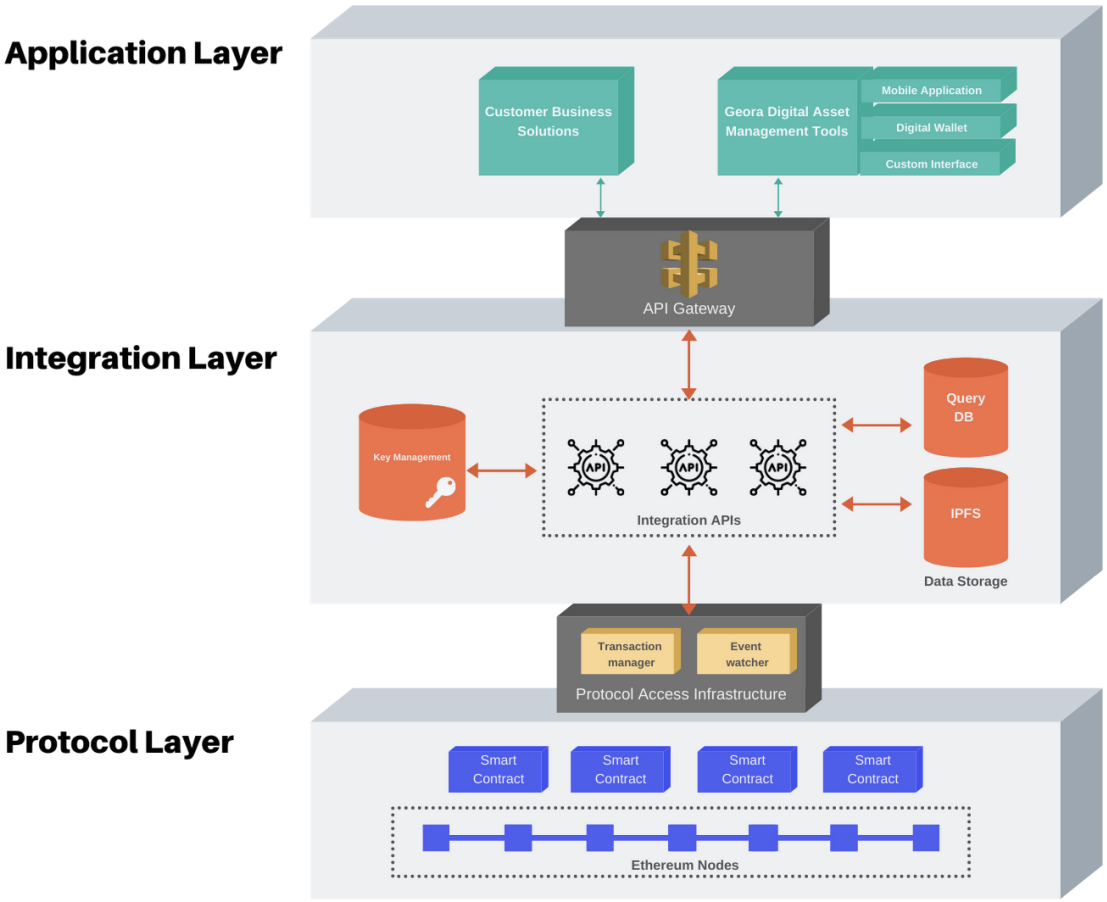
GEORA

Technical Overview

The Geora protocol is a blockchain-based system for managing and monitoring commodity supply chains. Geora provides digital infrastructure and open-source tools that allow users along agricultural supply chains to build trade and finance solutions. This document contains an overview of the technical design and implementation of the project, including its components and the technologies used.



GEORA

Core Technology

Geora is a hybrid blockchain system composed of three layers:

- *Protocol layer*: contains core logic and immutable, verifiable data, using the Ethereum blockchain
- *Integration layer*: simplifies access to the protocol by providing key management, data storage, and integration APIs
- *Application layer*: contains tools for building rich workflows on the protocol, including financial contracts and agreements, and provides applications for customer use-cases

Common strategies for privacy and permissioning are used across all three layers to ensure customer data is secure.

Protocol layer

The protocol layer is the source-of-truth for data in Geora. A private, distributed network of Ethereum nodes contains asset and workflow data. Core logic is encoded into smart contracts on the network, which govern asset ownership, certification, and processing. All participants of the network are able to verify that the logic is correctly executed.

Data stored in the protocol layer is immutable and versioned: each update to the system adds another identifiable layer to its history. This history cannot be rewritten, providing an auditable record of changes to any data in the protocol, as well as an execution record for all workflows. The histories of these workflows can be accessed and analysed by tools in the higher layers.

The protocol layer supports financial contracts, agreements, and workflows, which are encoded as Ethereum smart contracts. These workflows can operate on assets, certificates, users, and digital currency to perform domain-specific actions.

The protocol layer is developed using ubiquitous Ethereum token standards like ERC-20 (fungible tokens) and ERC-72 (non-fungible tokens), allowing for interoperability with other protocols. Geora has developed infrastructure to scale and manage the private network, including a transaction *nonce* manager and event watcher, that simplify permissioned access by functions at higher layers.

Integration layer

The integration layer has three main functions:

- *Providing integration APIs*: Geora exposes access to the protocol layer through a simplified REST API, which assumes no blockchain knowledge.
- *Key management*: to keep customer information secure, Geora manages their cryptographic keys. These keys are tied to customer identity and used to sign and verify actions in the protocol layer.
- *Data storage:* the integration layer provides a fast, queryable database that reflects data stored in the protocol layer and exposes it to applications. It also stores encrypted certificates in IPFS, a distributed data storage solution, which are hashed and attached to assets in the Ethereum smart contracts.

The layer is made up of a number of components deployed across Amazon Web Services and DigitalOcean, and relies upon managed providers of databases (Amazon Relational Database Service), secret management (AWS Secrets Manager), and file storage (AWS S3). Components are developed in both TypeScript and Go languages.

By abstracting the protocol layer behind integration APIs, Geora is able to upgrade the protocol as required without forcing changes on consumers. This allows changing the underlying blockchain technology in accordance with new technological developments and prevents lock-in to Ethereum.

Application layer

This layer contains applications developed by both Geora and its customers. Applications can provide a broad range of functionality, from utilities like asset grading or classing through to full end-to-end systems modelling a particular supply chain. Applications communicate with Geora via the integration layer, shielding users and developers from protocol details.

As part of the application layer, Geora provides a digital toolkit that can be used to build workflows and contracts to address customer use-cases across many supply chains. These workflows can be shared, adapted, and re-used to aid development and integration.

Applications in this layer are built using technologies appropriate for the use-cases and platform. This includes web applications in .NET and React, system integrations in TypeScript, and mobile applications in React Native.

GEORA

Protocol Performance

Blockchain protocol

Geora uses the Ethereum blockchain to power the protocol layer. A private, permissioned network contains nodes which execute and verify all transactions. These nodes are operated by both Geora and its customers, creating a consortium chain.

The network is secured using the IBFT2 consensus protocol, which provides finality and fault tolerance and prevents bad actors from adding incorrect data or breaking the rules of the system. With a current block time of two seconds and high gas limits, the network is capable of processing hundreds of transactions per second in parallel.

The network is highly-available and composed of multiple validator nodes, supporting nodes entering and leaving the network, as well as node failures, without compromising uptime.

Privacy

Customer privacy and flexibility of data permissioning are built in to Geora at all layers. Geora supports *data privacy*, making asset and workflow data available to only those with permission, as well as *transactional privacy*, which obscures a customer's counterparties and the actions they take within financial contracts.

To achieve these goals, Geora uses a four-pronged privacy solution:

1. *Merkle trees* secure asset data at the protocol layer by compressing all data into a single hash. The protocol can share this hash across all nodes without revealing any of the constituent data. Through Merkle proofs, workflows and contracts can check specific values in the data without revealing the entire asset.
2. When customers upload certificates, the protocol encrypts the data using a unique data key per certificate and stores it on IPFS. Users can share and revoke access to these files using their own private keys via asymmetric encryption.
3. Each user in the system can hide their identity using pseudo-anonymous on-demand identities. For each action they take, the user can generate a new identity using a hierarchical deterministic wallet, that cannot be traced back to their public identity.
4. Within workflows and contracts, state channels hide the details of actions from non-participants. The channels perform individual steps of a workflow away from public view and reveal only the final outcome.

GEORA

Sample Workflow

This example describes how Geora would encode a workflow involving the financed sale of wheat. In this scenario, a bank is financing a buyer, who is purchasing grain from a grower. The bank will pay the upfront cost of the wheat purchase; the buyer can repurchase the wheat from the bank at any time by paying the value plus interest.

The grower accesses Geora through a custom mobile application in the application layer. Throughout the farming process they add data and certificates to their wheat asset, such as an organic certificate, in order to improve its value. This data is stored privately in the protocol and integration layers.

When the grower is ready to sell the wheat, they introduce the asset to the buyer, who sees it in their own web portal within the application layer. When the buyer agrees to purchase, they partner with the bank and use Geora's digital toolkit to create a new contract in the protocol layer, which governs their finance agreement. After the parties agree to the contract, it is executed: the grower is paid immediately, and the bank takes possession of the wheat asset. This transaction is executed as an atomic swap: the same transaction contains both the transfer of grain title and the payment to the buyer, so when the smart contract is executed either both transactions will succeed or both will fail. This provides the means to remove counterparty risk by matching delivery to payment.

The bank interacts with Geora directly, by integrating its systems with the integration and application layers. It is able to pay the grower, take possession of the asset, and make it available for repurchase by the buyer through its existing systems and processes. When the buyer decides to repurchase, the contract calculates interest in the application layer, and the payment is settled via the protocol layer.