

Use Case

Supply Chain Management

Problem

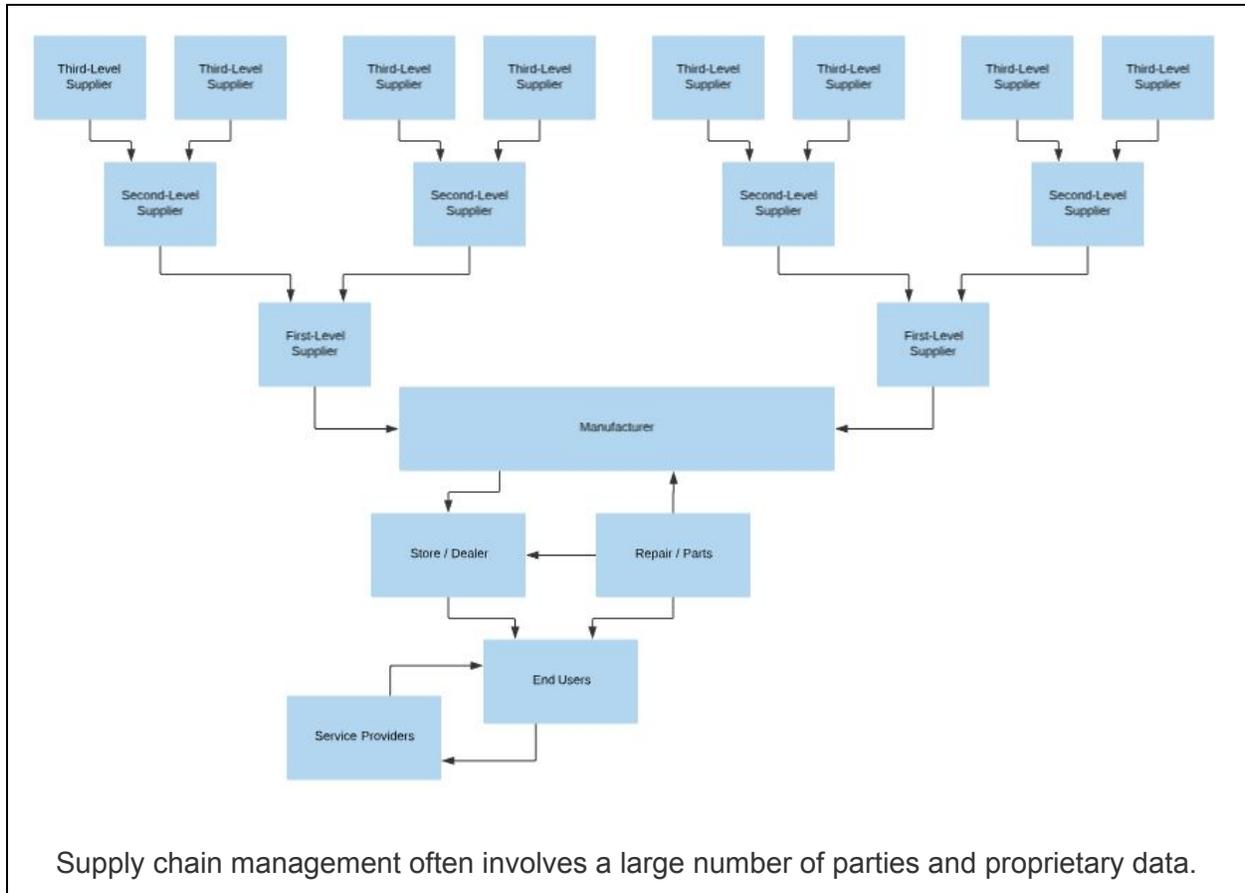
Supply chain management presents a difficult problem, which traditionally has been handled using highly-manual, highly-segmented systems that track items across businesses and suppliers. Solutions are difficult to implement successfully due to ever changing real world requirements, regulations and scalability challenges. The shared nature of blockchain data structures has the potential to upend how components are tracked and managed across businesses, breaking down legacy barriers between inventory management, procurement and supply chain management systems.

Background

Current enterprise supply chains are managed across various types of systems that often generate siloed data that must be reconciled through highly-manual processes. A shared digital ledger offers an elegant solution where all participants operate from a shared record, obviating the reconciliation issues that plague current supply chain solutions.

A shared distributed ledger allows every stakeholder in the process to monitor the progress of individual components as they flow through the chain, creating permanent and immutable records. Use of a permissioned digital ledger (as opposed to Bitcoin's permissionless ledger) allow for a variety of access permissions to be granted for various datasets residing on chain. This is an especially attractive feature for supply chains that span across multiple parties: information pertaining to supply levels or component delays could be considered proprietary information that might not be appropriate to disclose to the other parties.

Another important benefit is the potential to reduce the introduction of counterfeit components and theft. Manufacturers want to ensure their products get to intended destinations, while at the same time, buyers want to make sure the products they receive are from legitimate sources. If the record of transfer between parties is provably correct, it eliminates the potential for unknown sources to be introduced into the process and provides global oversight to all parties to reduce fraud and theft.



Internet of Things (IoT) device tracking offers another exciting possibility when combined with blockchain-based supply chain management. IoT-connected transport containers can be used to report real-time location information on a blockchain throughout transit. Container status and position are then able to be queried by any stakeholder involved in the supply chain. Furthermore, this on-ledger data can be integrated with smart contracts in such a way that a large portion of the finance and insurance facilitating the physical movement of goods can be streamlined. This has the potential to remove unnecessary intermediaries and greatly increase efficiency. Smart contracts used in this fashion have the potential to automate trade finance, shipping insurance, escrow services and payments for all members in the supply chain while at the same time reducing costs.

Solution

Manifold's serverless blockchain platform provides a foundation to build highly-scalable supply chain management applications. Manifold delivers a secure, extensible, and future-proof platform for blockchain-based innovations by combining powerful AWS services, our proprietary ledger technology, and automated synchronization to multiple public blockchains. Utilization of our infrastructure results in dramatically lower operational costs and complexity.

Description

Manifold's blockchain platform is exposed as a set of REST interfaces that can be securely accessed from any internet connected source to submit data for codification into the blockchain. Data verification and processing is encapsulated into separate, discrete Lambdas for stateless execution. Data is then written to AWS' fully managed autoscaling database DynamoDB for persistence.



*Lambdas run code only when triggered,
using only the compute resources needed*

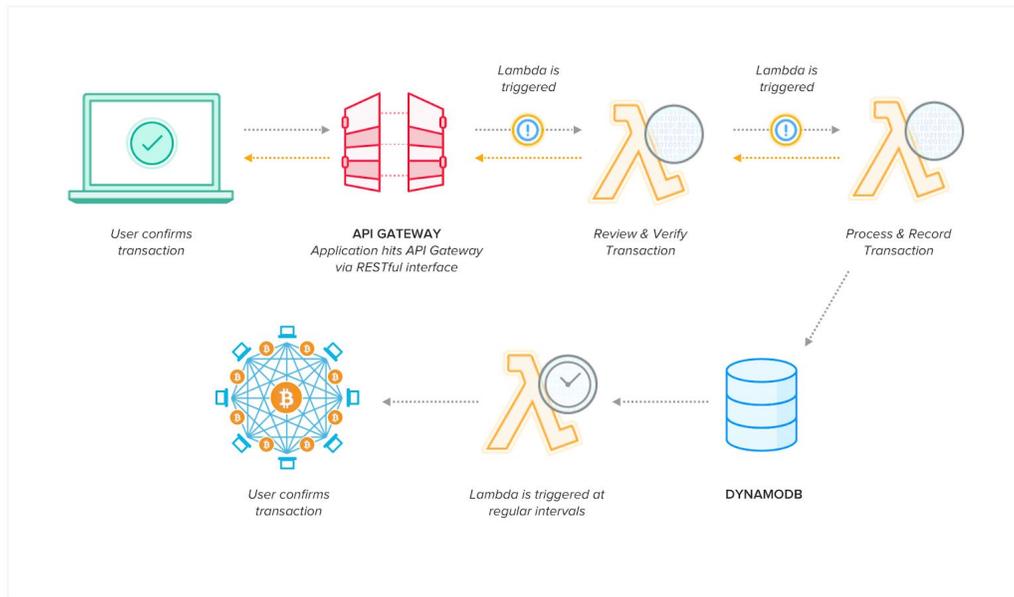
Compute resources are minimized

The stateless nature of AWS Lambdas means that PII, KYC, or other sensitive information can be shared with the Lambdas to allow for a determination about the veracity of a transaction without the possibility of that information being retained in the cloud. This reduces the perceived risks associated with cloud migrations while simultaneously maintaining compliance for companies working with sensitive datasets.

As AWS Lambdas are stateless, they can not be used to execute malicious code or other than intended commands. These Lambdas function as trusted gatekeepers to the secure blockchain data and are the only entities given append-only write access to the datastore, ensuring confidence in the integrity of the intermediate chains between verification periods. Furthermore, the use of a Lambda system architecture allows easy chaining of additional functionality, as needed.

Technical Architecture

Transactions are generated on an external system (IoT device, mobile app, back-office server) and submitted to a RESTful endpoint hosted by an AWS API gateway. When a transaction is received, it triggers a series of Lambda executions that first review and validate the transaction before processing and recording it to the blockchain.



All data is then protected by the selected public blockchain(s) by periodically recording the most recent interval's hash to them. This approach ensures data immutability and enables easy independent verification of that data.

Bottom Line

As blockchain projects transition from lab and proof-of-concept environments into the harsh and unforgiving real world, they will need a future-proof platform capable of delivering the scalability and throughput needed to achieve their vision. Streamlining supply chain management with a shared, secure ledger is an ideal application for the Manifold platform.