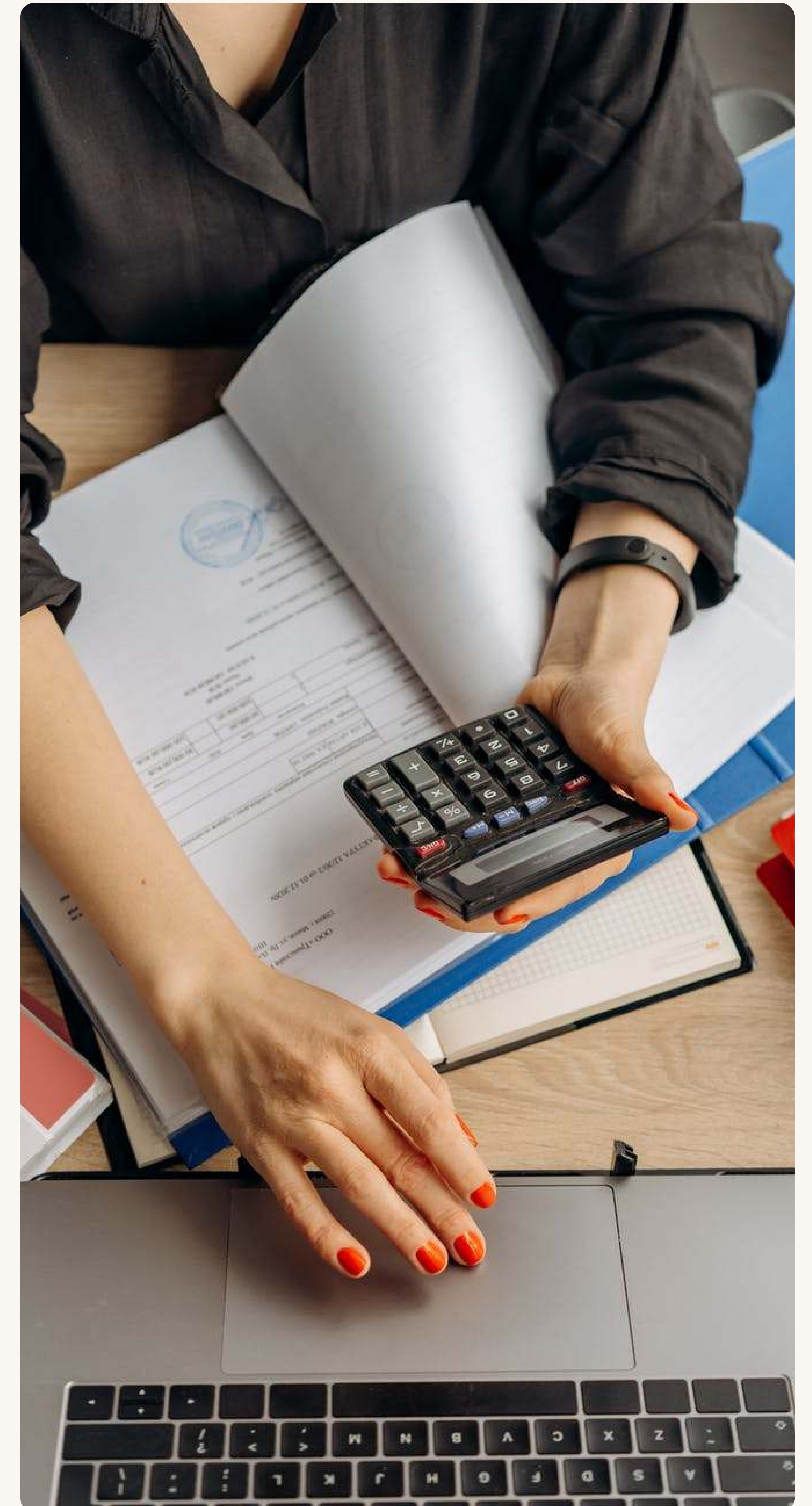
Oct 2020 starting a pilot project with Trumpf to enable Trumpf to provide their customers with a “pay per part” model.

Relayr (via MunichRe) finances the entire machine, paying the seller, then invoices the buyer on an output basis- Relayr finances the machine and bears the investment risk.

Customers pay a previously agreed price for each cut sheet metal part generated by the IoT devices – which feeds data to Relayr’s platform.

Relayr is an IoT/data consolidation specialist with their own tech stack that claims to be the “only IoT company capable of insuring business outcomes”.

They also provide insurance/guarantees against potential production downtime. Moving companies from Capex to Opex solutions.





ERSTE GROUP / LINX4: INDUSTRIAL IOT FINTECH

This combination of tech and finance is helping machinery OEMs to provide “pay per use” or “pay per outcome” financing services. The seller receives full payment, from the financier, for the item sold. Buyer pays per use (e.g. on the number of items produced by the machine).

IoT sensors track usage, send the information securely to the Linx4 Blockchain platform, and send the same information to both buyer and seller. The Linx4 platform tracks usage and relays.

IOT CONNECTIVITY AS A SERVICE

SPTTEL – creating a “backbone” for IoT devices to connect to, to enable data exchange and joint development, charging in a similar way to Amazon AWS.

ROLLS ROYCE “POWER BY THE HOUR”

The original concept was to pay only for engine uptime, i.e. a fixed cost per hour (net of purchase costs, maintenance etc.). As soon as an engine stopped working, Rolls Royce was incentivised to fix it asap.

Whilst this concept has been around for many years, it has been augmented recently with the addition of sensors to better anticipate when an item is likely to fail, to minimise disruption.

ALLIANZ FRANCE

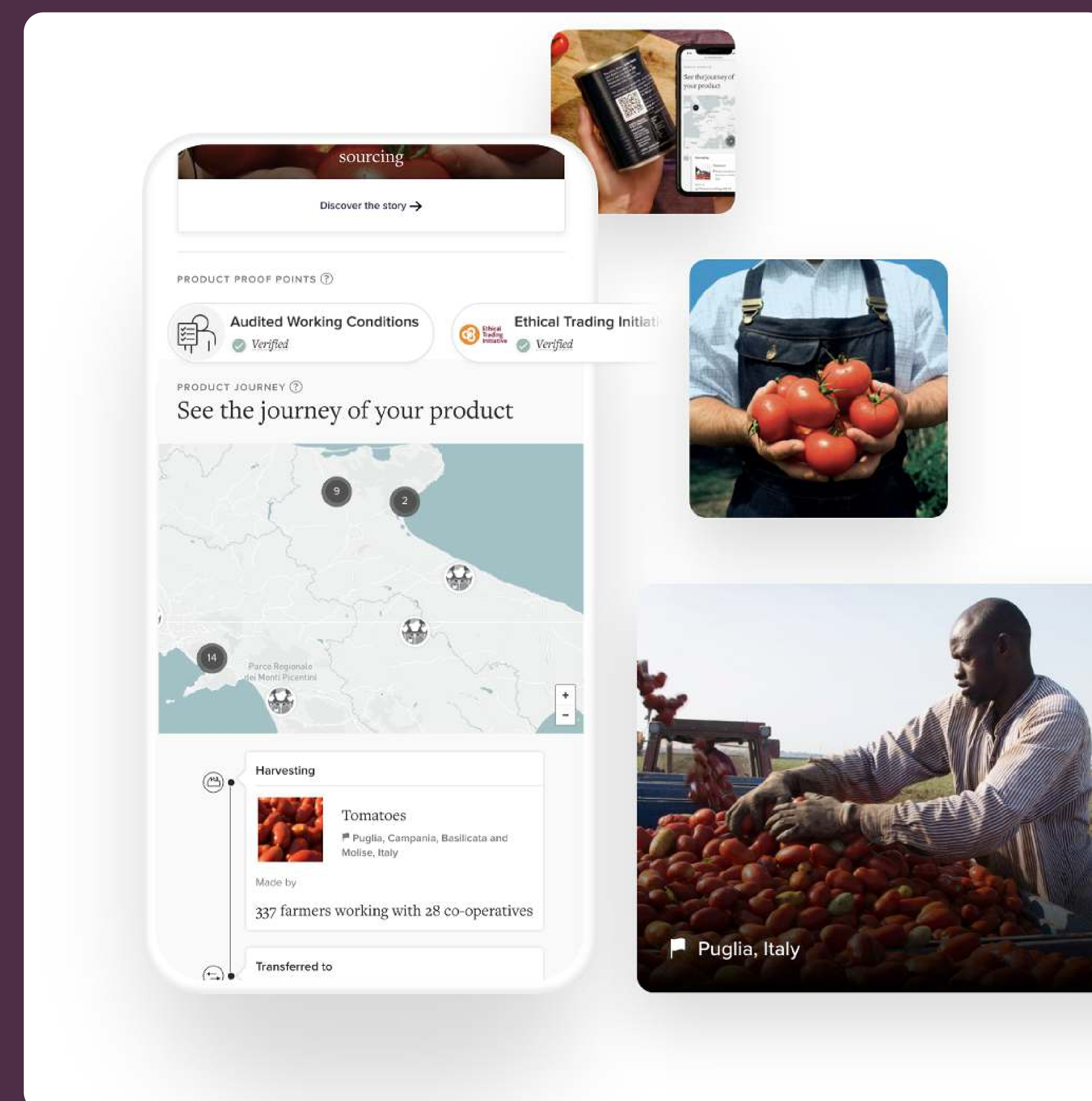
Allianz France and its partners have developed connected tools that continuously monitor construction sites for risks such as fire hazards, short-circuiting and building deformation as part of a digitized insurance offering for the construction industry.

Supply chain

PROOF OF SOURCE: PROVENANCE

Provenance aims to stop “greenwashing”, by providing transparency into whether a product genuinely meets its claims, to help consumers know if a product has a positive impact on people and planet.

Online marketplaces can enable their tagging system. Alternatively, individual SKUs can have QR codes which explain exactly where the products are sourced from (e.g. responsible fishing), in a trustworthy manner.



PROOF OF SOURCE: EVERLEDGER - DIAMOND MARKETPLACE

Everledger enables the tracking of diamonds provenance, so that consumers can ensure that their diamond is not associated with a conflict zone. Diamonds are scanned to measure their unique dimensions and shape, and a digital trail of ownership is established.

IBM / WAL-MART “IBM FOOD TRUST”

The IBM Food Trust is a collaborative network of growers, processors, wholesalers, distributors, manufacturers, retailers, and others, enhancing visibility and accountability across the food supply chain. Built on IBM Blockchain, this solution connects participants through a permissioned, immutable and shared record of food provenance, transaction data, processing details, and more. 11 members initially in 2018, had grown to 80 by 2019 and stood at 300 members and 6 million products by July 2020 (Forbes).

These kinds of applications require minimal sharing of information: Purchase orders, invoices, and payments do not need to be included on the same Blockchain. As a result, companies that are wary of sharing competitive data are more willing to participate on the platform.

The benefits are clear. If a company discovers a faulty product, the Blockchain enables the firm and its supply chain partners to trace the product, identify all suppliers involved with it, identify production and shipment batches associated with it, and efficiently recall it. If a product is perishable (as fresh produce and certain drugs are), the Blockchain lets participating companies monitor quality automatically: A refrigerated container equipped with an IoT device to monitor the temperature can record any unsafe fluctuations on the Blockchain.

And if there are concerns about the authenticity of a product that a retailer returns, the Blockchain can allay them, because counterfeit goods would lack a verification history on the Blockchain. Companies across industries are therefore exploring this application of Blockchain, motivated either by regulations requiring them to demonstrate the provenance of their products or by downstream customers seeking the capability to trace component inventory.

VACCINE DISTRIBUTION

- Installing sensors in a truck to ensure driver doesn't go off-route.
- Pfizer sensors in the vaccines container confirm temperature stability throughout the journey.
- Everywhere: British NHS hospitals tracking current inventory of fridges.

TEST KIT TRACKING

For COVID-19 control and reliable testing, authentic testing kits and personal protective equipment (PPE) are truly vital. Together with Blockchain startup SUKU, Smartrac developed a digital verification solution to securely authenticate healthcare equipment and provide supply chain transparency.

By equipping COVID-19 test kits and PPE with Smartrac's Circus NFC tags, the solution utilizes Avery Dennison's Digital Identity Platform to feed tag data to SUKU's Blockchain-based supply chain application. The data from the mobile engagement then confirms the authenticity and provenance of the tagged product, reassuring customers and ultimately increasing trust. Customers can also view their purchase price of PPE compared to the global average, providing transparency to help in the fight against price gouging. The physical implementation into existing operations is seamless as the NFC tags are included in the final step when everything is packaged.

KENYA - CUSTOMS AND BORDER MANAGEMENT

Kenya implemented the "Trade Logistics Information Pipeline", Integrating private sector and government sector to come up with a coordinate operations framework. Moving from entirely paper documents to electronic documents.

Paper documents were traditionally exchanged manually, physical printouts which took time to be located and delivered, and were very often misplaced, or even falsified. Implementing a Blockchain documentation solution not only speeds up port performance (reducing COGS) but reduces the possibility of corruption and better integration with global supply chains.

Goods are inspected and approved using the platform, and precise location of items and status in the shipping process is known at all times.



Logistics

END TO END JOURNEY VISIBILITY

Particle is an IoT specialist house, implementing their own backbone to implement their IoT solutions for clients.

Cold chain logistics: sensors in container/ packaging gives confidence that goods were kept cold throughout the journey.

The US Natural Resource Defence Council estimated that 1 in 7 vehicles of perishable items are thrown away.

Geofencing the route reduces risk of unscheduled stops/rerouting.

Road and rail item tracking, precise item location based on tags.

FLEET MANAGEMENT

Route optimisation

- Identification of optimally located vehicles for pickups (Elecom).
- Geo boundary alerts (for when drivers don't follow the route) (Singtel – fleet manager).
- Optimising refuelling costs: e.g. balancing location, route, corporate discounts at certain fuel stations.



Driver behaviour and safety

- SaferDriver track record – identify history of dangerous driving.
- Tracking driver fuel utilisation – identify wasteful / dangerous drivers. Things like unnecessary idling, accelerating and decelerating patterns, breaking habits, average speed and so on affect the fuel efficiency. Using IoT, fleet managers can track all such data through embedded sensors and work with the drivers to improve the fuel efficiency.

Vehicle maintenance

- Sensors (e.g. tyres) indicating when maintenance is needed, scheduling or predicting when it might be needed.
- Vehicle identification certification - qualifying actual ownership / that it meets weight / safety requirements.

Environmental compliance

- Track emissions, identify worst polluting drivers/vehicles.

Agriculture

SMART AGRICULTURE

allMETEO, Smart Elements, Pycno, Crop Performance and Soil Scout

Collecting environmental and machine metrics to optimise crop yields, reducing the chance of ruining a crop, and enhancing the overall yield. Placing moisture detectors in the soil allows farmers to water fields when they are too dry or improve irrigation. Connecting to weather services helps to predict incoming rain, so that they do not get over watered. Better yield predictability helps farmers purchase the right number of seeds and fertilisers prepare for optimal distribution.

AGRI - INSURANCE

One example is Allianz, which has partnered with Bayer AG and several German farm-equipment makers to form a consortium called 365FarmNet. They have established a marketplace for agricultural information where growers can buy GPS, diagnostic, crop, fertilizer and other data from any consortium member; download it to their computers and farm equipment; and use it to take action, such as drawing up crop plans for the coming planting season and calculating their insurance requirements.

- With stats on asset or system usage and performance from the industrial-sector company, customer insurance decisions are more informed.
- Through linkage to an insurer, or multiple insurers, the customer has access to a wider range of insurance options.
- The industrial organization can negotiate on its customer's behalf, sharing data with the insurer to enable better risk management.
- The industrial organization may conveniently deliver insurance through its service platform.
- The insurer gains value through increased service sales.

The insurer, through access to customer and usage data, can mitigate risks and keep insurance premiums low.



CATTLE MONITORING

SCR by Allflex and Cowlar use smart agriculture sensors (collar tags) to deliver temperature, health, activity, and nutrition insights on each individual cow as well as collective information about the herd. Such sensors can identify sick animals so that farmers can separate them from the herd and avoid contamination. Using drones for real-time cattle tracking also helps farmers reduce staffing expenses.

AEROBOTICS

Aerobotics interprets imagery from satellites, drones and mobile phones to provide predictive information on crop health.

It offers insurers data they can use to build an accurate picture of the effects of an agricultural loss event or to help the farmers they insure to better manage their risks.

Data Sharing

DAWEX - CREATING DATA EXCHANGES

Dawex focuses on finding ways to enable groups of users to create their own data exchange marketplaces and monetise them. Allowing them a platform to capture and compare their data. They have also added IoT data functionality to their menu.

Although their technology doesn't appear to be Blockchain enabled, the concept could be applied.

Identity Wallets for individuals and equipment

IDENTIFY VERIFICATION: KNOW YOUR CUSTOMER, KNOW YOUR OBJECTS, KNOW YOUR DEVICES

- BlockPass (Chain Of Things).
- Single validation platform for KYC (bank accounts, crypto transactions, phone companies etc).
- Deletes data once you are verified.

CONNECTING IDENTIFICATION DATABASES

Tykn combines personal and government databases to create a single ID.

Only allows access to specific data fields, and only when authorised by the user without centralising the data.

Facilities management

SMART BUILDINGS

Devices fitted to buildings can be used to better inform building design and maintenance.

Sensors tracking actual building occupancy can be used to better inform energy utilisation (e.g. balancing air conditioning), refining cleaning schedules, or even tracking locations of lost people during an emergency.

SMART PARKING, DETECT WHEN SPACE IS AVAILABLE

Sensor technology that indicates whether their space is taken or not.

Larger parking lots fitted with sensors to indicate whether they have free spaces or not.

SMART BINS

Smart City Solutions provide rubbish bins that are solar powered, compact rubbish, detect when they are full and notify the council when they need emptying.

Energy

PROVIDING ENERGY TO REMOTE AREAS

- Liquidstar (a Chain Of Things creation).
- 1 in 7 people are too far from the grid.
- Connecting to “hubs” where people can carry a battery and charge it.
- Clarity on which hubs drew which energy and to which devices it was transferred.

Infrastructure

GOVERNMENT: EMERGENCY RESPONSE

- Person injured. Sends 911 sms or calls. Urgency indicated by condition.
- GPS coordinates collected from the cell tower. Closest available ambulance identified.
- Available ambulance receives coordinates, navigation system routes to the injured person.
- Route sent to Traffic Control System - turns lights to green for ambulance.

- Light status fed back to ambulance (plus intersections with no lights).
- Incoming ambulance sent to other drivers' navigation tools/self driving cars identify incoming and move out of the way.
- Ambulance progress sent to injured person.



06

Key issues in opportunity assessment for CPS+BC in trade

Participation incentive	P31
Leading with size	P32
Building the ecosystem	P32
Challenges/What would it take to win	P33
Relevant established groups and Consortia	P34
Trade Blockchain consortia	P35
Potential Partners: CPS providers	P38



Participation incentive

Whilst there are clear benefits to integrating IoT securely with Blockchain, the combination is subject to network effects.

The more users a platform has (e.g. a marketplace), the more interesting it is for other users. For example, few retailers on the marketplace means fewer products listed. Fewer products listed results in a marketplace that is of little interest to consumers. Fewer consumers makes it harder to attract potential vendors.

Even in marketplaces where all that is required is to enter your list products, scaling two sided marketplaces takes significant investment.

Factoring in the diversity of IoT devices and technologies, the time and cost of systems integration projects makes onboarding new members to the network a much harder proposition. Maximising the opportunity potential would involve all parties to be “smart” factories, able to share their data in a common Blockchain. Given the current diversity of standards and technologies, such an opportunity would face the challenge of building compatibility with the majority of technologies and standards to make joining the platform as easy as possible for the user.

Alternatively, with a sufficient incentive (e.g. lower costs), users would be more willing to join on their own. Given the high cost of technology integration projects, a significant incentive would be needed for users to go to such effort and cost to implement IoT technologies. Whilst the Industry 4.0 efficiency case (5-15% McKinsey) makes sense for an individual factory, it still needs investment, which many players may not have as immediate priorities.

Simplifying the offer could be another approach – rather than having a fully-integrated approach, at least enabling suppliers with the right tags to identify item provenance may help to meet some of the offer requirements, without full system integration.



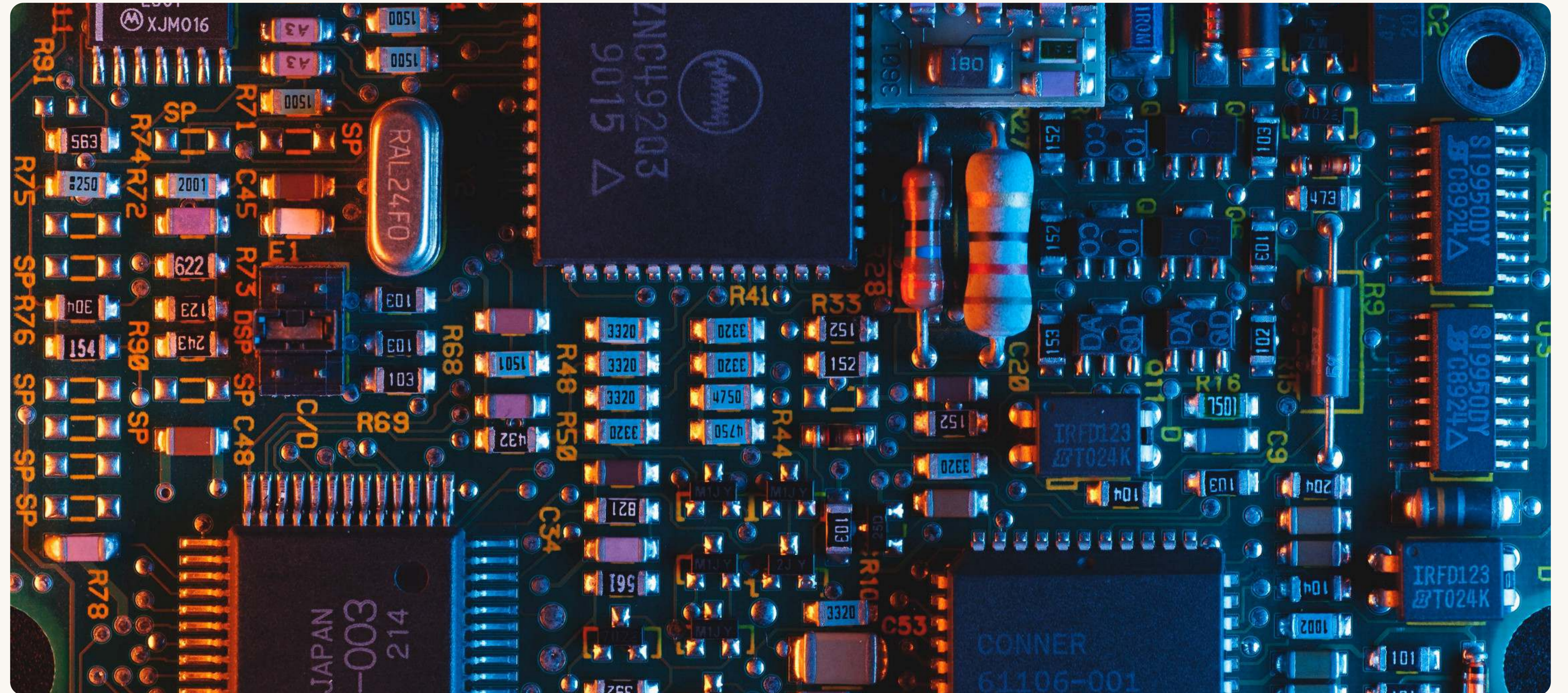
Leading with size

Success in CPS/BC likely to come from those with sufficient size to influence. Parties need to be able to organise consortia and lead technology definition.

Opportunities would need to appeal to powerful members in the chain, to get their support to encourage their network to get onboard.

LIKELY ALLIES COULD INCLUDE

1. Major purchasers (e.g. Walmart, Carrefour, Nestle)
2. Major logistics provider forwarder (e.g. Maersk)
3. Financiers (e.g. Credendo)
4. IoT hardware providers (Auk Industries) or consultants familiar with the space, (IBM)
5. IoT/Blockchain specialist houses (e.g. Supply Chain of Things, or Particle.io)



Building the ecosystem

With a sufficient incentive in place, finding ways to easily enable smaller/low tech members in the ecosystem will be critical to platform success.

Hardware focused opportunities would need to be simple enough – almost “off-the-shelf” - to be deployed easily and quickly to gain traction in a network. Adoption here would need full support of an influential player to succeed. IoT devices would need to be cheap enough. Hopefully, once standardised in the above off-the-shelf solutions, economies of scale can be achieved.

Building a solution that is compatible with as many standards, platforms, legacy systems as possible is no easy feat, and installing it correctly to ensure that they cannot be misused/manipulated by suppliers requires significant thought.

More generic software focused solutions would also need to be very focused on specific use cases that are common to all players in the ecosystem, where data would be very similar in nature (e.g. order number). These are considerable obstacles, and one suggested approach here would be to identify the most common standards first and target those users, or to find established Blockchains and find ways to integrate products/offers into them.

Challenges/What would it take to win

SELECTING A STRATEGY

Several paths to achieve this exist.

A “fuller” option (including the S&OP integration) at this stage would likely involve building a Blockchain platform, selecting preferred technology options (from an established provider such as Auk Industries), and then building an ecosystem of integrated IoT suppliers (including implementation). This would require significant push from an industry player to build.

The (suggested) lighter option would involve seeking out existing consortia of members with shared interests and leveraging whatever standards have been developed. Both ends of the spectrum come with challenges and benefits.

	FULLER OPTION: TOUGHER BUT HIGHER UPSIDE	“LIGHT OPTION: QUICK BUT SMALLER POTENTIAL
Technology	<ul style="list-style-type: none"> • Create new platform and “IoT package” with preferred vendor(s) • Fully customisable to ensure data captured reduces risk • Can define simple/scalable solution for rapid implementation 	<ul style="list-style-type: none"> • Leverage existing vendors or combinations • May limit ability to customise, however fields should be fairly standard across industry • Platform needs to integrate with multiple platforms - creates complexity
Ecosystem	<ul style="list-style-type: none"> • Needs building from scratch • Selecting key partners important • Can define standards that mitigate risk • May be harder to create consortium with desired partners 	<ul style="list-style-type: none"> • Existing consortia may have aligned on standards/platforms. Financing could be an additional benefit for them • If standards don’t meet our needs then it might be harder to influence • May be easier to join a consortium than to create one
Customers	<ul style="list-style-type: none"> • Better able to choose partners 	<ul style="list-style-type: none"> • Depends on available consortia
Speed to market	<ul style="list-style-type: none"> • Slower, need to build technology and ecosystem 	<ul style="list-style-type: none"> • Faster, can try to sell to consortium customers
Strategy	<ul style="list-style-type: none"> • Winner takes all: having a controlling stake in the group means you define the standards (and to what extent other financiers can join in) 	<ul style="list-style-type: none"> • Participation: Many players can benefit from the approach, including other financiers
Partner selection	<ul style="list-style-type: none"> • Need to select initial partners carefully 	<ul style="list-style-type: none"> • Potential to partner with multiple tech partners and consortia

BALANCING RISK REDUCING DATA VS SYSTEM COMPLEXITY

- Clear definition of what data would be helpful to reduce risk is required, identifying what are the biggest impactors to the risk premium.
- With so many potential data points to collect (and so many potential systems involved), this can be a never ending story. It is important therefore to identify what are the key ones that will really impact the rating.
- Identified data requirements then need to be balanced against building a simple enough solution that can be easily/cheaply implemented. A “Standard” package of IoT options and technologies that is easy enough to install, ideally with limited investment (e.g. IoT tags printed that can be read by NFC on mobile phone scanners).
- It may be necessary therefore to sacrifice some information “richness” to build a simpler application.
- In the “light” case – this could be made even lighter, by adopting existing standards.

PICKING THE RIGHT INDUSTRY PARTNERS:

- Partners with enough power to influence. At minimum, the partner should command enough power to influence their own suppliers.

Ideally, they should also be able to influence their customers to some degree too.

- Major influence by a small number of players.
- Many vendors (lots of potential finance clients).
- Vendors with higher financing needs.
- Where players have shared interests and some form of standard sharing (e.g. Maersk helping create Digital Container Standard Association).
- European retailers/manufacturers with multiple suppliers. Retail - Schwarz, Aldi, Tesco, Ahold Delianze, Auchan etc., or Nestle, Unilever would all be able to impact. Highly fragmented – lots of potential customers.



Relevant established groups and consortia

DIGITAL CONTAINER STANDARD ASSOCIATION

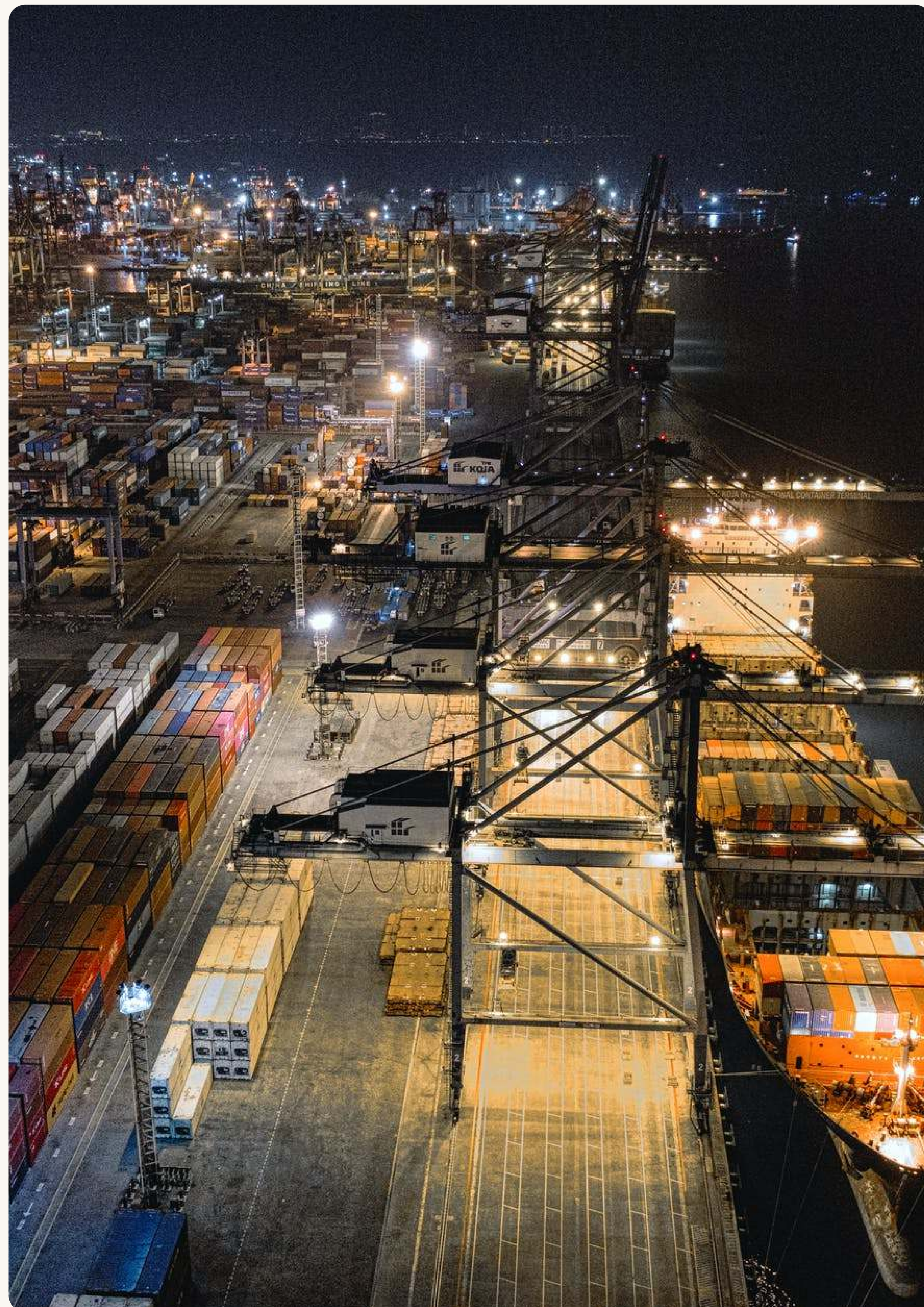
Maersk spearheaded the foundation of the Digital Container Shipping Association (DCSA), which aims to establish standards for a common technology foundation that enables global collaboration. Their goal is to make shipping services easy to use, flexible, efficient, reliable and environmentally friendly.

They have already established IoT standards for remote monitoring of “reefer” (refrigerated) containers which can be downloaded by anyone. Dry containers do not yet have standards.

CHINA - IOT STANDARDS ASSOCIATION

China established an inter-agency council in 2013 to coordinate the government’s policy and action on IoT. The council members include the National Development and Reform Commission (NDRC), Ministry of Industry and Information Technology (MIIT), Ministry of Science and Technology (MoST), the Ministry of Education and the National Standardization Administration.

With the support of this council, China issued a Directive on IoT industry development and the IoT Action Plan in 2013, specifying 2015 targets in terms of top-level design, standards formation, technology R&D, application and promotion, industrial support, business models, safety, government support, laws and regulations, and workforce training.



TRADE Blockchain consortia

TRADELENS

With 170 customers as of September 2019, and having accounted for 50% of global container capacity, and an applications marketplace that will enable participants to build around it, Tradelens looks to be a formidable partner.

This Blockchain platform, originally established in 2017 between IBM and Maersk, initially struggled to bring partners onboard for fears over actual neutrality. So IBM and Maersk changed it from a Joint Venture to a loose partnership. Maersk is seen as a real leader in this area – also spearheading the development of the Digital Container Shipping Association non profit, dedicated to defining standards in this arena.

TradeLens is based on the Hyperledger Fabric Blockchain framework.

Recently expanded to include other major shippers (MSC, CMA CGM, Hapag-Lloyd and ONE). Five of the top 6 shipping companies (excluding China's COSCO). Efforts to integrate are still work in progress however.

Standard Chartered was the first financial company to join (March 2020).

INDUSTRIAL INTERNET CONSORTIUM (IIC)

The IIC is Working to define standards, members include Accenture, Samsung, China Telecom, China Mobile, Dell, Ericsson, Hitachi, Huawei, J&J, Microsoft, Mitsubishi, PWC, and Toshiba.

The Industrial Internet Consortium was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the industrial internet by identifying, assembling, testing and promoting best practices. Members work collaboratively to speed the commercial use of advanced technologies. Membership includes small and large technology innovators, vertical market leaders, researchers, universities, and government organizations.

GLOBAL SHIPPING BUSINESS NETWORK (GSBN)

- China’s equivalent to Tradelens.
- CMA CGM, COSCO Shipping Lines, COSCO Shipping Ports, Hapag-Lloyd, Hutchison Ports, OOCL, Port of Qingdao, PSA International and Shanghai International Port Group (SIPG).
- The GSBN will be established as a not-for-profit organization that operates and facilitates a secure and trusted data exchange platform for all stakeholders along the supply chain. The consortium will nurture community participation and introduce a wide range of services and applications to streamline operation processes and overall efficiency.

To support this vision, CargoSmart will be the technology solutions provider and platform operator for the GSBN.

- GSBN may have an advantage when it comes to IoT integration – as China already has well established standards for IoT device manufacturers.

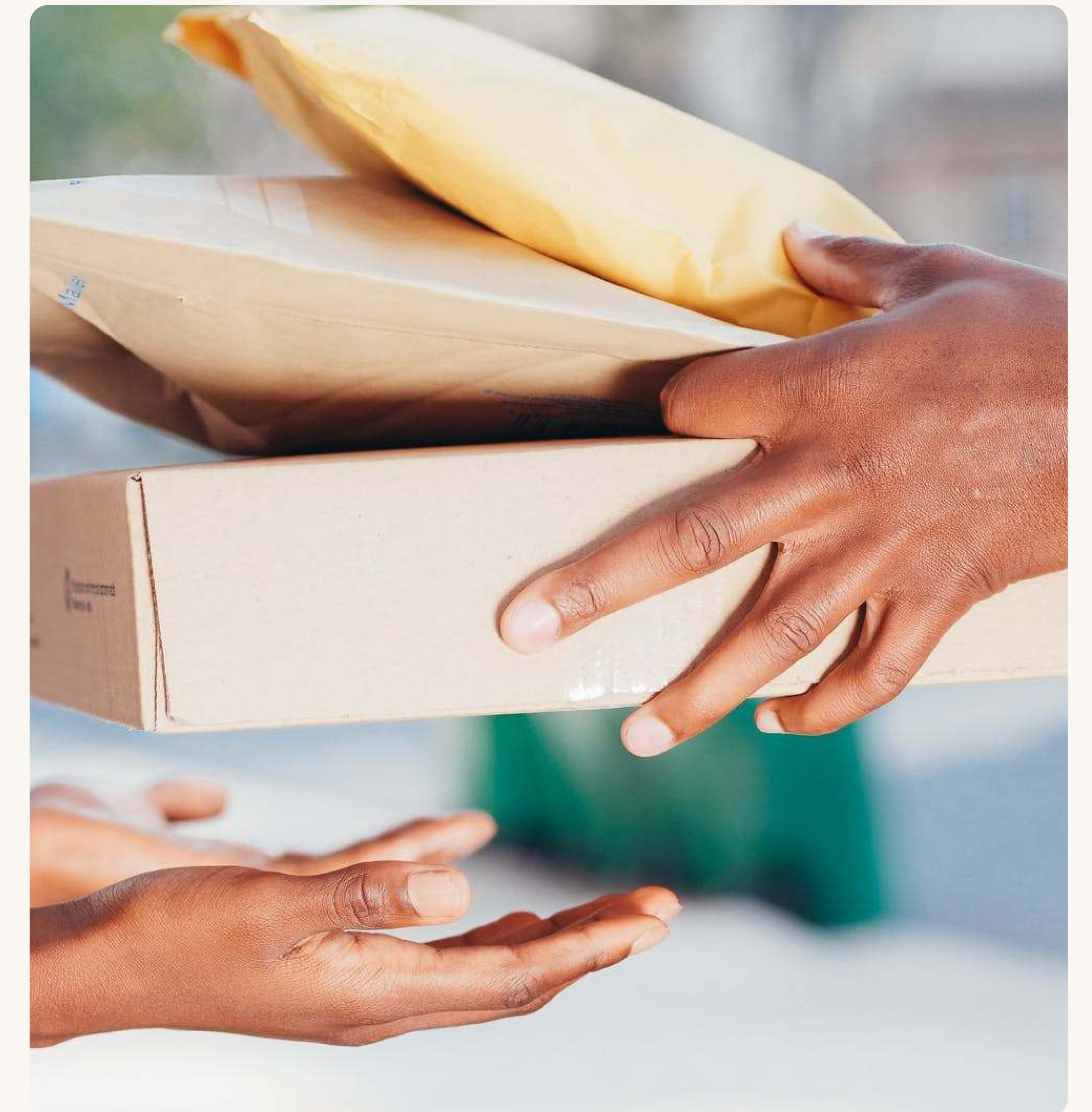
WE.TRADE

- we.Trade “the world’s first enterprise-grade Blockchain enabled trade finance platform.
- Traders, particularly SMEs, who traditionally did not have access to bank guarantees, invoice financing and credit insurance, use we.trade to enhance their cash flow and digitise their existing paper-based processes.

- we.trade is a joint-venture company owned by 12 European banks and IBM, with shareholders including CaixaBank, Deutsche Bank, Erste Group, HSBC, KBC, Nordea, Rabobank, Santander, Societe Generale, UBS and UniCredit.

- Commercially launched in January 2019, we.trade’s technology is currently licensed by 16 banks across 15 countries.

- It uses event based triggers, so it could potentially be linked with IoT device triggers.



KOMOGO

- Komogo is focused on “structured commodity finance”, this Switzerland based venture says its mission is “To catalyse the commodity trade network by providing a fully decentralised, interoperable Blockchain solution to act as a data exchange for the industry.”
- A consortium of 15 financial institutions including Dutch banks, trading companies, and oil giant Shell, was leveraged by MUFG to conduct its first transaction on Blockchain.



MARCO POLO

TradelX is a founder of the Marco Polo Network, which is a growing distributed trade and working capital finance system. Based on Corda's enterprise-grade DLT protocol, the network allows companies to manage trade finance transactions connected to their ERP platform using their own interfaces. It also allows participating companies to store trade data on the Blockchain, enriched with automated contract enforcement, identity management, asset verification and tracking.

The network already has over 35 leading banking partners such as ING, DBS Bank and Bank of America. It works with a number of corporate partners including Accenture and Pole Star, as well as tech suppliers such as R3 and Microsoft.

While in its most generic form, Blockchain allows all members of the network to see each other's transactions, Marco Polo's Corda implementation enables users to restrict who gets to see transaction data, making it ideally suited for trade finance information exchange. It is also open for new network partners and companies looking to improve their working capital performance.

HYPERLEDGER

Hyperledger (or the Hyperledger project) is an umbrella project of open source Blockchains and related tools (Hyperledger Fabric/Iroha/Sawtooth/Besu) used to build Blockchains.

It is rapidly gaining traction, with increasing number of participants (including TradeLens).

Started in December 2015 by the Linux Foundation, the project has received contributions from IBM, Intel and SAP Ariba, to support the collaborative development of Blockchain based distributed ledgers.



The objective of the project is to advance cross-industry collaboration by developing Blockchains and distributed ledgers, with a particular focus on improving the performance and reliability of these systems (as compared to comparable cryptocurrency designs) so that they are capable of supporting global business transactions by major technological, financial and supply chain companies. The project integrates independent open protocols and standards by means of a framework for use-specific modules, including Blockchains with their own consensus and storage routines, as well as services for identity, access control and Smart Contracts.

Early members of the initiative included Blockchain ISVs, (Blockchain, ConsenSys, Digital Asset, R3, Onchain), well-known technology platform companies:

(Cisco, Fujitsu, Hitachi, IBM, Intel, NEC, NTT DATA, Red Hat, VMware), financial services firms (ABN AMRO, ANZ Bank, BNY Mellon, CLS Group, CME Group, the Depository Trust & Clearing Corporation (DTCC), Deutsche Börse Group, J.P. Morgan, State Street, SWIFT, Wells Fargo, Sberbank), business software companies like SAP, academic institutions (Cambridge Centre for Alternative Finance, Blockchain at Columbia, UCLA Blockchain Lab), systems integrators and others (Accenture, Calastone, Wipro, Credits, Guardtime, IntellectEU, Nxt Foundation, Symbiont, Smart Block Laboratory).

FISHTAIL (LOCKSTEP)

Recently rebranded, Fishtail provides trade financing in a way that incentivises environmentally friendly purchases. “The more sustainable your shipment, the better the rate!”

COVANTIS

Covantis is a Blockchain enabled trade finance platform, using Consensus technology (created by Ethereum’s co-creator).

**POTENTIAL PARTNERS
CPS providers**

There are many providers in this space. It is a highly fragmented space with endless technologies for Tags, Tag printers, Tag readers, IIoT devices, networking applications, processing, storage, analytics etc. with no clear standards in place.

As such, a suggested approach here would be to leverage existing players in this space who have already established a preferred set.

Finance Commodities procurement	<ul style="list-style-type: none"> Tradeable, BlockChain LC. Creates a special purpose investment vehicle, governed by Smart Contracts, which takes title to the inventory. Enables financiers to take ownership of inventory capital. Saves 0.5-2.5% of financing costs. 50% of cost vs. LC
PoP Codes (Proof of Provenance)	<ul style="list-style-type: none"> IoT Tags used to track PoP (Proof Of Provenance) - used to track cargo progress in real time – better traceability Creates a series of code stickers containing provenance info, for automatic upload to client system on receipt
Consumer Provenance apps	<ul style="list-style-type: none"> Precise batch level information of what went in to each product
Confirm goods quality – reduce risk	<ul style="list-style-type: none"> Track and trace commodities
Manage transactions	<ul style="list-style-type: none"> LC / Contracts (Smart) / Blockchain Export Document Tracker / Program Buying
Zero Knowledge – data sharing	<ul style="list-style-type: none"> Optimising S&OP – integrating through the chain
Blockchain gateway	<ul style="list-style-type: none"> Combine interoperable banks

SKUCHAIN

SkuCHAIN is a “Liquid Supply Chain” concept - Focused on unlocking financing opportunities in supply chain solutions for enterprise. Cloud ERP, Resource planning, data sharing tools. Claims to allow “buyers to collaborate with each other as if they are on a shared ERP system).

Their combination of software and hardware knowledge could make an interesting partner, and limit the need to develop technology (their website suggests they may have the “backbone” needed for this). Option could be to add financing to their existing offer.

AMBROSUS

Ambrosus is a Blockchain powered IoT network for food and pharmaceutical enterprises, enabling secure and frictionless dialogue between sensors, distributed ledgers and databases to optimise supply chain visibility and quality assurance. It provides a flexible data model that enables onboarding of all real-world supply chain entities (product, batch, box), the measurement of their attributes, and the tracking of related logistical events. Their API can create unique digital identities for every item you want to track and analyze along the way. This identity and history will be stored permanently and immutably on the Ambrosus Blockchain.

Ambrosus is an ecosystem that plans on using the Blockchain and IoT in order to track products through the supply chain whilst guaranteeing product quality, safety and origin for the customers. This is done with the intention that the consumers have the right information about the products they are buying. This information can also be used in order to draw up Smart Contracts amongst the supplier and the consumer – in turn enforcing quality control, creating a system of “interconnected quality assurance”.

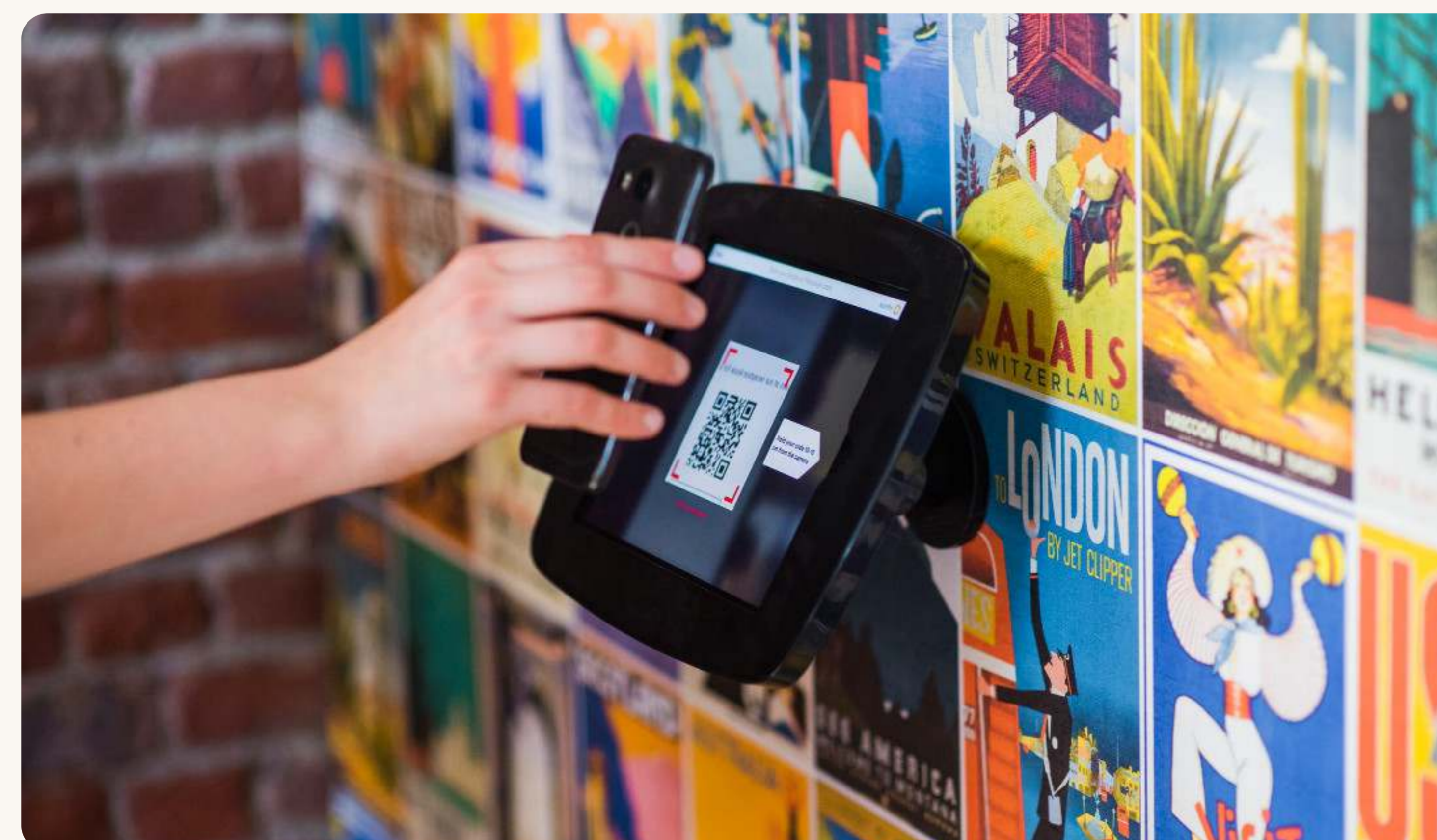
The Ambrosus project began with the aim to ameliorate and enhance the global supply chains through an ecosystem which can record and execute the complete history, movement and transactions of products.

PARTICLE

Particle Have packed up combinations of technology to implement IoT solutions across a whole range of IoT use cases (Asset tracking, Fleet Management, Predictive Maintenance, Environmental Monitoring, Compliance Monitoring, Order Fulfilment).

CHAIN OF THINGS

Chain of Things (CoT) is a research lab and venture studio dedicated to leveraging the nexus between Blockchain and IoT to solve fundamental problems in the connected devices space and to develop highly efficient futuristic applications. CoT will address the point of device identity from birth to solve for systemic issues of security and interoperability. With this it will develop and deploy industrial, environmental, and humanitarian projects through corporate partnerships, joint ventures, and internal projects.



They previously ran a “Chain Of Shipping” conference (in 2016) with a number of developers, ports, banks and advisory companies. No product seems to have been developed by them in this space.

IOTEX

IOTEX is building a root Blockchain that other Blockchains (or “sidechains”) can connect to – aiming to be the spinal cord for IoT systems. It aims to become as lightweight as possible to facilitate faster transactions – targeting IoT transactions.

UBITQUITY - ADDING A BLOCKCHAIN LAYER TO EXISTING DATABASES

An API between existing title records and Blockchain.

Each transaction stored in a Blockchain, on top of an existing database.

IOTA - INCENTIVISING DISTRIBUTED NODES

“IOTA is a decentralized, very lightweight micro-transaction token that is optimized for the Internet-of-Things. It is essentially a blockless ledger without any sort of fees on transactions. ‘Money of IoT’ to incentivise node participation.

Appendix

Developing common standards

MAERSK HELPS FORM THE DIGITAL CONTAINER STANDARD ASSOCIATION

The Digital Container Shipping Association (DCSA), aims to establish standards for a common technology foundation that enables global collaboration. Their goal is to make shipping services easy to use, flexible, efficient, reliable and environmentally friendly.

They have already established IoT standards for remote monitoring of “reefer” (refrigerated) containers which can be downloaded by anyone. Dry containers do not yet have standards.

THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

The OSI developed by ISO, is a framework for network communication. The OSI contains seven layers: application, presentation, session, transport, network, data link, and physical. Each layer uses services provided from the layer below it and offers services to the layer above it.

The IoT technology concentrates on two broad types of standards, namely, (1) technology standards (network protocols, communication protocols, and data aggregation standards) and (2) regulatory standards related to security and privacy of data.

FMI FUNCTIONAL MOCKUP INTERFACE

This is an open source simulation concept that was originally designed to develop autonomous vehicles. It allows multidisciplinary developers and engineers to learn a common platform that can be used to develop an off/online simulation or can be used in embedded control systems (CPS). It is open source. Each discipline can define their controller code for controlling a component. To create the FMI standard, a large number of software companies and research centres have worked in a cooperation project established through a European consortium that has been conducted by Dassault Systèmes under the name of MODELISAR.

NIST CPS PUBLIC WORKING GROUP

The objective of the CPS PWG is to develop a shared understanding of CPS and its foundational concepts and unique dimensions (as described in their “CPS Framework”) to promote progress through exchanging ideas and integrating research across sectors and to support development of CPS with new functionalities.

The framework aims to identify common: Vocabulary and Reference Architecture, Cybersecurity and Privacy, Timing and Synchronization, Data Interoperability, and Use Cases. It also serves as a useful checklist to sense check ideas and build on problem statements in this space.

ONEM2M

interoperability enabler for the entire CPS, M2M and IoT Ecosystem. Developing Technical Specifications and Technical Reports, which address the need for a common IoT Service Layer that can be readily realized through an API embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with IoT application servers worldwide. A critical objective of OneM2M is to enable users to build platforms, regardless of existing sector or industry solutions, to enable wider integration and cross- system value to be derived than is currently possible.

OneM2M aims to attract and actively involve a wide variety of organizations from IoT related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. to address R&D issues in cybersecurity. The CPS Voluntary Organization (supported by the National Science Foundation) is an online site to foster collaboration among CPS professionals in academia, government, and industry.

THE NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT (NITRD) CPS SENIOR STEERING COMMITTEE

This committee coordinates programs, budgets, and policy recommendations for CPS research and development (R&D).

This includes identifying and integrating requirements, conducting joint program planning, and developing joint strategies for the CPS R&D programs conducted by agency members of the NITRD Subcommittee.

CPS includes fundamental research, applied R&D, technology development and engineering, demonstrations, testing and evaluation, technology transfer, and education and training; and "agencies" refers to Federal departments, agencies, directorates, foundations, institutes, and other organizational entities.

AVNU ALLIANCE

A community for creating an interoperable ecosystem servicing precise timing and low latency requirements of diverse applications using open standards like Time-Sensitive Networking (TSN).

This alliance focuses on creating interoperability tests and certification for products used in applications requiring bounded latency, reserved bandwidth, and synchronized time.



07

About AREA42

AREA42 is the Trade Innovation Ecosystem of Europe and the home of a buzzing TradeTech Community. At AREA42 our team is united by a common mission: to create, innovate and manage solutions for a fluid and risk-savvy trade environment. We believe in a frictionless B2B trade environment empowered by TradeTech.

AREA42 was born out of the realisation that we need to recode trade finance for the digital era, and we need to break away from previous, unfruitful attempts at corporate innovation. We are the trade innovation ecosystem, a community-based effort to come up with disruptive solutions to real market needs. One of our ventures, Marjory, caters to marketplaces, offering them a catalogue of workflows with a multitude of service providers and helping them to smooth out their

integration processes. This is because we believe marketplaces are one of the key business models in the future. Other research avenues include data and artificial intelligence, as well as digital ways to help SMEs and micro-enterprises manage their trade risks.

Lode Vermeersch is head of AREA42, Credendo's innovation ecosystem. Having worked in banking, insurance technology and innovation for the past 27 years, Lode has first-hand insights on why it is so difficult to innovate in a corporate environment. He also knows how important it is for the trade finance industry to modernise and start catering to new types of companies — and new types of trade. At AREA42, Lode is responsible for unlocking long-term growth engines by scouting new ideas, developing experiments and accelerating them into new products.



Interviews with

- Senior Risk and Investment Specialist Asian Development Bank
- CEO – Auk Industries (IoT Device and networking provider)
- Investment Director – Ericsson Ventures
- Associate Partner - McKinsey

References

- US National Industry of Standards and Technology NIST Framework for Cyber-Physical Systems: Volume 1, Overview
- Particle.IO How the internet of things is modernizing the transportation and logistics industry
- Particle.IO 4 Best Practices for managing cold chain logistics
- Particle.IO Blockchain Identity Management: The Definitive Guide (2020 Update)
- Eastern Peak IoT-in-agriculture-technology-use-cases-for-smart-farming-and-challenges-to-consider

- McKinsey Digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things
- McKinsey What-separates-leaders-from-laggards-in-the-internet-of-things
- McKinsey Supply-chain-finance-a-case-of-convergent-evolution
- McKinsey Industrial IoT generates real value--if businesses overcome six myths
- McKinsey The-Internet-of-things-Mapping-the-value-beyond-the-hype
- Businesswire GovCoin-Systems-Implements-Social-Welfare-Payments-Distribution
- Arxiv A journey in applying Blockchain for cyberphysical systems
- Spendmatters What finance costs do suppliers pay for early pay finance
- IoT Now Ayla IoT-Platform-Build v Buy Whitepaper
- Consilium Trade Finance Ctf-product-features
- GS1 EPCIS standards gs1_epcis_source_to_shelves
- DHL glo-core-Blockchain-trend-report

- BlockSocial Blockchain's impact on supply chains
- BuiltIn Blockchain insurance companies
- IOTA Global-trade-and-supply-chains
- Reasonstreet business-model-pay-per-use
- Accenture the-iiot-opportunity-for-insurance
- Siemens Mindsphere Atos_UseCase_IndustrialLeaseOptimization
- KnowIS Banking meets industry: IoT as a motor for new financing models
- Use cases: positiveblockchain.io
- BlockSocial Blockchain's Impact on Supply Chains
- Investcorp Emerging-use-of-IIOT.pdf
- IOT News Are traditional financing models becoming increasingly irrelevant with IoT?



AREA 42
Trade innovation made easy

This is the end... or just the beginning.

Surf to www.AREA42.tech to discover all about TradeTech!

AREA 42