guardtime

guardtime.com

Blockchain Designed for Supply Chains: Guardtime Supply Chain Framework

By David Shorthouse, Michael Xie

Whitepaper
April 2020

Abstract

For the past several years, blockchain technology has gained increasing attention from many different industries including supply chain. Blockchain technology can enhance the efficiency of supply chains by connecting previously disconnected islands of supply chain systems and participants, potentially end-to-end. It can also bring trust and controlled transparency to supply chains, and introduce cross participant process automations and governance in operations. The potential benefits of digital transformation through blockchain have attracted many related pilots and proposals to the supply chain industry. However, few are evidenced in production, which raises the question of whether the right type of blockchain is being applied to this sector.

This paper explores the opportunities and challenges for blockchain in supply chains, and highlights requirements for the introduction of blockchain technology in order to make a convincing value proposition. Finally, Guardtime's KSI® blockchain and Supply Chain Framework is introduced, with use cases. Arguments are presented which support the value proposition of this solution for enterprise supply chain in the areas of scale and performance, process automation, connectivity, provenance, authentication, and innovation through light touch integration.

Introduction

Supply chains are a vital part of today's global economy for both digital and physical worlds. An efficiently managed and collaborated supply chain can benefit all participants' operations from end-to-end, help enterprises to reduce costs, boost revenues, and create better brand loyalty. Today's supply chains are mostly managed by centralized ERP systems that focus on operations within an organization for the purpose of serving this single organization only. These systems worked for the past 20 years and helped supply chains to grow globally. It is apparent though that modern supply chains increasingly suffer from two forms of disconnect; one business related, and one technology based.

Trends and Challenges

The following trends are apparent in modern supply chains:

+ With growth, globalization, and the growing requirements for sustainable practices, modern supply chains have become complex demand-driven networks, with a trend towards an increased use of outsourcing of manufacturers and suppliers. Key business operations are performed across a complex network of entities often stretched across the globe.

+ Business privacy pressures over upstream sourcing networks or downstream distribution networks has made end-to-end visibility and transparency extremely difficult; a business driven disconnection.

In contrast, current supply chain systems remain largely unchanged, having a centralized operation and monolithic complexity. This creates challenges:

+ Isolations, operational disconnection, and an inability to communicate between the supply chain participants are common. In many cases, Electronic Data Interchange (EDI) can be used to plug this technical disconnect, which often brings a heavy price in terms of complexity, cost effectiveness, and performance. Failing that, we fall back on widespread use of manual processes across the supply chain, leading to obvious inefficiencies, and opportunities for mistakes and fraud.

+ Centralized ERP systems are difficult to change, often needing outsourced developers or consultants. It is difficult to innovate with these systems to take advantage of new smart technologies such as the use of IoT, industry 4.0, machine learning and artificial intelligence.

+ Business efficiency is reduced as potentially key interactions are not monitored directly, making collaborations and real-time responses by the business not possible.

The upshot is that the supply chain network becomes complex to manage, making it costlier to maintain, harder to monitor stock levels and ensure quality control, less efficient, and vulnerable to disruption, fraud, and diversion.

Blockchain and Supply Chain – Vision and Experience in Practice

The introduction of blockchain was seen as a game changer for the supply chain industry in many aspects. This is because blockchain can in theory bring multiple benefits to the supply chains industry in terms of efficiency, automation, connectivity, decision making and innovation, that directly address the challenges we highlighted. These benefits include:

+ A means to connect multiple participants and their systems over the supply chain network, incorporating transport, identities, and operation governance. Often times, this not only means connecting with isolated systems and operators, but also with devices (such as IoT and smart phones) and machines (such as robotic systems and industry 4.0);

+ Connectivity brings data transparency and visibility among supply chain members, systems, and events. Data collected across large, decentralized, and cross-border supply chain networks is then trusted, accountable, and actionable for better business decisions.

+ Trusted and verifiable supply chain automations[1] are possible across participants of the supply chain through the use of smart contracts. Automation is a prerequisite to achieve business agility, consistency, and efficiency through programming. However, cross boundary automation must be based on a universal trust mechanism, which is a key ingredient for inter-company supply chain collaborations [1].

+ Combining supply chain data transparency and trusted data will lead into a future generation of prescriptive and predictive supply chains [2]. The addition of other cutting-edge technology such as big data, machine learning, and artificial intelligence, and better business decisions will follow.

+ Provenance histories are a significant blockchain innovation for supply chains. They can not only immutably record supply chain events, but also the time and identity of the entity responsible for them. Combine provenance with digital twin[2] technology and third party verification[3], and you have a powerful new toolset. Applications include exportable and verifiable evidence for consumers, regulators and authorities such as customs dockets, certifications, or evidence of sustainable practices.

+ While intentional fraud can be difficult to eliminate, verifiable accountability over supply chain events combined with the latest physical authentication technologies will reduce the opportunities for bad actors and counterfeit operators.

+ Blockchain decentralized storage can help supply chains to mitigate cyber security risks that can lead to data modification, data losses, and data hijacking, which can easily cause supply chain disruptions.

+ The introduction of digital tokenization[4] can enhance integration, asset management and coordination among the members of a supply chain [3].

These benefits are easy to appreciate and have led to a number of announcements of blockchain based pilots and initiatives across the supply chain industry in the past few years. The pilots have largely focused on solving supply chain pain points such as sourcing provenance,

1 Automation refers to the ability to convert supply chain business practices into algorithms and deploy with the blockchain framework

2 Supply chain digital twin - the virtual representation of a supply chain asset that reflects the lifecycle of this asset in a digital format

3 Validation refers to programmable logic to assure data stored and shared over blockchain is immutable and trusted

4 Tokenization refers to the ability to create digital claim with blockchain and assign it to a value asset (physical or digital), and then manage the lifecycle of this value asset with corresponding digital claim

counterfeits, track and trace, compliance, and data transparency. There has however been little evidence of these pilots making it into widespread production.

To be useful to supply chains, blockchain has to be able to scale and perform with realistically large networks of entities or nodes. It must respect business privacy, and the way business is transacted. Also, to avoid massive disruption and cost, it must allow a light touch integration with existing systems.

Blockchain - Choose the Right Tool for the Job

There is general agreement that blockchain technology has great potential to make supply chains more connected, agile, efficient, transparent, automated and cost effective. However, not all blockchains are the same. Public blockchains such as Bitcoin and Ethereum are truly transformative technologies, enabling people for instance to perform cryptocurrency transactions anonymously from their own desktops. However, they are unlikely to be the right blockchain tool to apply to supply chain operations for enterprises that require real-time decision making, due to uncertain block settlement times and unpredictable network congestion. Therefore, we must take care to ensure the right blockchain toolset is chosen for a specific job by considering how they perform against a set of criteria.

Performance and scalability

One of the contributions that Satoshi Nakamoto gave to Bitcoin is the longest chain protocol [6]. This protocol is widely adopted by many other cryptocurrency focused blockchains including Ethereum, EOS, and Cardano. In this protocol, a new block proof is generated by a single computer over a network, followed by the application of a network consensus model in order to build the blockchain. However:

+ For enforcing network trust, the protocol requires high energy consumption.

+ Transaction throughput can be a limiting performance factor due to indeterministic transaction ordering, forking of competing chains during new block creation, and consensus speed due to network delays among the vast number of validators/miners.

As an alternative to using the longest-chain protocol, enterprise-focused DLT (Decentralized Ledger Technology), such as Hyperledger and Enterprise Ethereum have become available. They typically require a trusted consortia to be set upsetup prior to blockchain operation in order to oversee block creation operations. Ongoing management of these consortiums are necessary to deploy, operate and integrate these types of blockchains.

However, considerations include

+ The usage of a consortium in this type of protocol raises the issue of business privacy and efficiency.

+ As a result of these complex setups, most of the leading DLT technologies have high bandwidth usage between nodes owing to the protocol design and architecture. This makes it difficult to scale for large supply chain networks.

Data privacy

In order to commit transaction data into the blockchain, the majority of public blockchains and Enterprise DLT's by design require transaction data to be captured by the blockchain in its entirety to guarantee data integrity and immutability. This is a risk from both data privacy and operational aspects because:

+ Supply chain data and processes will be shared with both trade partners and also non-relevant parties on the blockchain. Due to the design of these blockchains' transaction models, there are only limited ways to protect data privacy when using these blockchains.

+ Data can be encrypted prior to committing it to the blockchain, which introduces the complexity of key management and distribution across the supply chain network.

+ Investment in more complex cryptographic computations such as zero knowledge proofs of the committed data. However this has an additional impact on operational cost, scalability and performance.

Automation with smart contracts

While business automation using smart contracts is an attractive idea, it does carry performance overheads. For example, blockchains with account based [4] or channel bound [5] smart contracts such as Ethereum, Enterprise Ethereum, and Hyperledger can run into throughput issues while running smart contracts as they are constrained by the blockchain account/channel binding design, and therefore, cannot easily scale using conventional and proven approaches such as load balancing, and clustering.

Integration and operational cost

Due to the steep learning curve, complex setup and service management models, many blockchains are becoming known for their disruptive and costly nature for current IT investments, this is because

+ Complexities in deployment, identity management, and supporting IT administration result in high capital investment cost (CAPEX) with limited and uncertain return of investment.

+ Many blockchains require competing gas fees when transactions are committed to the blockchain network. This can significantly increase the operational cost (OPEX) associated with running such a solution over a supply chain network.

+ Where the blockchain design enforces a limited choice of cloud solution to host the blockchain infrastructure and replicated ledger storage, the hosting costs can become significant.

On the other hand, existing supply chain solutions and ERP investments are mostly created with conventional technology stack and paradigms. Blockchains that cannot offer conventional interfaces, APIs, and service management for interoperability and light touch adoption, will introduce risk and cost when adopted by the supply chain. After all, ERPs are working and represent significant investment, so interoperability with a chosen blockchain solution is essential.

Maturity

It has been noted that most of today's leading DLT blockchain technologies capable of working with supply chains are still in their infant stages in terms of software stability, interfaces, security, operation, management of patches, upgrades, service and ease of deployment.

Guardtime's KSI® Blockchain - A Mature Solution for Supply Chain

In this section, we introduce Guardtime's KSI® Blockchain, which was designed to provide a massively scalable and responsive data integrity service for the requirements of government and commercial enterprise. We will argue that KSI® Blockchain combined with Guardtime's Supply Chain Framework is capable of fulfilling the value propositions for blockchain identified for the supply chain industry.

Guardtime's KSI® Blockchain is one of the most mature blockchain technologies in production in terms of design and longevity. It was first adopted by the Estonia government in 2009 for its eGovernment initiative, going live in 2012[5]. Since then, KSI® Blockchain has been running 24/7, protecting the digital records inside Estonia's e-services systems, which hosts 99% of state services online.

KSI® Blockchain though is fundamentally different from cryptocurrency focused and longest-chain protocol based blockchains. It is particularly suited to global supply chain applications where the ability to perform with scale across multiple entities essential [7]. Inherent properties include:

+ Rapid Integration - The key infrastructure is privately maintained and globally available, so rapid integration is possible with existing company infrastructure and databases (such as ERP systems) using simple APIs. This ensures existing supply chain operation and systems will be impacted as minimum as possible.

+ Attack tolerance and reliability - Being a mature technology, it has been battle tested in production since 2012, this reduces capital investment risks.

+ Proof of Data and Process - a mathematical proof of data and process is provided through a KSI signature, which may be verified independently across the supply chain.

+ Privacy - The blockchain layer does not store private data or host smart contract functionality.

+ High Availability and Scalability - Designed for extremely high data registration rates globally (capable of up to 1 billion registration/second on the entire blockchain network scale).

+ Deterministic - It is deterministic both in transaction commitment (one block per second), and storage (a few GB growth per year). A guaranteed response time of one second is adequate for most enterprise use cases.

+ Data Accountability - KSI signatures contains the signing identity.

+ Predictable cost - there is no peer competition for processing of transactions onto the blockchain, so there is no incentive fee associated with transaction inputs. This reduces energy usage and allows for predictable OPEX.

+ Controlled network traffic - Proof of data integrity for an entity is implemented with a series of one-to-one network connections between participant gateways and the KSI® Blockchain infrastructure. Thus data privacy is conserved by default and network traffic controlled and minimized.

+ Modular Design

    - Gateways operate at the edge of the Internet to ensure easy to scale and highly available blockchain transaction operations. Gateways are also responsible of generating and delivering Proof of Record, a.k.a KSI Signature, for every transaction received from blockchain clients.

    - A globally deployed Aggregation Network which is a decentralized network of computers working together to compute new blocks as opposed to other blockchains where single computers are block creators. The Aggregation Network

5 See KSI-blockchain at e-estonia.com/solutions

ensures that KSI® Blockchain network can perform well at the highest level.

- Core nodes (Voters) that use Guardtime's proprietary Proof of Authority algorithm to achieve agreement. Once a hash is voted, a new block is broadcasted to the edge network Gateways through the aggregation network to ensure blockchain availability at the edge of Internet.

Additional features such as ledger or database storage, trusted messaging, provenance histories, and process automation are added without affecting blockchain performance, using additional layers of technology as required. Note that the Supply Chain Framework (SCF) described later is one such additional layer.

Guardtime Resonance Layer

The Guardtime Resonance is an application friendly layer that combines application data, its schema, and its KSI signature data into trusted data constructs, called Dockets. This allows cross boundary parties to efficiently share and verify application data in multiple ways, online or offline, and on a need-to know basis for privacy. New Dockets can be cryptographically linked to existing Dockets in various ways to form extended data histories, called provenance, which can be independently verified by other parties in the supply chain.

With the KSI® Blockchain and KSI Resonance layers in its technology stack, Guardtime developed its Supply Chain Framework (SCF) to best leverage its blockchain capabilities, address the business and technical disconnections that exist in supply chains today, and provide a path to innovation.

Guardtime Supply Chain Framework (SCF): Bringing Innovation to Supply Chain

The key design goals of Guardtime SCF were to enable the closure of the business and technology driven disconnections prevalent in modern supply chains with minimal disruption (light-touch) to existing systems, and to provide a pathway to innovation.

Design features include:

+ Provision of core supply chain functionality for transparency, provenance histories, connectivity, collaboration, automation, trust, channel integrity, cross-boundary identity, data exchange, authentication and autonomous audit trails.

+ Cryptographic digital twin functionality that allows immutable provenance trails to be captured across a supply chain, which may be exported and verified independently.

+ Ensure performance with agility through a separation of the data and business process integrity layers.

+ Configurable and programmable components and APIs, with support for data privacy.

+ Support for tailored Decentralized Applications (dApps) and permission-based ledgers (localized and application focused) instead of heavy , complex smart contracts.

+ An agnostic stance to the supply chain ecosystem model. The framework, or an Extended Supply Chain Application built with this framework, can be a part of centralized or decentralized supply chain.

+ Modularized design with implementations and operations supported for either a network of participants or a single participant.

Primary Integration Approaches

The framework provides two approaches to allow supply chain integration, interfacing, and development using KSI® Blockchain as the trust anchor. Supply chain implementers can choose whichever method makes the best sense to them based on existing investments and available IT infrastructure. The solution can be deployed in a combination of two main approaches:

+ Using Generic Supply Chain Framework APIs
+ Using Tailored Extensions

Using Generic APIs

Here, the framework provides a straightforward set of off-the-shelf HTTP RESTful APIs for generic purpose supply chain operations. The framework is deployed as a node in the participants' network or cloud and interacts with clients directly. By using these generic APIs, existing supply chain solutions for a participant can record and exchange supply chain data and documents with other nodes on the network. Impact to existing automation in current solutions are minimized. Existing supply chain systems can either directly engage these APIs or use an integration agent for connected and trusted supply chain operations.

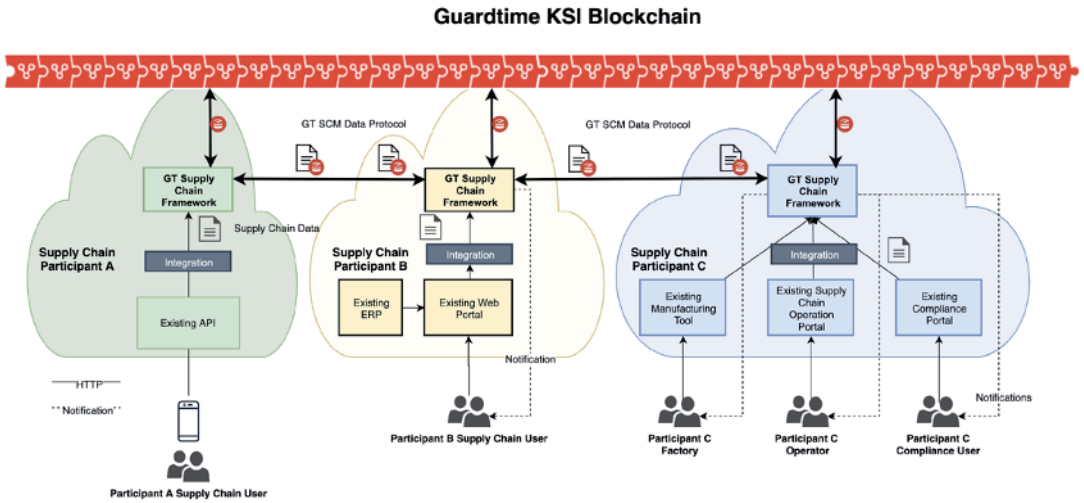

Figure 1: Approach 1 - Using Generic Supply Chain API Nodes in Supply Chain Network

The above example diagram demonstrates a three-participants supply chain network using the Framework as supply chain APIs. The API server nodes interact with each other for supply chain operations. Within each participant's network, an Integration layer is added to help existing supply chain systems (API servers, mobile solutions, portals) to interact with these APIs. The Processing Trade use case discussed below is one of the examples of using these off-the-shelf Supply Chain Framework APIs.

Using Tailored Extensions

Here, the framework provides a set of customized, expandable application APIs and interfaces that allow for tailored supply chain application extensions. By using this approach, supply chain developers can build Extended Supply Chain Applications to define tailored business rules over exchanged data and blockchain backed automations.

The below example diagram demonstrates a three-participants supply chain network using Extended Supply Chain Application built with the Framework. The extension Logic and APIs are built for this supply chain. Each extension is deployed as a supply chain node, and interacts through client interfaces such as mobile phones and web portals. In addition to the default Framework functionalities, the extensions provide additional functional behaviors for the connected supply chain systems. The Wine Supply Chain use case discussed in the later section is an example of using Supply Chain Framework with Extensions.

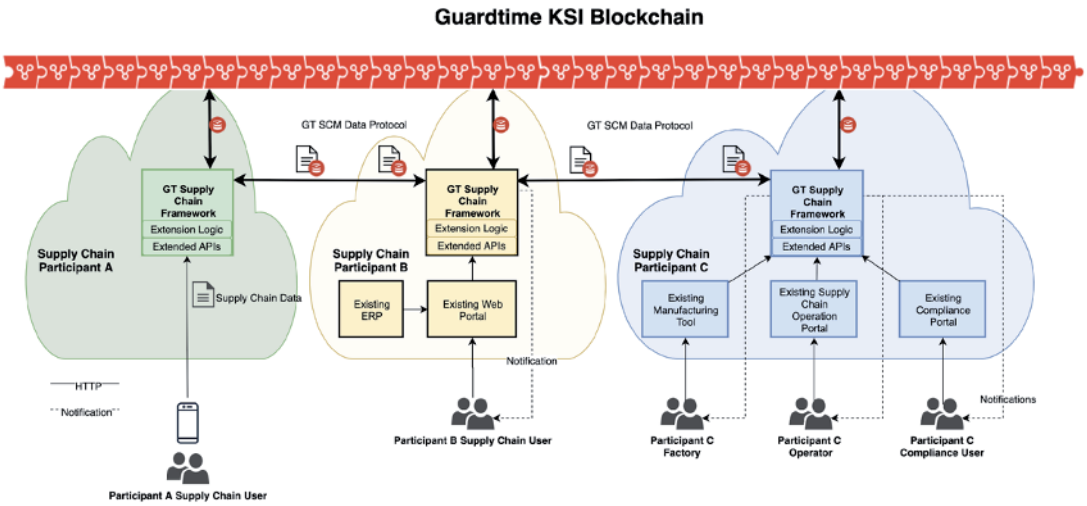

Figure 2: Approach 2 - Tailored Supply Chain App

Case Studies

Since the introduction of the Framework, it has been used to solve multiple supply chain problems and improve supply chain networks for different industries and for different purposes, including defense contractor software supply chain, government regulation compliance, and consumer goods track and trace. Below are two example uses cases, one uses the Framework as an off-the- shelf API platform to meet with compliance requirements, and the other uses Extended Applications built with the Framework to implement detailed business logic and processes.

Case 1 - Processing Trade Compliance Supply Chain

Guardtime worked with one of the largest global Consumer Goods companies[6] [XYZ] in the world to address its Processing Trade issues in China. Processing trade refers to the business activity of importing all or part of the raw and auxiliary materials, parts and components, accessories, and packaging materials from abroad in bond, and re-exporting the finished products after processing or assembly by enterprises within the mainland China [8].

Due to the potentials in duty tax fraud, Chinese Custom requires suppliers, manufacturers, and logistics providers involved in Processing Trade to provide detailed and connected documentation trails in a timely fashion. Failure to provide necessary and accurate documents in time can result in fines and sometimes suspensions in the Processing Trade license. In 2017, the total trade value from Processing Trade in China was approximately 65% [9] of its total of $2.3 trillion global export.
This supply chain use case involved a large number of trade partners ranging from suppliers, manufacturers, and logistics providers. Each had their own ERP related tools to manage supply chain activities and documents. Chinese customs requires related supply chain documents across trade partners to be connected with their applications and submitted using their defined forms.

Historically the process was largely manual and error prone due to the technical disconnections between the trade partners and the custom's systems, and the complexity of the documentation requirements. XYZ has in the past been fined multiple times for failing to meet compliance requirements due to a variety of reasons, with no certainties often where the problems had occurred as there were no reliable records for the business processes.

On review, Guardtime found the issues are less with automation and process governing in existing ERPs, but more with coordination, audit and error minimisation arising from the outputs of all the disconnected ERP systems.

The Supply Chain Framework was deployed as a solution:

+ The system was used to collect related ERP documents from trade partners in time, automate Custom forms generations based on related ERP documents, establish provenance trails based on connected ERP data, participants blockchain identities, and then ensure timely submission to the Custom from each trade partner.

+ Localized integration points and portals were also developed to ensure the APIs can properly integrate with XYZ and trade partners' ERPs and Custom EDI portals.

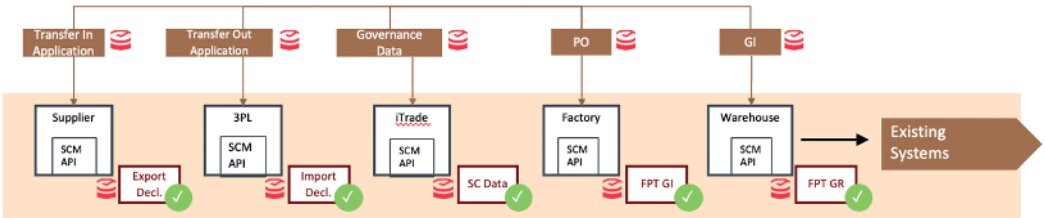

Figure 3: Processing Trade Supply Chain Logical Parties

6 Name withheld

+ Using localized ledgers built with the Supply Chain Framework, the solution helped XYZ and its trade partners to become more compliant with the regulations, more efficient in the filing process, reduced the chance of errors, and above all reduced disruptions.

Guardtime's technology achieved these all while meeting the performance and availability requirements from a large supply chain network with a great volume of supply chain data. In addition, with the introduction of this compliance ledger layer, XYZ also became more agile in terms of onboarding new suppliers for their Processing Trade operations.

Case 2 - Wine Supply Chain

In recent times Australia wine has reported worrying instances of counterfeit bottles in its export markets, and of unauthentic and untraceable grape sources used for local production. In 2017 Australian wine commentator Jeremy Oliver estimated that up to 50 per cent of wine that retails for more than $35 a bottle in China is fake – either through a fake label, a refilled bottle or a copycat brand [10]. Australian wine supply chain displays the same business and technology disconnections we have previously highlighted across its network of grape growers, wineries, bottlers, resellers, distributors (local and international), consumers and regulators, which leads to opportunities for bad actors.

To see what blockchain could do to protect the reputation of Wine Australia, and to support the objectives of its Label Integrity Program (LIP) for the quality and authenticity of its wine, Guardtime worked with Australian wineries and growers and created a supply chain product "Guardtime Vino" in the form of Extended Applications from the Supply Chain Framework. The Vino platform was designed based on the best practices and compliance rules for the industry.

+ It uses a set of tailored APIs, data definitions, business logic, exchange rules, operational portals and mobile applications to automate wine supply chain operation processes for the different stages of the supply chain. This includes data capture for growers (sales, registration and distribution), winery and bottler (production, sales, distribution), logistics, distributor, and end consumer (authentication, provenance receipt).

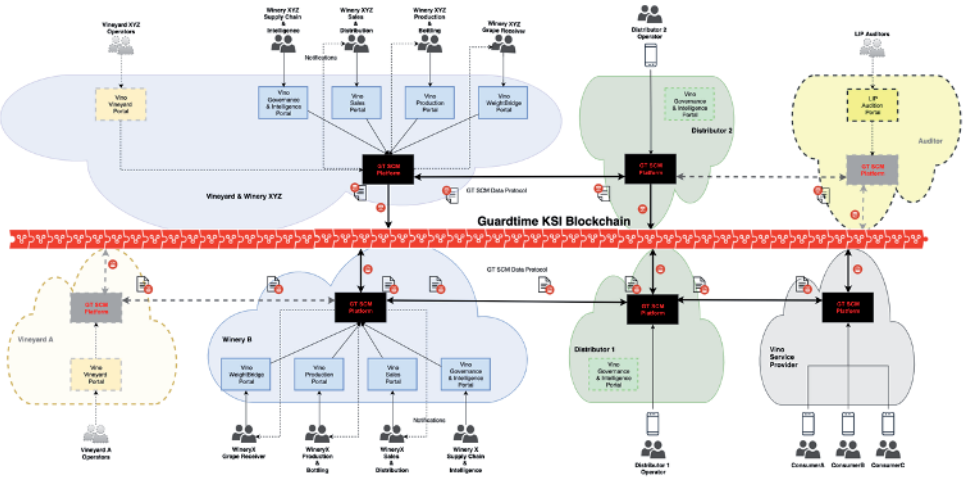

Figure 4: Vino Supply Chain Operational View

+ Using decentralized ledgers and process automations built in Guardtime Vino, Vino allows operators to efficiently manage digital twins per bottle of wine, building provenance records with data capture into Dockets at any node of its supply chain network, in real-time.

+ The wine making processes captured by Vino is able to record how each authenticated grape source is depleted and converted into final wine products (either in barrels or bottles) over time - a form of mass-balance monitoring.

+ Blockchain protected authentication mechanisms may be added in the production process for every bottle of wine. These authentication mechanisms allow consumers to use mobile phone-based applications to authenticate the wines.

+ The platform supports cutting edge bottle authentication and anti-tamper methods e.g. NFC, ink-based tagging, and quantum materials.

+ Consumers can authenticate a bottle of wine with a mobile phone app, and thereafter receive and explore its provenance history while allowing full data accountability. In addition to authentication, these apps may be developed to allow businesses to form a deeper relationship with consumers (closing the existing disconnect).

+ The mobile scans results are useful to the wineries. They may be analyzed for counterfeit product distributions and impact analysis on their consumers. These insights and direct engagement with consumers can help businesses to gain better knowledge and make better decisions with their supply chains.

+ The provenance records may be made available to regulators who can independently verify the records. This provides evidence of responsible sourcing from grape suppliers and winery production in line with the LIP.

Through the Vino product built with the Supply Chain Framework, Guardtime was able to demonstrate a solution that addressed the challenges raised by the Australian wineries and showed the power of trusted data collected by the brand owner. Vino shows that brand protection, integration, automation, authentication, innovation and agility can be provided by the right blockchain solution that can respond in near real-time. Above all, the functionality of the platform is easily extended providing a pathway to further innovation.

Conclusion

For good reasons blockchain technology brings a lot of interest and hype to the supply chain industry. Blockchain can fundamentally address the business and technology disconnects that exist in modern supply chains, and bring business benefits such as product visibility, channel integrity, data transparency, regulatory compliance, supply chain accountabilities, product authentication, fraud detections, and innovation.

However, like any technology created to solve business problems, existing blockchain technologies, while sharing common fundamentals, are designed with different focuses and implemented differently to address different challenges and requirements. Therefore, not every blockchain is suitable for solving supply chain's challenges.

In contrast to most existing blockchains and blockchain enabled distributed ledger technologies today, Guardtime's KSI® Blockchain is designed with scalability, availability, performance, privacy, ease of integration in mind. KSI® Blockchain was built with the explicit purpose of ensuring data trust at scale, and verification for anyone, anywhere and anytime.

The Guardtime Supply Chain Framework leverages KSI® Blockchain and Guardtime Resonance technology. It is designed to enable blockchain for modern complex supply chains, allowing integration with existing ERP systems with minimal disruption. Depending on the actual business problems and complexity of existing supply chain solutions and infrastructures, the framework can be used as an off-the-shelf supply chain system with ledger, provenance, and communication delivered through APIs for easy integration, as for the Processing Trade use case. Alternatively, it can also be extended with detailed business logic, data definitions, governance rules, and supply chain automations using Extended Applications on cloud or mobile phone, as for the Vino use case.

In conclusion, we argue that Guardtime's Supply Chain Framework will facilitate digital transformation of supply chains with minimal disruption to existing systems while bringing full data accountability, and proof of data. It is designed to allow rapid introduction of new functionality and innovative technologies to existing businesses, such as IoT, industry 4.0, big data, machine learning and AI, which is difficult to achieve with traditional ERP systems.

References

[1] I.W. G. Kwon and T. Suh, "Factors affecting the level of trust and commitment in supply chain relationships," Journal of Supply Chain Management, vol. 40, no. 1

[2] C. Wentworth, "The Supply Chain Gets Smarter - Autonomous supply chains at the nexus of IoT, AI, and Blockchain," MWD advisors, 2018

[3] V. Babich and G. Hilary, "Distributed ledgers and operations: What operations management researchers should know about blockchain technology," SSRN Electronic Journal, 2018

[4] Ethereum white paper, Ethereum account, https://github.com/ethereum/wiki/wiki/white-paper#ethereum-accounts

[5] HyperLedger Fabric ChainCode, https://hyperledger-fabric.readthedocs.io/en/latest/chaincode4noah.html

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008

[7] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees," 2007

[8] Processing trade, http://china-trade-research.hktdc.com/business-news/article/Guide-to-Doing-Business-in-China/Processing-Trade/bgcn/en/1/1X000000/1X002LEV.htm

[9] L. Yan, W Tian, M. Yu "China's Processing Trade and Value Chains," 2018

[10] Weekly Times, May 2017 https://www.weeklytimesnow.com.au/agribusiness/decisionag/food-fraud-high-roller-of-the-crime-scene/news-story/a9837a9f2232ec5c520e2997f03bb617