INTERNATIONAL INSURANCE SOCIETY

An affiliate of The Institutes | Risk and Insurance Knowledge Group

# De-Risking the Supply Chain
# with BlockChainTechnology and Data Integrity

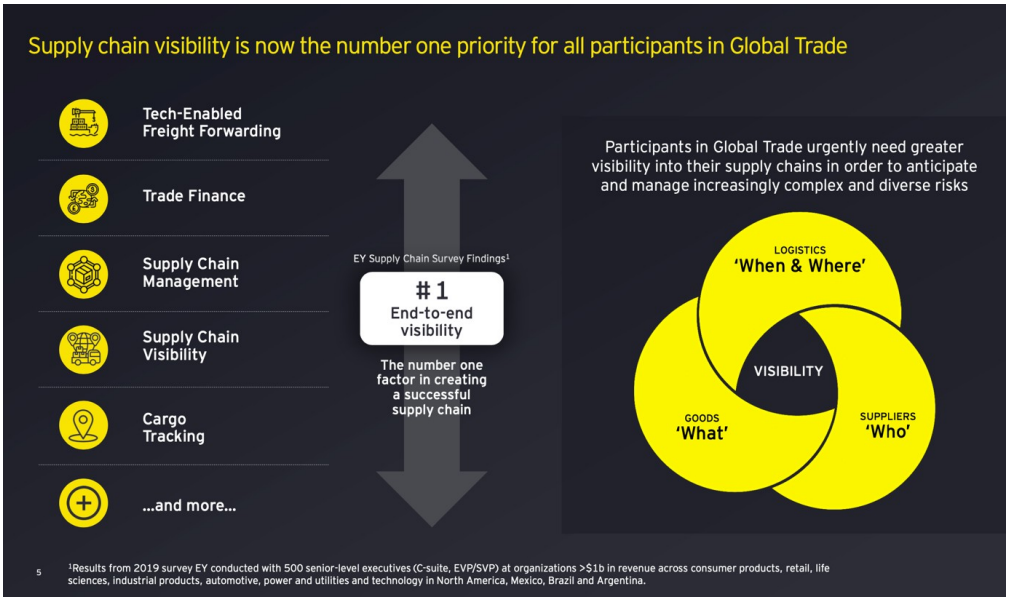

## Abstract

Recent cyber events such as Solar Winds/Sunburst (December 2020) and Colonial Pipeline ransomware attack (May 2021) were supply chain data breaches that affected government, corporations and customers, adding to cyber activity on critical infrastructure during COVID-19 supply chain disruptions. This behooves the insurance industry and their customers, to tighten risk management around data integrity while events remain fresh in mind and ensure better future preparedness. We look at risks and mitigation in cyberspace on global supply chains, port infrastructure and transportation as they become more digitized. Protecting new digital assets conversely applies to monetize them and scale up liquidity in a marketplace via an ecosystem of players with same financial interests. Mitigation leads to more insurance touchpoints in cyber risk, business interruption and parametric insurance, business models using data driven innovation encapsulated by blockchain auditability. We discuss adoption of exponential technologies to address mega endemic business problems affecting global trade, that of supply chain visibility and trade financing protection gaps which threaten sustainability in multiple markets. Trade finance suffered due to the pandemic, so available capital needs to be deployed where required. This addresses the dilemma of extending financing to suppliers who constantly struggle to obtain financing because of geo-political reasons, foreign exchange risks, limited access to credit, collateral shortfalls or short-term liquidity. We are mindful to address the green supply chain and apply ESG (Environment, Social, Governance) principles coupled with exponential expansion of sensors, cloud computing and data volume with Internet of Things (IOT) networks. Blockchain technology is becoming mainstream post pandemic. Properly implemented, this eliminates inefficient paper processes, removes trust deficits while improving transparency and visibility amongst supply chain parties while preserving data privacy and integrity in the whole ecosystem.


## Overview

Supply chains are becoming digitized, globalized and present a complex mesh. Innovation in cyber and data integrity by design is paramount. The fourth industrial revolution (Industry 4.0) brings a new digital ecology around smart cargo containers, cross cloud platforms, additive manufacturing (3D-printing), IOT sensors plus an explosion of data that drives fast 5G networks and soon quantum computing. Legacy

ERP (Enterprise Resource Planning) systems struggle to provide automated and trusted data exchange between parties in supply chain networks across borders, leading to a disconnection. Restricted track and trace information on goods passing through warehousing and distributors threaten the required provenance and visibility of data both upstream/downstream as seen in diagram below.




Increasing emergence of digital counterfeiters leads to fresh challenges in fraud. Quality and compliance regulations raise the bar in consumer expectation of product quality and procurement accountability. Concerns on authenticity of a product that a retailer returns, would be dismissed, as counterfeit goods lack verification history on a blockchain.

The pandemic ravaged world has experienced supply chain failures of sufficient magnitude to accelerate significant changes in logistics underpinned by technology investments. Solutions emerging can scale and respond in real-time. Intelligent data access and visibility make data usable. The current notion of data access comes from yesterday's technology where data are physically shared which leads to distrust. Data visibility is a mindset change where data does not travel, outside of payment transactions, and can be analyzed with permission without leaving the owners environment using a provenance audit trail via a path of digital tokens.

De-risking the supply chain is a major undertaking. A Swiss RE Sigma paper covers the macroeconomics of this very well, so we focus on the business-driven technology aspects ofthe de-risk equation around visibility, secure trade and closing the trade finance gap.

Asian Development Bank (ADB) said in 2019 that the trade finance gap was $1.6 T[ii] and since the pandemic now revisedto $3.4 T[iii]. SMEs (Small and Medium Size Enterprises), often in emerging economies, are most affected with more chance of trade finance rejection. The banking and insurance sectorscan step up respectively to aid short term trade financing and help close the protection gap.

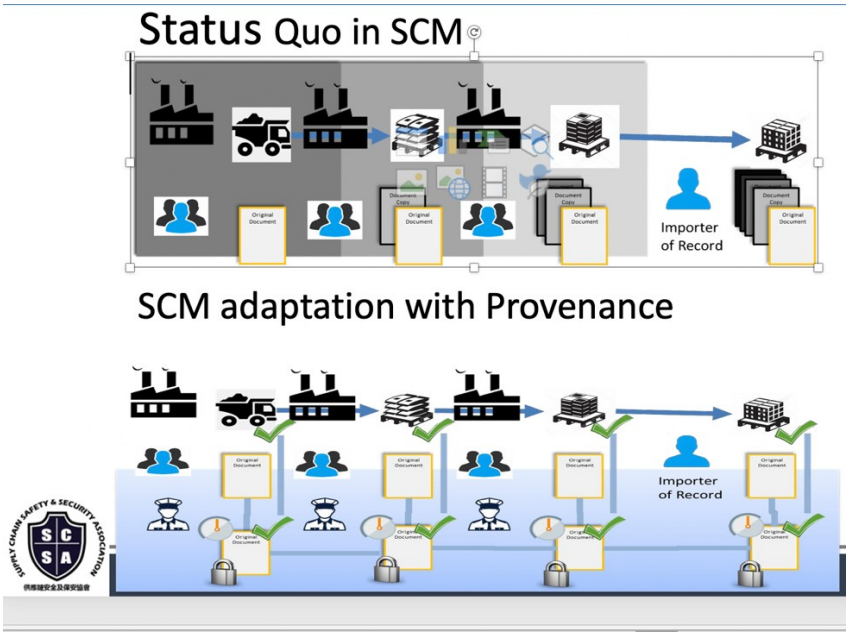
Blockchain technology plays an important role in garnering trust between parties. The impactof this global trade finance gap is serious and an impediment toward poverty reduction and inequality, which the UN's Sustainable Development Goals (SDGs)[iv] aimed to address in 2015. The International Chamber of Commerce (ICC) estimates a capacity of $5 T.[v] is needed for the trade credit market just to return to 2019 positions.

Trade finance shortages affect imports of staple food and medical supplies as well as exports of vital income-generating products. Such shortages weigh heavily on SMEs, who are often collectively the largest employers, creating a ripple effect on financial inclusion. As 90 % of goods go by sea, the pandemic has caused crew exchange issues and delivery delays with problems still mounting. Overcoming SME financing hurdles will pay attention to blockchain technology to improve trust and transparency among transacting parties. This will involve the use of non -fungible digital tokens (NFT) and the smart contract programs that drive them as they function and execute on the supply chain and regional trade blockchains.


## Expediting Secure Trade with BlockChain

Current supply chains rely on 'one up, one down' traceability as each member of the chain trusts the representations/certifications of trading partners. Creating secure traceability of information throughout the supply chain is vital. Visibility up and down and cross border is problematic. Tracing paths back in a supply chain to recall a product or confirm declarationsin cases of suspected malfeasance is a challenge. Interoperability between partners will provide reliable information about shipments and ports of departure in order to perform the necessary checks and balances involved in customs valuation. When data visibility exists so does the ability to detect manipulation or misrepresentation. Trust and verify needs to be embedded in the whole ecosystem so good performance in the supply chain management (SCM) will reward the participants and maintain data provenance.

A recent significant event that saw the collapse of the supply chain finance specialist, Greensill Capital, in conjunction with trading partners and financiers, potentially could have emanated from invoices that were not visible or genuine in the provenance trail.[vi]

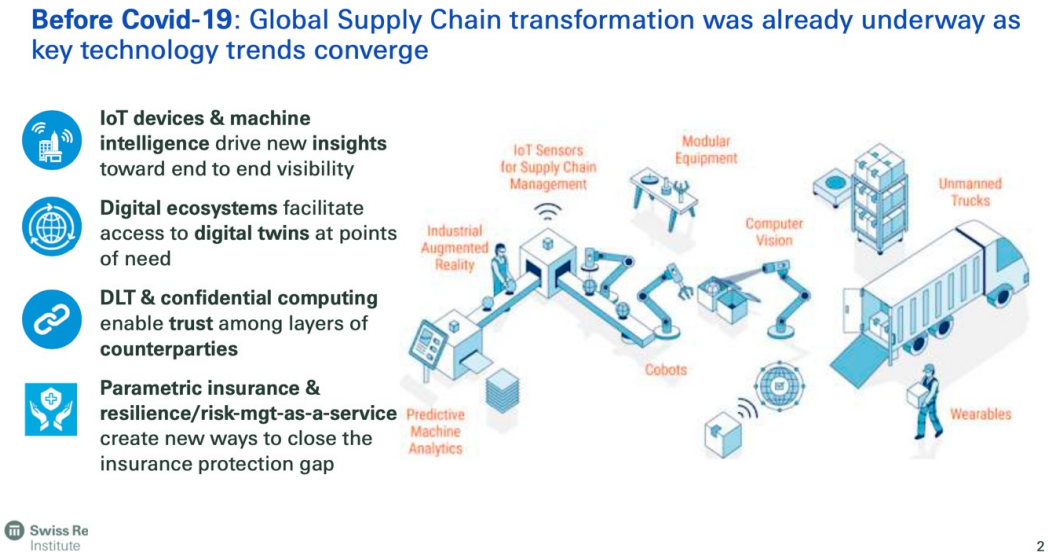



The supply chain has moved from trust to trust but verify and is achieved using a digital/physical twin concept. A digital twin is a virtual representation matching the physical attributes of a “real world” factory, port, product or manufacturing component in real-time through a network of devices such as sensors,

drones, robots and cameras. The data collectedand analysed is a dynamic model that drives insurable business outcomes.

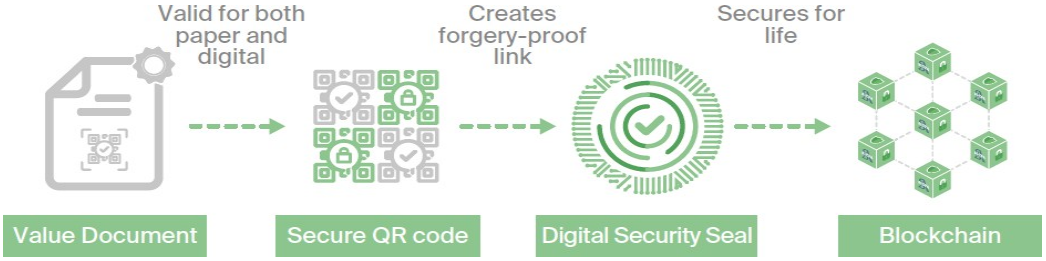
Blockchain technology underpins the process to secure the digital environment which could be deceived if a counterfeit/substandard physical object is inserted or a cyber-attack occurs. Incorporating a physical element on the goods such as RFID codes can secure identity as the link to its digital twin. Digital twins provide assurance that goods, shipments, and related documentation can be confidently validated with immutable records. This is a major source of supply chain technology investment post pandemic to address the visibility issue.

The transformation was already in place before the pandemic but is now accelerated.




Blockchain transforms a 'single window' snapshot of the supply chain into a secure and immutable history of entities, material, and events over the life of a trade using cryptography known as data provenance. Actual data is not stored on the blockchain only the cryptographic representation of the data, (hash key), is registered (signed), making sure data identity and privacy is preserved. The hash key identity connects to actual data stored in ledgers or databases to validate the data integrity at any point in time, separating the blockchain layer from the data store. Auditability can be extended down to the device level as tamper proof hardware to maintain cyber integrity. Complete independent verification of the data is done using only mathematics. This verifies who signed the data, what the data should be, and whattime the data was signed, without explicitly knowing the entity sending the data.

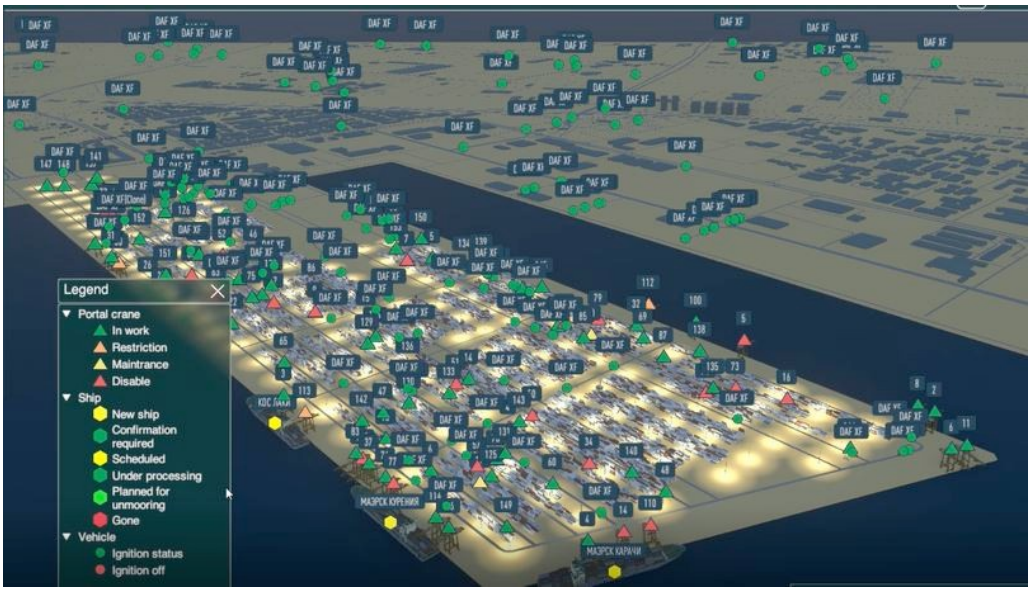
A physical asset such as a bar code, RFID or QR code is cryptographically sealed into a digital twin token and signed using a hash key immutably binding the data to the blockchain. This includes the identity of the entity that created the token and registered the component, aswell as what location and point in time they did so. The token becomes a time capsule for thatasset forever, immutable and tamper proof.



Relevant events are captured and the audit trail will include both supply chain data (licenses/certificates) as well as data that supports detailed analysis of the broader supply chain (corporate/inspection history). This granular, tokenized, secure data set is protected to provide data visibility on a permissioned basis for trading partners and regulators. As the entity signing the data can differ at each supply chain stage, the tokens represent accountability and ownership at a point in time. The tokens contain evidence of asset provenance and contextual attachments so the verifying entity can use them as input to a data integrity validation decision: Was this asset manufactured by known or trusted entities and did it come from the correct location? Can authorized participants access the digital twin of the product and declarations that move through the supply chain? Buyers can verify a digital chain of custody back to the origin and licensing agents can review licences. The lithium battery case study later in the paper shows this process in action.

Digital twins are already prevalent in seaports/airports which allow workers to operate at the intersection of cyber and physical worlds using artificial intelligence (AI) where decisions are tracked on the blockchain using machine learning. Having trusted data available in real-time, the operational control system determines the sequence of logistics tasks and activities by correlating a data flow collected from smart sensors, cameras, and vehicles in the network. Forklifts, cranes and freights can be moved, tracked and positioned along with inventories of goods, loading and unloading of cargo, and live updates can be shared with port supervisors. Ericsson and the Port of Livorno are a good example[xv].

The data collected through 5G feeds a digital twin engine, shown below as green and red tags which is the operational data. This was developed in the UAE (United Arab Emirates) by the Saiber-NNTC Alliance (Pradeep Luthria/Rustam Khametov) [vii].




Ports are gateways to the world that are of extreme importance in an interconnected scenario for supply chain risk. Challenges that ports face today is how they can evolve to become more efficient, competitive, and sustainable as well as mitigating cyber-attacks and delays. A blockchain aware solution can reward ports for less delays.

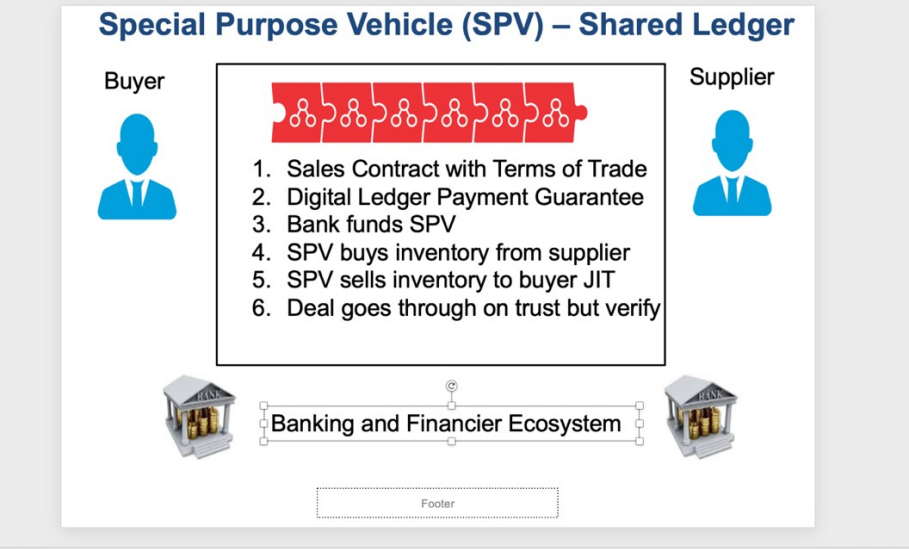
## Closing the Trade Protection Gap

A safer and trusted supply chain allows banks to extend loans to SME distributors and suppliers. Blockchain addresses the challenge of supply chain finance (SCF) by digitizing rules around letters of credit. Many SMEs do not get liquidity because of lack of trust, financiers' inability to monitor inventory policy and suppliers not financed within the buyers cost of capital. Large international banks have

withdrawn, opening doors for regional banks to fill liquidity gaps, and get cross border coverage. SMEs in emerging markets are impacted most by barriers to trade finance. The Organization for Economic Co-operation and Development (OECD) states that SMEs remain underrepresented in global trade.[viii]

SCF creates liquidity through buyer or seller led approaches and optimizes availability and cost of capital. A distributed ledger attached to the blockchain allows sharing of information, monitors the physical flow of goods, and mitigates financial risk allowing access to financing. The buyer and seller sales/purchase agreement exists on the same ledger, so asset tracking is transparent and trust deficit with financiers removed. All parties see a copy of the transaction. Inventory is bought outright, financed from the buyers cost of capital via a special purpose vehicle (SPV). The supplier receives early payment and the buyer guarantees payment receiving title for the inventory. The immediate benefit is that the suppliers' receivable cost is removed which can be 15-30% in developing countries. The buyer gets real-time visibility and control over the inventory without holding it on their balance sheet and will get a lower cost for the goods from the supplier who has early capital.

The seller holds inventory at the pleasure of the buyer and when buyer is ready to use the inventory it is sold back to the buyer "just in time" which is ESG friendly. The letter of credit is digitised into a 'digital ledger payment commitment (DLPC)' which de-risks the trade transaction to the financiers. The trade documents and delivery are held with the DLPCwhich is a digital token or smart contract representing the trade. Third party financiers (banks or high net worth individuals) fund the SPV as they are visible to buyers cost of capital in pre deal discussions and see clear chain of title in provenance from supplier to buyer plus the buyer payment guarantee. They can now see that the trade deal is de-risked and they are not guaranteeing offline transactions so can finance without risk. The whole ecosystem has benefited plus it rewards all parties for well-structured trade finance.




## Onboarding Players to Supply Chain Ecosystem

Onboarding players to the supply chain ecosystem is a challenge due to the trust deficit, suspicions around data sharing and competition. Legacy ERP (enterprise resource planning) will remain in place for the short term, but the fast pace of technology adoption will drive change. Many functions like accounting and governance will interoperate with the blockchain technology using intelligent API's (application programming interface) which integrates the various flows of transactions across the multiple parties involved. For a successful supply chain ecosystem, participants should be on the inside looking out and not vice versa, including regulators and compliance authorities.

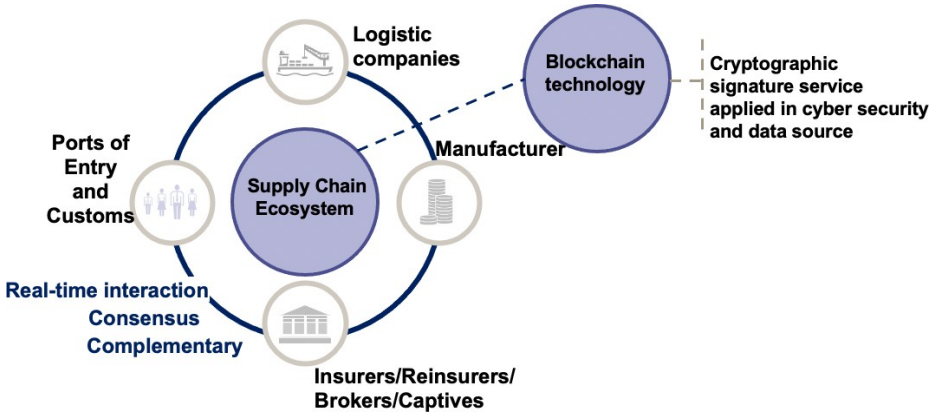
Applications requiring data liquidity (movement) but minimal information sharing such as purchase orders, invoices, and payments can be on separate blockchains. Companies waryof sharing competitive data are then willing to participate on a permissioned platform. Multiple supply chains exist so all participants will not need to adopt a single solution however a single chain of custody or single version of the truth can be

created by interoperability. Thisalleviates the material integrity customs challenge at the port of entry, since at no point can a ‘clean’ provenance trail be used to represent material that came from another supply chain.

Building a trusted ecosystem entails a governance mechanism to determine who joins the network, what data is shared, privacy, who has access, how disputes will be resolved plus useof IoT devices and smart contracts. Data sharing impacts inventory-allocation decisions and pricing by making information in the supply chain more transparent for products.

Blockchain requires a consensus protocol for maintaining a single version of the transaction history that everyone agrees in the ecosystem. Incentives can be given to onboard. Education isrequired to inform participants that consensus will be done by permission and not by “mining” using up electricity, as in the cryptocurrency public arena, which is not ESG friendly.

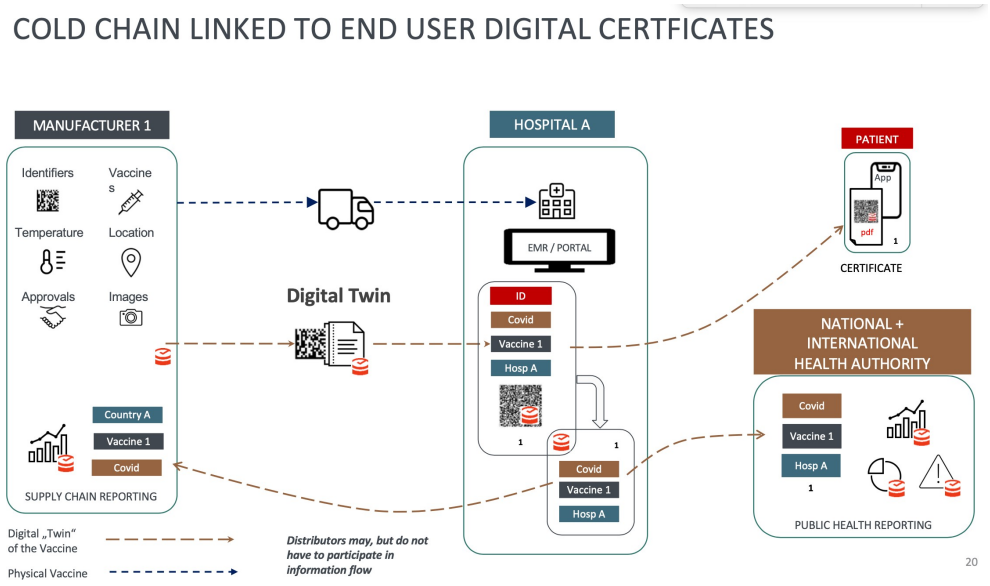
Digital supply-chain ecosystems create embedded insurance opportunities as tokens act asdigital agents operating between machine-to-machine interaction. They create a dynamic marketplace for buyers/sellers to interact directly, enabling the collation of data for the delivery of digital products, enabling insurers to offer risk management as a service for supply-chain risk reduction via a digital marketplace.




## Tokenisation of the Supply Chain

A token is the digital representation of any asset on a blockchain. There are many kinds of digital tokens – some represent money, others equities and functions. All have an equivalentin the physical world. Digital tokens will drive the supply chain for greening, tracking, and tracing, cybersecurity, and verification of ownership. Non-Fungible Token (NFT)[ix] supply chain development offers precise tracking of goods from the production unit to inventory. These tokens represent digital equivalent of non-exchangeable unique assets and have been widely publicized publicised in the art collection world. Each of the goods passing through the supply chain has a unique NFT assigned to it which can store and trade value in the physical world.

Gold, real estate, diamonds, art, patents, and collectibles are all being “tokenized”. Tokens tracking goods, monitoring conditions, and guaranteeing provenance with IoT devices with ablockchain are change agents. Perishables in a cold chain including vaccines/ medicines can be traced by IoT sensors and help to retrace longer transport routes. A refrigerated container equipped with an IoT device to monitor the temperature can record any unsafe fluctuations on the blockchain as shown below.




*Courtesy of Guardtime*

Trust is one of the most important features in supply chain management. Tokens at each transfer point tracks the status of the IoT devices and builds trust by storing the data onto the blockchain with digital twins. Data collected by IoT sensors represent a value and can be offered, tendered, and paid through tokens in a data asset exchange. This forms a contractual process between data supplier/receiver by the use of a digital token. IoT sensors can act autonomously and turn into a participant in the ecosystem with their own identity. Devices, data, and people combine to provide a single source of identity in an ecosystem. For the insurance industry this offers a highly distributed sensor, evidence-based, data driven environment for authentication and risk management using performance based regulatory tokens.

## Monetisation of the Digital Asset

Once protected, the digital asset can be monetised. Incentives are needed to create mindset change for participants in a supply chain to adopt data sharing strategies. Participants provide traceability information of a product via a unique token, and when that product is sold, they can be compensated. Logistics providers could be paid royalties for data associated with moving/storing of goods as well as service fees. For an insurance transaction,a participant could be a non-traditional insurer entering the market and collecting the premium. This is a precursor of valuing data as an asset to make it tangible on balance sheets.

Tokens create an asset on a blockchain that can be used in a collaborative environment and, when traded, becomes monetizable on a digital asset exchange. This removes onboarding impediments as everyone is rewarded for some activity which previously was perceived to have no commercial value. Onboarding the actual customers via their suppliers is an incentive for all upstream players to join an ecosystem, especially if they can trade data they own. The tokens in the supply chain provenance contain documents that add value to the overall trade in the different stages and without these documents the trade will not proceed. Examples are product certificates, shipping notes, bills of lading, letters of credit and then the purchase order which triggers the trade and records the monetary value. Data assets are now being traded in tandem with goods. Tokens represent value in many forms such as loyalty points, paybacks, discounts, vouchers to purchase other goods, carbon credits and credit risk profile enhancements. Thus, the entire supply chain is incentivised, with trust deficit removed, and not just looking at one stage but all participants being rewarded in a successful trade.  This will increase revenue in a marketplace by scaling up the tokens to increase liquidity.  The more customers onboard from online sources, the more liquidity for the products and the digital twins, from QR codes downstream enabling provenance and reward for onboarding customers, and this has a cascading effect. Applications that convert digital assets into digital tokens to then trade them on the blockchain represent a tangible result of how blockchain is a change agent across all supply chains.


## Smart Contracts and Parametric Insurance

Smart contracts form the basis of all digital tokens today. They function as parametric structures so are a viable mechanism for embedded insurance providing alternatives to indemnity products beyond natural catastrophes. This also opens a new market protecting smart contracts themselves from failure, as a new line of intangible business known as DeFi(decentralized finance) which umbrellas all the intangible assets including cryptocurrencies.

The unique NFT supply chain token secures goods from being modified, damaged and fraudulent activities in the supply chain. A smart contract will be set up for each asset in the supply chain representing physical goods as part of the NFT.

Smart contracts are the programmable code in the blockchain network that works on the consensus mechanism. All permissioned parties in the ecosystem share a copy of each transaction and approve before the trade moves to the next stage of the supply chain. Thesmart contract plays a key role in data liquidity for payments/refunds when the required conditions trigger an event, the consensus mechanism keeps the payment safe and secure.

The release of payments and other actions are enabled by technology and rules-based operations. The smart contract is not reliant on a human third party or central operator and iscurrently being developed in Insurtech in relation to short term risks where there are clear parameters as to payment, the potential for disputes is low and the claims management process is uncomplicated or pre-determined. There is already a range of IoT related insurance products on the market, such as smart city, autonomous transport type products, where innovators use smart contracts to connect the devices with the underlying insurance policy. Cryptocurrency DeFi companies are using smart contracts in conjunction with stable coins to protect the volatility of bitcoin and peer currencies.

Parametric insurance solutions in operation work on a pre-agreed event loss, not indemnity, and eliminate complexity of loss investigation, giving customers the confidence of a cash payment close to the event occurring. Transparency is the cornerstone of parametric solutionsso provenance in the supply chain is the root of the process. This is well aligned to intangible risks where no physical asset exists, but cash flow events need to be insured. The components of a parametric contract consists of a peril, trigger(s) and the limit of pay out which does not exceed the value of the client losses. Having actual risk data from the supply chain provenance will improve the basis risk of the cover and reduce reliance on assumptive modelling. Limits can be tiered or paid out in full when triggered. The Port of Long Beach was recently subject of a successful parametric solution[x] wherein a major importer was concerned about supply chain disruption if the port went off-line due to earthquake. The parametric policy specifying the earthquake magnitude trigger was issued for the benefit of the importer. The need for real-time analysis of risk comes from the increasing exposures in the marine and aviation sector of increasing digitization, increasing port size, delays, cargo turnover, autonomous transport all in combination leading to larger risk accumulations. Some ports, especially in Asia, are advanced IOT facilities with reduced human intervention.

Supply chain perils could be cyber-attack, logistics delay, IT outage at a port, earthquake, or typhoon, for example. For cyber risk mitigation techniques are required. When covering IT networks and large facilities there is no single point of failure in the SOC (Security Operations Centre) due to multi cloud environments. The whole SOC and endpoints within need real-time snapshots of liability evidence from blockchain monitoring acting as a trigger to pay the claim. In duration delay there is a need to quantify lost revenues/related extra costsof such a disruption to check for historical data in order to get frequency. Then trusted datasets are wrapped around the key exposure in order to create the triggers in the contract. The question is, will insurers want to use automated smart contracts in parametric constructs?

Third party independent data is key to the trigger process such as weather data, flight delay details, port delay index and when smart contracts are used, these external data feeds are called oracles in blockchain vernacular. These feed and trigger a smart contract automatically. Underwriters would like a short period of manual investigation rather than to just allow the smart contract to trigger automatically but in the IOT sensor world there is no human interaction. To minimise basis risk (false triggering) the smart contract often does not rely on one oracle but uses a consensus approach where the multitude of sensor data can be benchmarked, and outlier data points removed. The immutability of smart contracts holds risk for underwriters as they are irreversible transactions and programming bugs can have major consequences as in the 2016 DAO hack[xi]. AI can help to make programs safer and to detect errors early. The absence of errors in smart contracts is an essential underwriting item for the widespread use and acceptance of such solutions for parametric insurance.

Nano satellites and earth observation provides insurers with a geospatial overview of supply chain global risk exposure. Event tracking from manufacturing to transport, optimising cargo cost, minimising environmental impact and then matching cargo and location delivery with climate change measurement to optimise the last mile. Precise locations of warehouses harmonised in the cloud allow insurers can see how their risk is spread and where high accumulations occur. It is not unusual to sign data from satellite close to the origin of the datafor provenance as done in the military/defence supply chains.


## Impact on Insurance Opportunities

Trusted, granular data is available from these ecosystems. It enables data driven underwritingwhich provides protection against a wider range of intangible perils such as cyber, crypto, supply chain and Intellectual Property (IP). The more transparency an insurer receives regarding supply chain exposures, the more insurable the risk becomes, hence the value of the digital tokens which mitigates access to suppliers of suppliers, a risk in supply chain insurance, as due diligence is often not done on all suppliers in a hierarchy. Global supply chain changes are already driving new insurance with Swiss RE estimating a $1 T. investment over the next 5 years to construct new logistic and construction facilities generating $65 B of insurance premium. The diagram illustrates intangibles in the outer ring.


Source: Swiss Re Institute.

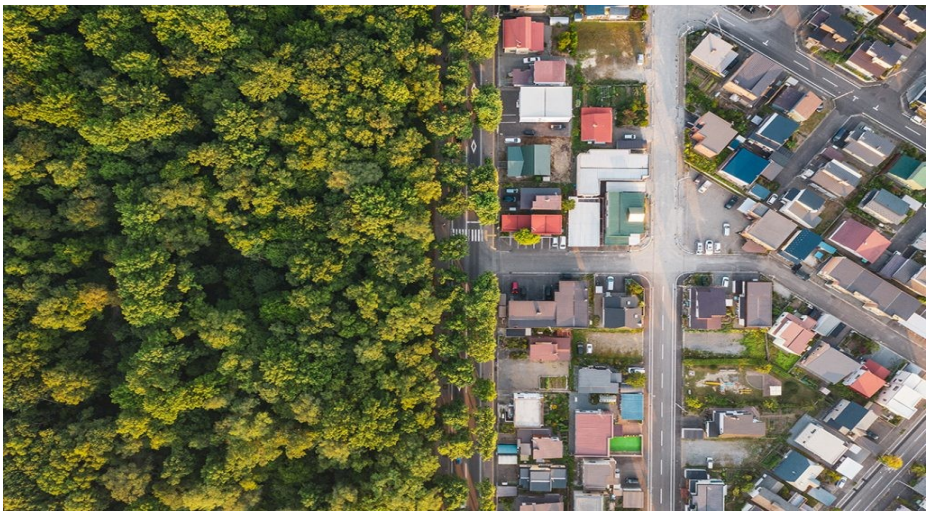
With trusted data appearing at supply chain touchpoints, more premium will be generated at lower cost of claims. Traditional indemnity insurance will continue in the post pandemic commercial world for physical business interruption but blockchain developments with parametric insurance will have a significant impact on Non-Damage Business Interruption (NBDI) where the damage is of a non-physical nature.

NDBI policies protect earnings following events that could trigger claims such as electricity, blackouts, strikes, cyber-attacks, pandemics, and hotel occupancy, so that companies are coveredfor profit losses and expenses incurred ensuring business continuity and any contractual fallout in the contingent business chain.

For the taxi and property sharing companies, physical damage is less of a risk priority than those related to cash flows which affect their share price, market valuation and reputation. Corporations need to provide data about their supplier hierarchy by modeling and monitoring production flow to identifying the risks inherent in a supply chain including transport and logistic vulnerabilities. Natural and man-made catastrophes also pose accumulation risk forinsurers and need to be correlated as an enterprise holistic model.

Lloyd's of London has launched a business interruption cover for SMEs based on a parametric policy[xii] wherein the parametric trigger protects against critical IT disruption/downtime. This could apply to services such as cloud, e-commerce, or e-payment systems. The Insurtechindustry (now valued at $7.1 B[xiii]) is exploring avenues to gather new streams of data via blockchains that can help offer innovative solutions to customers.

Intellectual property is another intangible asset getting attention from the blockchain developers and IPwe[xiv] have recently brought global patents onto blockchain with an AI layer, tokenising with NFT and offering insurance along with the token-based asset.



## Supply Chain Risk Management and Governance

Improving supply chain sustainability is vital in achieving the UN's SDG sustainable goals. Solving the visibility (provenance) and trade finance gap problems go a long way towards addressing sustainability. Technology is required to get transparency to track carbon footprints and "green smart contract" implementations become standard as they create trusteddata sharing between IOT devices in electricity reduction, utilising efficient cloud computing environments. Carbon credit tokens can be used to track the impact of climate change at various stages of the supply chain which can then be traded on a carbon exchange marketplace. Products made in one country may carry a higher carbon tax than others.

Supply chain cyber-attacks are increasing, endangering critical infrastructure. Corporations face class action lawsuits over alleged lack of data integrity that leads to a ransomware attack, causing delays and higher consumer prices. Sound underpinning of data, cyber and machine integrity in the cloud is required to protect customers from accidental or malicious cyber events. Third parties get an accurate snapshot of any supply chain stage with immutable evidence of liability with information available from IoT devices, shipping, airlines, port authorities, weather, news feeds, and satellite tracking sharing data through cellular networks. This evidence will stand up in a court of law and can be used as forensic evidence for subrogation since the truth of the whole supply chain can be independently verified.

Supply chain risk transfer leans towards "first time" SME captives as a response to price increases in a hardening market. SMEs can lower cost for additional capacity, controlling the level of risk they retain versus what they transfer to the market. Reinsurers are offering SMEs multi-year virtual captive contracts held on their balance sheet where no claims bonus type payments flow back to the SME. However, digital worlds need digital captives.

Captives are a niche within corporate insurance and the last frontier for digitisation. A digital, flexible, lightweight captive can be formed on the blockchain with interoperability that manages a captive insurance programme to serve the individual needs of SMEs. Risk data collection can manage issuance of policies inwards/outwards, collect premiums and handle claims using parametric techniques from smart contracts. This is a "captive in the cloud" securely delivered over the internet. Stored in the cloud, the responsibility for maintenance and performance of this service is removed from the day-to-day activities of the captive manager. Cloud -based captive platforms allow infrastructure-free access tocaptive management technologies and remove the margin of cost.

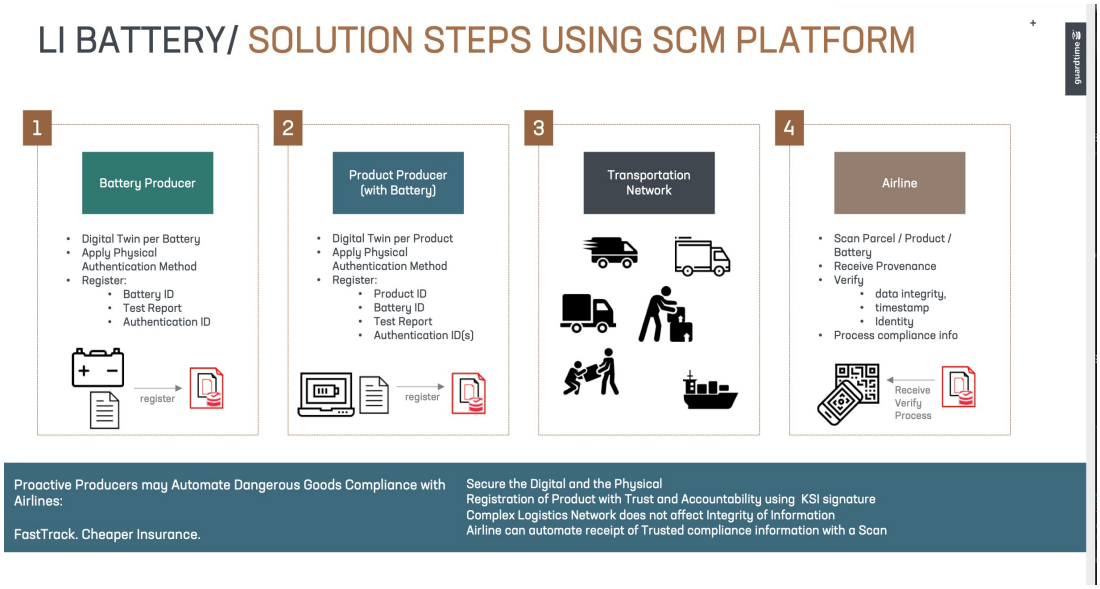
Balanced regulation is important for the digital world project success and regulators must adapt. Industry 4.0 is pushing the limits of established law which was not designed to handle digital tokens. Having 20$^{th}$ century law for 21$^{st}$ century technology entails arbitrage risk, so regulators need to be part of the ecosystem in real-time. By automating certain regulatory rules, a level of self-governance can be achieved based on trusted data that passes the privacy law and financial security trading test. For the supply chain we have to be very clear on the purpose and usage of tokens and how they are constructed as smart contracts.

Smart contracts are the crossroads of information technology, regulation, and law. Standards are still being developed. Given the extent of tokenisation, without standards, due diligence is needed to cover smart contract failure risk and the captive route may be the risk transfer approach, especially crypto currency lending. This topic is moving fast in legal circles.

Digital tokens operate in multiple ways and can form part of an investment contract, payment exchanges and also complete digital platforms. Providing access to actual risk data and early warning cyber alarms, they enable risk management as a service in a digital ecosystem. This allows risk accumulation in real-time which quantifies effects on insurance risk pools. A DAO (decentralized autonomous organisation) is a corporate entity on a blockchain platform and operates like a digital mutual company so this will have impact on how insurance is enacted and regulated moving forwards. This is symbiotic to Takaful insurance, cooperatives and microinsurance. Every industry has different regulations/compliance and different datasets required for their regulators. A typical brand owner in a supply chain may conduct multiple supplier audits a year. These are expensive and unreliable due to the need to trust the suppliers who are providing the data. Implementing blockchain in supplier processes would provide a much higher degree of certainty and enable the automation of these audits on demand without any possibility of insiders or malicious outsiders interfering with those processes. Product recall is also an expensive and brand-damaging exercise.  Providing global visibility of product location and state provides precision in recall management.

## Lithium Battery Case Study

The lithium battery conflagration risk is a serious supply chain problem of our time. Primarily an aviation safety problem, it applies to all transportation.  Raw materials come from South America, batteries are made in Japan/Korea, product manufacturing is in Mainland China and air transportation/customs goes through ports such as Hong Kong. Re-export crossborder cargo systems find it difficult to identify unsafe batteries in each shipment. Lithium batteries are often mis-declared or under-declared. Identifying liability and responsibility on the parties involved in the shipping process is challenging. There is a risk of fire while being transported and the fire is inextinguishable due to intense heat. Compliance and visibility upstream/downstream needs addressing by a blockchain approach to avert serious events with loss of life.  Already there have been many incidents caused by forged documents and fabricated testing reports. Counterfeit and recycled batteries often do not meet the standards and enter the supply chain. As many products contain these batteries, the magnitude of the problem is exponential as these are dangerous goods. In 2020 there were estimated to be 18 billion lithium batteries in the transport handling system with numerous fire events. The solution is to create trusted digital provenance of lithium batteries using digital twin techniques so that they can be readily verified by customs and cargo handlers. All records have full immutability and accountability so we can link back to the producers of the whole lithium battery supply chain so the captain of the plane/ship can trust and verify the cargo.




The battery manufacturer creates the physical asset with a bar code and a digital twin tokenis assigned to create a cryptographic seal of the origin of the battery which contains identification, certification, originator and registry, binding data to the blockchain. As the asset travels through the various stages of the supply chain the token is verified for accuracyby an independent app without having to go back to any centralised system. At each stage, anew updated token is created, reflecting any change of ownership which starts a chain of provenance. Once it leaves the order stage, the digital twin reflects the provenance and each recipient can reflect the authenticity of the asset.

Standard message syntax between tokens provides access to control enforcement, secure data transfer and data lineage history provides a cryptographically sound history of any data asset which is independently verifiable at the airport/seaport. Tokens are nested with previous tokens providing cryptographically linked events. An ecosystem is onboarded from the manufacturerof the battery to the manufacturer of products, to logistics and cargo handling, to customs and then to airlines and ships where the captain could use a verification app to see a trusted chain of custody in the cargo. The battery manufacturer association would be a signing entity for the goods. Should a counterfeit or rogue recycled battery enter the supply chain the token will give an alert. The importer of record and customs agent have access to secure original copies of all events in supply chain and verification tools to verify that the cargo is as per declaration. The customs agent also has a detailed, reliable, and ever-increasing history of entities and actions that can be used for anomaly detection.

## Conclusions

The global supply chain community received a 1-2 punch in 2020 with a pandemic and cyber-attacks with no robust preparedness for either. The use of blockchain technology to transform supply chains was already underway but not in time to address these major events.The result was government chaos, transport delays, fraudulent activity, counterfeit goods, anda marked increase in the global trade protection gap as SMEs failed to get the supply chain finance they needed. The increased cyber activity is very concerning as bad actors chose to attack supply chains at various points of failure in software and data, affecting multiple computers at once and coming one step closer to a major critical infrastructure event.

Ransomware events increased 25x in the last year and this is a peril that can be addressed by data integrity. Despite the best intentions corporations at board level did not invest enough indata integrity mitigation and failed to break the kill chain of enhanced visibility into attacks. Ransoms paid alone are significantly higher than the cost of mitigation. It is important moving forwards that insurers know for sure to what extent insureds attempted to mitigate and the industry should not be concerned to incentivise their customers for proper data maintenance and good safety practices the same way as they did with anti-virus and encryption software. Accelerated digitization, adoption of multi cloud strategies and machine to machine communication means there is no longer a single point of failure and corporations must adopt multiple dimensions of security posture and monitor data in real-time as a critical asset. By installing provable compliance, human configuration error can be prevented. Use of trusted granular data and third-party evidence ushers in a better era of risk transfer around ILS and parametric insurance and digital captives to house both cyber and supply chain risk.

Within the parenthesis of cyber/data integrity, supply chains are at an inflexion point to embrace an ecosystem model where all the participants share and work together in permissioned environment to secure and be incentivised on safe trades. Giving total visibility upstream and downstream in the supply chain mitigates against perils such as lithium battery fire on board transport. Similarly, breakdown through lack of supply chainfinance threatens sustainability and hinders efforts to create a greener supply chain.

Answers lie in technology and the data protection aspects of blockchain as well as removing trust deficits between participants. New technologies should not be adopted lightly. It is plainly obvious that recent events coupled with Industry 4.0 change require global supply chains tohave a serious industrial change on how we approach trade. The adoption of digital tokens, such as NFT, means we can connect the digital and physical worlds to great benefits, and we are seeing the advent of digital twins in seaports and airports. The digital world has significant advantages over the physical world in the fact that distances can be overcome without loss of time. The time factor itself takes on a different meaning because time can easily be retraced and objects can be copied and duplicated without further effort.

It is important to mention additive manufacturing or 3D printing. Shortage of PPE during the pandemic resulted in a shift to local manufacturing and this will continue and extend to other areas such as making spare parts on board ships to reduce maintenance stops at ports. This situation has allowed companies to take a detailed look at what steps are necessary to create adigital inventory so that parts can be printed from the cloud and integrated to supply chains. The following chart summarises the benefits of applying the strategies in this paper.

| | |
|---|---|
| **Digitization and Automation** | Remove dependencies on manual paper-based records, provide electronic standardisation |
| **Track & Trace** | Digital Twin will allow provenance records on goods to be maintained and updated |
| **Trust Mechanism** | New Trust Mechanism establishes trust in all participating entities in a supply or trade chain together with trust in trade data, provenance data etc.<br>This mechanism must allow for independent verification by third parties. |
| **Scale** | Continue to perform and respond when applied to large scale problems |
| **Privacy** | Allow controlled sharing of business data through permissioning on a need to know basis |
| **Interoperability & Integration** | Allow for interoperability and integration with existing systems |
| **Access** | Allow access by first and last mile users to enable true visibility across entire trade and supply chain; also allow controlled access by governments and customs offices |
| **Incentives to Business** | Appeal to businesses in terms of benefits, cost and functionality |
| **Adaptable** | Retain high degree of adaptability to allow incorporation of future technology (e.g. relating to anti-counterfeit measures) and avoid getting stuck with static legacy technology in the future. |

In conclusion we have addressed evaluating cargo at the border to visibility, data integrity and accountability over the time and distance of the import value chain with threat of cyber risk and fraud mitigated in cyber space. We have provided a cross-boundary, independently verifiable trust mechanism provided to underpin ERP systems, providing a cross-platform interoperability in a sustainable manner. This greatly enhances insurance touchpoints and willincrease liquidity and add tangible value, previously intangible, to balance sheets.

## References


[i] https://www.swissre.com/institute/research/sigma-research/sigma-2020-06.html
[ii] https://www.adb.org/news/global-trade-finance-gap-reaches-16-trillion-smes-hardest-hit-adb
[iii] https://www.sc.com/en/feature/global-trade-now-faces-a-us3-4-trillion-financing-gap/
[iv] https://sdgs.un.org/goals
[v] https://www.gtreview.com/news/global/icc-covid-19-recovery-will-need-us5tn-in-trade-credit-capacity/
[vi] https://www.ft.com/content/25fdb537-adf2-4c82-ad6d-7421898e4b7c
[vii] https://nntc.digital/news/nntc-announces-partnership-with-saiber-innovation-technologies/
[viii] https://www.oecd.org/trade/topics/small-and-medium-enterprises-and-trade/
[ix] https://www.forbes.com/advisor/investing/nft-non-fungible-token/
[x] https://www.munichre.com/en/solutions/for-industry-clients/parametric-solutions.html
[xi] https://pullnews.medium.com/understanding-the-dao-hack-for-journalists-2312dd43e993
[xii] https://www.reinsurancene.ws/lloyds-launches-parametric-policy-for-business-interruption/
[xiii] https://www.willistowerswatson.com/en-HK/News/2021/01/record-high-insurtech-funding-of-dollar-7-point-1-billion-achieved-in-2020
[xiv] www.ipwe.com
[xv] https://www.ericsson.com/en/blog/2020/12/digital-twins-port-operations


## Acknowledgements


Thanks to Guardtime (www.guardtime.com), SICPA (www.sicpa.com), CREW ASSIST (www.crewassist.org),Mar Sec Alliance (https://marsecallince.com) Alex Korb, Pradeep Luthria, Jonathan Jones

6.2021

**David Piesse**
**CEO, DP88**

**About the Author:**

*David Piesse is CEO of a family office, DP88, specialising in InsurTech initiatives in Asia - www,DP88.com.hk. David has held numerous positions in a 40 year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.*