AGENDA: SUPPLY CHAIN – SHEILA WARREN AND RADHIKA IYENGAR-EMENS

Outline

1. Background
    a. Supply chains: present state
    b. Operations in CA – **who can provide?**
    c. [TODO] Scale of stakeholders/market size in CA (number of people, $)- **who can provide**?
2. Blockchain Technology
   How might it add value? Benefits
3. Use Cases
4. Digital identity, data protection, cybersecurity
5. Implementation

. A. Framework for evaluating deployment (link to WEF Blockchain for Supply Chain toolkit)

B. Best practices/successes

C. Worst practices/failures

6. Recommendations: Legislation
7. Bibliography

Adapted from Inclusive Deployment of Blockchain for Supply Chains: Part 1 – Introduction, March 2019, World Economic Forum, by Sheila Warren, Christoph Wolff, and Nadia Hewett

Distributed ledger and blockchain technology promise to have far-reaching implications for supply chains. In fact, providing increased efficiency, transparency and integration throughout supply chains has been one of the most fertile areas for blockchain experimentation. Whether or not an organization or business unit is an early adopter, there is a high likelihood that most supply chains will be affected by blockchain technology at some point – whether using blockchain technology directly or at the application level, with connectivity or integration into an underlying blockchain-enabled data layer.

On the surface, the supply chain of the future very likely looks like those we know today, yet behind the scenes we can anticipate far-reaching changes that enable better communication, fewer disputes, higher system resiliency and substantial gains in operational efficiency. The resulting capabilities that blockchain technology can enable range from consumers using their mobile devices to validate the authenticity or pedigree of products before a purchase to insurance providers offering dynamic rates on single supply-chain transactions based on their ability to view transactions unfold in near real time and to validate all requisite events on the blockchain. As digital technologies such as blockchain increasingly encourage higher levels of trust among supply-chain partners, they will have effects on processes in the physical world as well. As a result, fragmentation within and across industries could diminish, the occurrence of errors and exceptions could decline, and operators could require fewer resources to complete the same tasks.

A typical supply chain may involve hundreds or thousands of business transactions every day. These transactions generally take place in a bilateral manner – for instance, between a supplier and a manufacturer or between a retailer and a logistics service provider – and are stored in each of the supply-chain actor's own ledgers. As a product travels from its origin to its destination in a supply chain, there may be many organizations involved. Each holds its own version of "truth" about the product's journey. The multiple ledgers (hence the multiple "truths") often lead to error, fraud, delays and inefficiency. Distributed ledger technology can reduce those complex bilateral communications and informational linkages and leakages by providing a single, shared, tamper-evident ledger that records the transactions as they occur. Transactions on a blockchain are typically confirmed by all participants via a consensus mechanism. Once validated and recorded on a blockchain, a transaction becomes permanent. No single participant, even a system administrator, can delete or change a transaction unilaterally. Therefore, blockchain enables supply-chain actors to share control over access to – and evolution of – the data. While several preconditions must be met, and depending on the type of blockchain, in general all related participants in a business network can simultaneously have an identical copy of the data at any moment in time.

Blockchain Use-Cases in Supply Chains

The concrete value brought by blockchain technology can best be understood based on use-cases. The following section outlines some of the most popular use-cases in the supply chain context to date. This section does not delve into all of the complexities and technical details involved in the application of the technology.

Product provenance and traceability

Due to an increasing demand from customers for the proof of legitimacy and authenticity of the products they purchase, there is a strong interest in the deployment of blockchain for product provenance, often referred to as pedigree. These products range from luxury items, such as diamonds, to aerospace and automotive parts, and organic and fair-trade food products. In general, blockchain has features that can help trace a product's digital footprint. The enhanced data integrity (aided by the immutability feature of blockchain) can lead to increased confidence from customers of products' legitimacy. Moreover, the use of timestamping (the process of establishing a chronological order among sets of events) in the blockchain can prove the existence of certain data at a point in time. The fact that the data is timestamped (tamper-proof) provides a single source of data integrity and allows users to retrieve a full history of activities. Information completeness can be enhanced as well, as blockchain can accommodate a wide range of data, including ownership, location, product specification and cost.

Blockchain is a way to prove the existence of tracking data (as well as the fact that it hasn't been changed) at a given point in time. While blockchain technology can guarantee that the data is not tampered with (the provenance and traceability data cannot be modified), it does not guarantee that the data recorded is accurate. Additional checks and balances may still be necessary to ensure increased data integrity.

Streamlining (global) supply-chain operations

A blockchain-based platform can support the digitization of paper-based documentation, and establish an immutable, shared record of all transactions among network participants in near real time. In this sense, blockchains are suited to large networks of disparate parties and are a solution to making the complexity of global supply chains much more manageable. It is important to note that digitization is a prerequisite for blockchain (digital product identity at some level, for instance, is a prerequisite to traceability using the blockchain). Blockchain technology can enhance end-to-end supply-chain integration. Currently, some companies use enterprise resource planning (ERP) systems to manage their internal processes and other systems – such as customer/supplier relationship management (CRM/SRM) – to interact with their customers and suppliers. They also use communication tools such as Electronic Data Interchange (EDI) and Extensible Markup Language (XML) messaging to enable information flows between different organizations. Together, these systems create somewhat more integrated supply-chain information systems, if only for parts of the data that exist in several places. However, this should not mask the fact that each participating entity still tends to have a limited view of where the products are at all times. While some platforms already aim to provide higher levels of visibility for all supply-chain participants, blockchains make such visibility more secure and immutable for all actors by allowing them to share and agree on important information. This removes data redundancy, double entries and crosschecking, which are very common in today's bilateral communications.

Automation and smart contract

There are still instances where current operations, processes and data exchange in supply chains are manual and error-prone. Secure data-sharing and, specifically, smart contracts allow for increased automation and efficiency through avoidance or redundant data entry, acceleration of transaction execution and reduction of errors and misunderstandings. Smart contracts can help with cascading of purchasing orders, invoices, changing orders, receipts, ship notifications, other trade-related documents and inventory data within a supply chain (Wang et al., 2018).

Trade finance

The Asian Development Bank estimates there was a $1.5 trillion trade financing gap in 2017, representing roughly 10% of global merchandise trade volumes. SMEs (small and medium-sized enterprises) and mid-cap companies represent 75% of the total trade gap. Left unsolved, the trade finance gap will rise to more than $2.4 trillion by 2025, according to Bain & Company estimates. However, a viable solution has emerged. Bain’s modelling estimates that new digital technologies, especially distributed ledger technology, can reduce a large part of this gap, facilitating about $1.1 trillion of new trade volumes globally (World Economic Forum, 2018a). Blockchain used in trade finance helps to remove inefficiencies from existing processes. Over time, it creates records that allow entities such as banks to enhance KYC (know your customer) processes and improve assessments. For example, blockchain can enable processes that can be used for faster credit risk assessment, minimized human errors in documentation checks, instant verification and reconciliation of records, automatic execution of workflow steps via smart contract, and instant and secure exchange of data (World Economic Forum, 2018b). An application is the securitization of assets on the blockchain, which enables them to act as collateral in previously unavailable supply-chain finance opportunities. This securitization allows for financing models, such as inventory financing, to flourish at scale compared to their relatively obscure and cost-prohibitive existence in a pre-blockchain world.

Anti-corruption and humanitarian operations

Trust afforded by blockchain may help prevent supply-chain actors from behaving unethically or opportunistically. Because every transaction builds on every other transaction in a blockchain, corruption or unethical behaviour should in theory be more readily visible to network participants. The technology can make it more difficult for unethical behaviour to occur; however, it is still important to recognize that existing and new checks-and-balances may still be necessary. Equally, a blockchain system could help to expose and eliminate corruption witnessed in certain public-private interactions. Blockchain could increase transparency and trust in humanitarian supply chains as well, where financial aid could not reach or was perceived to be unable to reach target beneficiaries (Hyndman and McConville, 2017).

Pharmaceutical Supply Chains – Adapted from the book, *Enterprise Blockchain Has Arrived*, copyright May 2019, by Radhika Iyengar and Jorden Woods

Introduction

In the life sciences sector, drug supply chains have challenges of limited data sharing and lack of process visibility which have led to a global epidemic of drug counterfeiting worth $200 billion globally. In the US, the Drug Supply Chain Security Act (DSCSA) was passed in 2013 and is focused on effectively combatting counterfeit drugs through drug serialization and traceability to ensure a safe and secure medicine supply chain. Since battling counterfeit drugs requires ecosystem cooperation across supply chains, centralized solutions have proven ineffective. The FDA, which oversees DSCSA enforcement, is actively evaluating blockchain solutions and providing a regulatory tailwind to the technology. Similar efforts are on-going in Europe.

The US has the highest rate of pharmaceutical spending per capita among the OECD, double that of the 10 highest income countries. An analysis of the expenditures shows that the US is comparable to other developed nations in the use of generic drugs with 83% in the US. This means that the high-priced branded pharmaceutical drugs account for the large discrepancy. High prices for pharmaceutical drugs and a thriving global shadow market for prescription drugs have created a megabillion-dollar counterfeit drug problem globally. The collateral damage includes higher costs for illness, and the hospitalization and premature death of hundreds of thousands of adults and children globally.

The high levels of inefficiency and fraud in healthcare systems arise from lack of data and process transparency, insecure data, and data siloing within organizations. As noted previously, permissioned enterprise blockchain systems are ideal for spanning ecosystems to increase data and process transparency, increase security, and improve data sharing between organizations. As a result, there is a strong conceptual fit between enterprise blockchain capabilities, and the type of solutions needed for the healthcare ecosystem.

Fighting Counterfeit Drugs

The global pharmaceuticals industry is big business, valued annually at $1.2 trillion. Pharmaceutical companies spend tens of billions of dollars and go through an arduous process to produce and commercialize prescription drugs. According to the World Health Organization, the counterfeit prescription drug trade is 10% of the global market.

Fake drugs for every therapeutic treatment exist, with a majority of falsified drugs targeted to chronic illnesses, antibiotics, antivirals, as well as alimentary drugs such as cholesterol and diet pills. In the US, we are also seeing demand for opioid drug, particularly those with fentanyl, a synthetic opioid. According to the Centers for Disease Control (CDC), fentanyl-related overdose fatalities are rising exponentially – from 2013 to 2016 fatal overdoses involving fentanyl have doubled each year, leading to tens of thousands of deaths.

With the mega billion-dollar global counterfeit drug market annually, there is a clear motivation in the pharma sector to fight counterfeiting. What is also at stake are human lives, with adverse reactions and effects to these fake drugs leading to illness and hospitalization and fatalities. In emerging markets, 10-30% of prescription drugs are counterfeit, and in certain parts of the world, up to 50% are fake. Issues range from tampered drugs to drugs with incorrect, often toxic, ingredients or incorrect proportions of ingredients.

Most of the counterfeit drugs are being produced in China and India but sold worldwide. A very relevant example of this type of fraud is the China vaccine scandal of 2018 where a government vaccination program was found to have administered hundreds of thousands of faulty vaccines to young children. In the US, the DEA (Drug Enforcement Agency) continues to conduct raids of fentanyl opioids. Various studies have shown that most of these opioids in the US are coming from China. In April 2019, China acknowledged the severity of the crisis and issued a ban on all fentanyl-related substances.

Globally, with the rising awareness of the impact of counterfeit drugs on public health, there have some major regulations forcing the pharmaceutical industry into compliance. In the US, the Drug Supply Chain Security Act (DSCSA) was passed in 2013 to require electronic serialization and traceability of all pharmaceutical drugs from manufacturer through distributor to consumer. Compliance is expected by 2023 with the critical milestones beginning in November 2019.

To assist with achieving compliance with the DSCSA, the FDA began a pilot project program in May 2019. The FDA selected 20 participants as part of the pilot program to evaluate and explore different methods of achieving compliance. Blockchain technology provides an immutable, shared source of truth and, when combined with serialization and smart sensors, can provide an effective method of establishing a safer and more secure drug supply chain.

Of the 20 participants in the pilot program, the FDA selected at least seven participants that are using blockchain-based technology platforms working to provide compliance with the DSCSA.[8] These include projects with MediLedger, the IBM/KPMG/Merck/Walmart, UCLA Health, Rymedi, The Optimal Solution, TraceLink, and IDLogiq. These initial pilots are positive and suggest that a blockchain-based solution will enable compliance with the Drug Supply Chain Security Act (DSCSA) while improving operations and reducing the supply of counterfeit drugs.

Europe's Innovative Medicines Initiative (IMI) is the world's largest public-private partnership between the European Union and the European Federation of

Pharmaceutical Industries and Associations (EFPIA) providing funding to health research directives, particularly to develop better and safer medicines. The IMI is allocating 18 million Euros to a Blockchain Enabled Healthcare initiative. The goal of the initiative is to create a common blockchain-based framework for the European pharmaceutical ecosystem enabling collaboration on common issues such as mitigating counterfeit drugs and improving shared data access.

The IMI Blockchain Enabled Healthcare initiative includes Europe's most prominent pharma companies including Novartis, Janssen | Johnson & Johnson, Bayer, Sanofi, Novo Nordisk, Pfizer, AstraZeneca, and AbbVie. A major push is in the counterfeit drugs battle, spurred by the Falsified Medicines Directive (FMD) regulation passed in 2011 to ensure the authenticity of medicines.[11] The regulation specifies that only licensed pharmacies and approved retailers can sell pharmaceuticals, including online. Compliance is being enforced as of February 2019 to have 2 safety mechanisms placed on the packaging of every pharmaceutical drug, a unique identifier and an anti-tampering device.

At the root of global pharmaceutical fraud is a supply chain transparency and product authenticity problem. Without transparency in the supply chain it is very difficult to pinpoint the origin of the fraud, identify the bad actors who perpetrated the crime, or verify product authenticity. What is needed is for the entire process, from production to quality assurance to distribution, to be secured in a secure database with each entry cryptographically signed and encrypted. This capability, and its resulting transparency, is exactly what blockchain technology provides.

Like in the case of food safety, the blockchain ledger can provide end-to-end transparency for drug production and distribution, including visibility into every stage of the supply chain. The implications of this level of detail are enormous. Not only does blockchain technology improve the traceability of prescription drugs in the supply chain, it can also ensure that international standards are upheld, such as GDP (Good Distribution Practices), ensuring the integrity and quality of the medication for the end user.[13] Additionally, it will also be much more difficult for bad actors to tamper with the process or for pharma companies themselves to market fraudulent products. It is for this reason that the blockchain community in China has called for placing all vaccine data on a transparent blockchain system.

With regulatory tailwind, the deployment of blockchain-based solutions has the potential to protect consumer safety and public health, restore consumer trust in pharmaceutical drug supplies, as well as bring operational efficiencies and restored brand trust for pharmaceutical companies.

Key Deployments

The key consortia for combatting drug counterfeiting include (all are in development):

- **MediLedger** is focused on pharmaceutical drug compliance with the DSCSA. It was accepted into the FDA pilot program in 2019. MediLedger was started in

2017 and includes 25 members that span many major pharmaceutical companies, retail pharmacies, and medical distributors such as Pfizer, Amgen, Genentech, Lilly, Gilead, Novartis, Sanofi, GlaxoSmithKline (GSK), Walmart, Walgreens, McKesson, Cardinal Health, Amerisource Bergen, FedEx, and others. Chronicled is the main technology partner. Product authenticity is required under the law by November 2019 for saleable returns, a $6 billion market in the US. The network plans to launch just prior to the deadline. MediLedger is built upon Parity Ethereum, which is a permissioned version of Ethereum for enterprise environments). It will use zk-SNARKs for privacy.

- **IBM/KPMG/Merck/Walmart** consortium is focused on compliance with the DSCSA. It was accepted into the FDA pilot program in 2019. The pilot is focused on traceability of vaccines and prescription medicines within Merck's supply chain and is using IBM's Hyperledger Fabric permissioned blockchain framework. The application will enable end customers to scan a QR code at pickup to see the provenance and authenticity of the product by providing information such as manufacturing site and duration on store shelves. The pilot project results will be available in Q4 2019.

- **Rymedi consortium** was selected by the FDA in 2019 to take part in the DSCSA pilot program. It is focused on data transparency and integration in health system transfers from manufacturer to pharmacy through to patient medicine use, with the purpose of providing real-world evidence and traceability. It is being deployed with various health systems in North Carolina, Indiana and Tennessee, and includes Good Shepherd Pharmacy and RemediChain, Rymedi, Temptime/Zebra Technologies, Indiana University Health, WakeMed Hospitals and Health, the Center for Supply Chain Studies, and the Global Health Policy Institute. While Rymedi is providing the blockchain platform to integrate upstream supply data, Temptime/Zebra Technologies is providing temperature monitoring targeted to specialty medicines.

- **IMI Blockchain Enabled Healthcare** is an EU-based initiative focused on developing a blockchain technology framework to address issues of drug counterfeiting, secure health data sharing, and more efficient clinical trials. It will address issues such as digital identity, off-chain storage, security, and scalability. The initiative is a public private partnership that includes 8 large European pharma companies including: Novartis, Janssen | Johnson & Johnson, Bayer, Sanofi, Novo Nordisk, Pfizer, AstraZeneca, and AbbVie in partnership with UCB Pharma. It will also include other members of the ecosystem including academia, health authorities, clinical research, hospitals, supply chain partners, patient representatives, and blockchain SMEs. The consortium is to be funded with 18 million Euros and is planned for launch in Q4 2019.

Use-cases	Description	Supply-chain objective	Examples
Product provenance and traceability	Blockchain-based systems support safeguarding the accuracy of product certificates and reduce risks of fraud and adulteration.	Improved product safety, authenticity, provenance and pedigree resulting in a reduction of fraud. The provenance link also helps producers and channel partners to create more intimate ties to consumers. Equally important, tracking goods throughout the production process improves the accuracy of forecasting and collaborative planning within the supply chain.	OriginTrail solution delivers verifiable supply-chain traceability and product authenticity, with existing applications including traceability for GMO (genetically modified organism) -free dairy products, free-range poultry and fresh vegetables, preventing counterfeiting in wine exported to China, and an integration with the internet of things (IoT) smart products platform.[2] Skuchain's solution enables tracking of goods on the stock-keeping unit (SKU) level and their transformations in production, particularly useful for tracking critical components such as sub-assemblies, parts and raw materials used to make finished products·[3]
Streamlining (global) supply-chain operations	Blockchain enables efficiencies for information transfers and data-sharing as well as for transaction execution among multiple entities in a supply-chain environment.	To digitalize global trade ("paperless trade"), provide end-to-end visibility and allow secure information sharing between organizations. This allows parties to take full advantage of essential blockchain features (information cannot be altered, more secure and jointly agreed upon) when sharing or transferring electronic documents or other information.	A few solutions exist today where blockchain is used to automate and digitize the bill of lading (BOL) or other trade documents. Examples include Wave[4] and CargoX.[5] Ocean carrier Zim (using Wave's solution) offers customers the opportunity to switch to blockchain-based electronic BOLs on select trades.[6] Separately, some port community systems (members of International Port Community System Association/IPCSA), carriers, shippers and banks participate in the development of a BOL proof of concept based on blockchain and smart contracts.[7] Truckl, a start-up focused on over-the-road transportation, writes every supply-chain event that occurs to the public blockchain, enabling higher trust between supply-chain partners while ensuring that parties act responsibly.[8]

Automation and smart contracts	Blockchain systems can automatically enforce rules and process steps. Once launched, smart contracts are fully autonomous: When contract conditions are met, pre-specified and agreed-to actions occur automatically.	To increase transaction efficiency through faster and more automated supply-chain processes, which takes cost out of the supply chain and also enhances the trust multiple parties place in each other.	The IPCSA example above exploits smart contracts for BOLs. The smart contract controls the endorsement process of the BOL while the application synchronizes the logistic process for entities holding the BOL. In addition, delivery orders are released automatically upon the presentation of the BOL from the importer back to the import shipping agent.[9]
Trade finance	Bringing trade finance products and processes (such as a letter of credit) onto the blockchain enables more secure commercial transactions as well as the sharing of information between exporters, importers and their respective banks on a secure blockchain-based platform.	To enable secure financial transactions in global trade along with increased efficiencies for transactional processes and reductions in operating costs.	Project Voltron (Documentary Credits) and Project Marco Polo (Open Account) each provide solutions that expand finance to a greater number of SMEs and introduce new opportunities to finance trade.[10] The Bank of America Merrill Lynch (BofAML), HSBC and the Infocomm Development Authority of Singapore (IDA) have developed a prototype to bring the paper-intensive letter of credit (L/C) process onto a blockchain (DHL, 2018).

Anti-corruption and humanitarian operations	Blockchain can deter supply-chain actors from behaving unethically or opportunistically while providing a full audit trail of the spending of financial aids.	To build a “fairer”, transparent, efficient and more reliable humanitarian supply chain.	The World Food Programme’s Building Blocks pilot project uses blockchain technology to help refugees of the Syrian Civil War. In the Azraq refugee camp in Jordan, 10,000 people receive food from entitlements recorded on a blockchain-based computing platform. Refugees purchase food from local supermarkets in the camp by using a retina scan instead of cash, vouchers or e-cards (WFP.org, 2017).

Digital Identity

(Adapted from Inclusive Deployment of Blockchain for Supply Chains Part 2 – Trustworthy verification of digital identities, April 2019, World Economic Forum, by Derek O'Halloran, Manju George, and Nadia Hewett)

Digital identity ensures integrity in connecting the physical and the digital world. In digital supply-chain transactions, it is essential for a legal entity to prove its own identity and check those of other parties, each of which requires a unique, verifiable and authentic digital identity.

Supply chains span borders and involve businesses from different industries; actors need to work collaboratively to optimize the flow of physical goods, information and financial transactions. Identity and trust assurance lie at the core of each of these interactions. Supply-chain organizations need to know and trust each partner they are engaging with, prior to offering digital services or access to resources. Organizations need to ensure they are dealing with the right entity and efficiently link a digital identity and a real organization, and more importantly evaluate the trustworthiness of a legal entity of interest. This process of dynamically verifying counterparts – digital identity management and verification – is a critical step in establishing trust and assurance for organizations participating in digital supply-chain transactions.

Today, most identity systems exist in isolation. Different public and private solutions record and maintain identical identity data potentially hundreds of times over, and are not interoperable, creating a significant amount of redundant identity information. This is a waste of resources for the network in question, is difficult to scale and is buried in errorprone and paper-heavy processes. Decentralized systems, such as blockchain, can encourage the development of digital identity. However, where existing laws and regulations have been drafted to consider digital identity (e.g. the eIDAS regulations in the European Union), they have tended to be drafted with a traditional view of data and digital identity – i.e. based on centralized, rather than decentralized systems. This means the regulations are not fully consistent with a decentralized system of digital identity, therefore organizations could miss out on a potentially promising archetype. California law generally similarly presumes a centralized system. Tracking emerging concepts in identity management will be a critical part of effective regulation in the supply chain space.

Data Protection

(Adapted from Inclusive Deployment of Blockchain for Supply Chains: Part 4 – Protecting Your Data, September 2019, World Economic Forum, by Anne Flanagan and Nadia Hewett)

The deployment of blockchain and other distributed ledger technologies in supply chains can offer considerable advantages. Nevertheless, their deployment and implementation can raise concerns about how best to both meet data protection laws and protect commercially sensitive data. Supply chain actors may be unwilling to take on what they perceive as additional legal risk, especially if data protection obligations become, or are seen to become, unduly burdensome. The California Consumer Privacy Act, for example, is at the forefront of a new wave of data protection legislation globally, and brings with it important practical and regulatory obligations, with the potential for significant penalties in cases of non-compliance. With respect to safeguarding commercially sensitive data in supply chain transactions, the deployment of blockchain may lead to a perceived loss of control, raising questions about security, access rights and how to structure blockchain solutions: e.g. whether only some subsets of data should be shared on the blockchain and/or whether data sharing should be limited to only those parties involved in the transaction.

In the course of selecting and deploying a blockchain solution, a supply chain operator should understand how blockchain protocols address both their data protection and privacy concerns4 and those of other supply chain partners (including any concerns about potentially revealing commercially sensitive data) early in the process so as to ensure that such concerns can be adequately met for all supply chain partners. However, in Deloitte’s 2019 Global Blockchain Survey, half of respondents cited privacy-related regulations as a matter of concern – markedly more than any other choice of blockchain regulatory issue.5 In many cases, data protection and privacy are enforced by legislation, e.g. the GDPR, or by commercial or supplier/ client contract (covering client or commercial confidentiality), but blockchain technology affects how we address these protected rights and legitimate commercial concerns and can require complicated analysis.6 This paper aims to provide an overview of the most common concerns regarding (a) data protection regulation; and (b) commercial confidentiality as raised by supply chain actors when considering blockchain solutions.

No supply chain actor will share its commercially sensitive data (whether via blockchain or otherwise) with its supply chain partners unless it can maintain its current competitive and informational advantages. The following outlines the most common baseline requirements for sharing data. Each of the examples is a real use case, with names hidden to protect confidentiality.

Transactions in a supply chain ecosystem cannot be fully transparent

While supply chain actors are interested in using blockchain precisely because it allows for transparency and visibility across multiple tiers upstream and downstream, it is undesirable to reveal data to this extent. First, many critical operational points in supply chains rely on a lack of transparency. One particular supply chain, for example, may legitimately try to enforce a lack of visibility about the identity of upstream suppliers, the prices paid by downstream suppliers, the true length of a cash-conversion cycle, the status of regulatory compliance, true levels of demand

and available inventory, and details about the production process. Secondly, if confidential information such as trade secrets needs to be revealed to regulatory bodies, for instance, customs and oversight agencies, they are revealed for compliance purposes only and in strictest confidence. This information cannot and should not be shared across the supply chain where it would be visible to other actors. Even if this data is aggregated without important identifiers, the possibility of analysing trends and patterns for economic advantage is too great for most supply chain partners to consider this level of openness.

Confidential information has to stay confidential

One may wonder why two supply chain partners transacting with one another would want to keep certain information from the other and yet log that information onto the blockchain. There are two reasons: – They believe that there is value in having the blockchain serve as a single source of truth for authenticated supply chain data so that participants can extract the particular data they need, and – The practical challenges of understanding what should be obfuscated and what can be revealed during a oneto-one integration process are too immense.

Companies want to use ecosystem data in forecasting and planning without revealing raw data

Collaborative planning across a supply chain based on the sharing of accurate demand forecasts, inventory levels on hand and production estimates has long been a goal for optimizing supply chain operations. In terms of logistics, ocean carriers need rolling forecasts from their customers while inland rail operators need to know the number of inbound containers from the ocean liner and port a few weeks in advance to plan a schedule and allot resources. These are just a few examples of how the increased flow of information across an ecosystem can lead to greater efficiency and ontime delivery. However, supply chains have been unable to achieve this because there has not been an incentive to share accurate forecast information with partners – and even if there was, there was no way to securely share such information across the supply chain in a coordinated and timely manner. Consider the demand forecast example. A buyer is incentivized to either inflate a demand forecast to ensure supply or secure a volume discount. Anticipating that this is the case, a supplier will therefore underproduce. A supplier, on the other hand, will likely under-report the inventory on hand if it is trying to create scarcity or inflate it if it is trying to satisfy outsized demand. The buyer will therefore adjust its actual purchases accordingly. Lack of coordination within a supply chain frequently leads to shortages or excess inventory, and the cost of such inefficiency is high enough to drive the need for greater transparency and collaboration. The supply chain partners, then, have to thread the needle of sharing information without giving away their informational advantage or revealing sensitive information. Bank and OEM need to know this information for supply chain finance on the blockchain. Bank currently knows this information for traditional supply chain finance. OEM CM VMI T2 Supplier ship invoice ship invoice In addition, the lack of a mechanism by which data could be shared securely and authenticated to multiple networks of platforms at the same time means that faulty data abounds even when supply chains set out with the intention to openly share their information.

Companies need to hide even critical pieces of information in a transaction

In perhaps the keenest reminder of how valuable and important, and therefore sensitive, commercial information is in the supply chain, there are instances where value can be unlocked by hiding certain information from parties even when those parties need to use that information in a transaction (particularly in commodities). This is best illustrated with a use case. A commodities producer would like to get its inventory off its balance sheet as soon as possible and recognize revenue. It can sell this inventory to a trading company or third-party financier on the blockchain, who can then sell to the end buyer at the appropriate time. However, the sensitivity of commodities prices is such that, while all parties would benefit from this financing structure, it would be commercially unacceptable to the producers for the financier in the middle to know the actual price. This use case is slightly different from the one in which parties acknowledge that information treated as confidential in the status quo must preserve the same level of confidentiality after a blockchain network is put in place. In this example, the information was not confidential when only two parties were involved. However, by bringing in a blockchain-based solution, that data must now stay hidden to participants on the blockchain, even where such information might be integral to the activities of the blockchain.

The simplest way to prevent data from being shared on the blockchain is to never log it there to begin with. One common misconception is that if a supply chain ecosystem goes “on the blockchain”, then any and all supply chain data will be shared by all parties; practically speaking, not all data needs to be on the blockchain. The truth is that the selective placement of data on the blockchain, typically from an enterprise resource planning (ERP) system, is one of the most important and time-intensive steps of using a blockchain system. An enterprise can choose to store information off-chain in its own centralized databases, or even in a database provided by the blockchain system that is one layer removed from the blockchain itself. Only information that needs to be shared with others will go on to the blockchain.

In any event, the best technique for storing authenticated data on the blockchain is to simply store the hash of data on the blockchain, while the data itself stays in a database off-chain. This is a popular solution for documents, which are data-intensive files. In addition to increased data privacy, this structure helps with the throughput rate of the blockchain. The less data there is on the blockchain, the less time it takes to run a query on it so that the data can be processed. For industry consortia that have come together to form blockchain networks, on top of which industry-specific applications will be built, on-chain/off-chain management of data is the easiest way to provide greater transparency and availability of data to the whole ecosystem without compromising proprietary or confidential information. For example, maritime trade community members or industry players are sometimes competitors and sometimes partners, and if they are using one blockchain network, such as TradeLens or the Global Business Shipping Network, special care will need to be taken to protect the data and to give blockchain network members access only to relevant information as carefully determined within the context of the blockchain's objective.

Cybersecurity

See Inclusive Deployment of Blockchain for Supply Chains Part 5 – A Framework for Blockchain Cybersecurity, December 2019, World Economic Forum, by Adrien Ogee and Nadia Hewett in collaboration with Hitachi

See also the Cybersecurity paper from the California Blockchain Working Group

Bibliography

DHL, 2018. Blockchain in Logistics: Perspectives on the Upcoming Impact of Blockchain Technology and Use-Cases for the Logistics Industry. Available at: https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf (link as of 21/2/19).

Hyndman, N. and McConville, D., 2017. Trust and Accountability in UK Charities: Exploring the Virtuous Circle, British Accounting Review, Vol. 50, No. 2, pp. 227–237.

Wang, Y. et al., 2018. Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda, Supply Chain Management: An International Journal. Available at: https://doi.org/10.1108/SCM-03-2018-0148 (link as of 21/2/19).

World Economic Forum, 2018a. Trade Tech – A New Age for Trade and Supply Chain Finance. Available at: http://www3.weforum.org/docs/WEF_White_Paper_Trade_Tech_.pdf (link as of 21/2/19).

Deloitte, 2019, https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf (link as of 1/16/19).