h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
ccass
COMPETENCE CENTER FOR
APPLIED SENSOR SYSTEMS

Team Project SS21

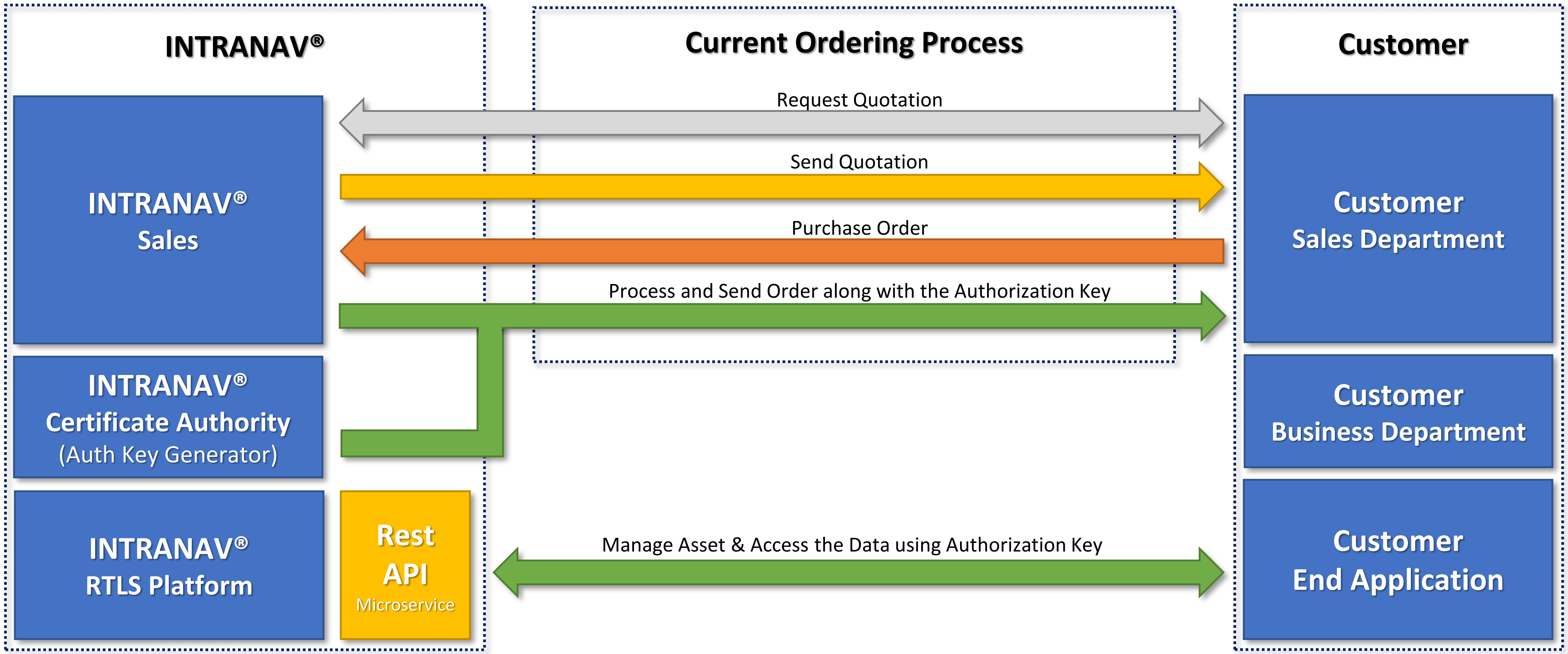
Blockchain Based Order and Access Management

Sachith Liyanagama, 769617
Ken Freise, 746041
Shakil Ahammed, 769709

Content

Current Method of Order Management

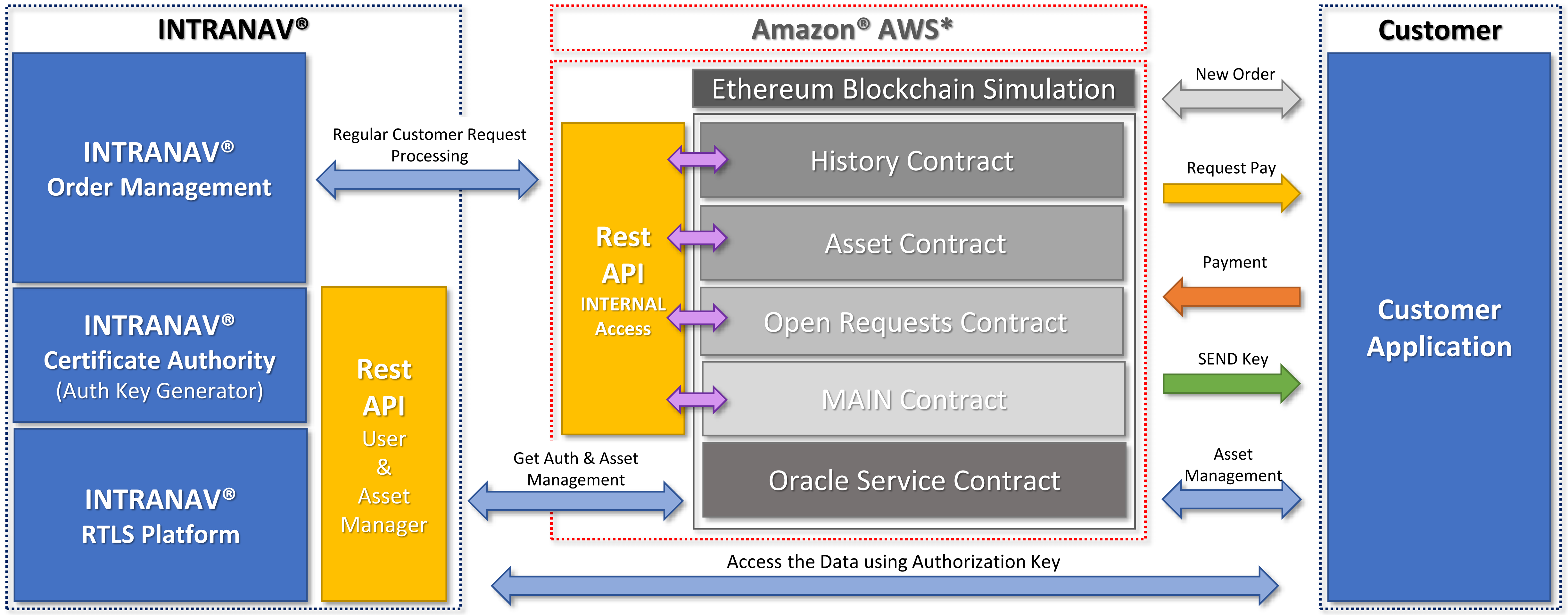
Traditional Order management



INTRANAV®
Current Ordering Process
Customer
INTRANAV® Sales
INTRANAV® Certificate Authority (Auth Key Generator)
INTRANAV® RTLS Platform
Rest API Microservice
Request Quotation
Send Quotation
Purchase Order
Process and Send Order along with the Authorization Key
Manage Asset & Access the Data using Authorization Key
Customer Sales Department
Customer Business Department
Customer End Application

Proposed Method of Order Management

Using Ethereum Blockchain



INTRANAV®
INTRANAV® Order Management
INTRANAV® Certificate Authority (Auth Key Generator)
INTRANAV® RTLS Platform
Rest API User & Asset Manager
Regular Customer Request Processing
Get Auth & Asset Management
Amazon® AWS*
Ethereum Blockchain Simulation
Rest API INTERNAL Access
History Contract
Asset Contract
Open Requests Contract
MAIN Contract
Oracle Service Contract
New Order
Request Pay
Payment
SEND Key
Asset Management
Access the Data using Authorization Key
Customer
Customer Application

What is Ethereum?

Ethereum Blockchain

What is Blockchain?

Blockchain is a specific type of database.

It differs from a typical database in the way it stores information; blockchains store data in blocks that are then chained together. As new data comes in it is entered into a fresh block. the most common use so far has been as a ledger for transactions.

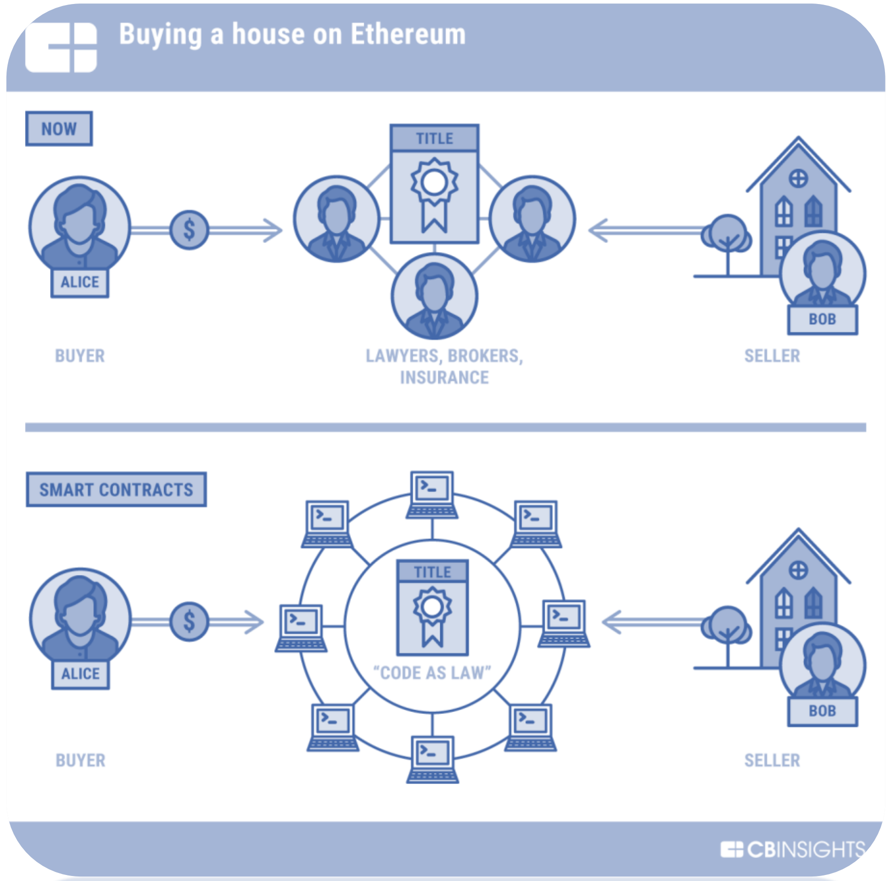
What is Ethereum?

Ethereum is a technology that lets you send cryptocurrency to anyone for a small fee. It also powers applications that everyone can use and no one can take down.

Ethereum builds on Bitcoin's innovation, with some big differences.

Both let you use digital money without payment providers or banks. But Ethereum is programmable, so you can also use it for lots of different digital assets – even Bitcoin!

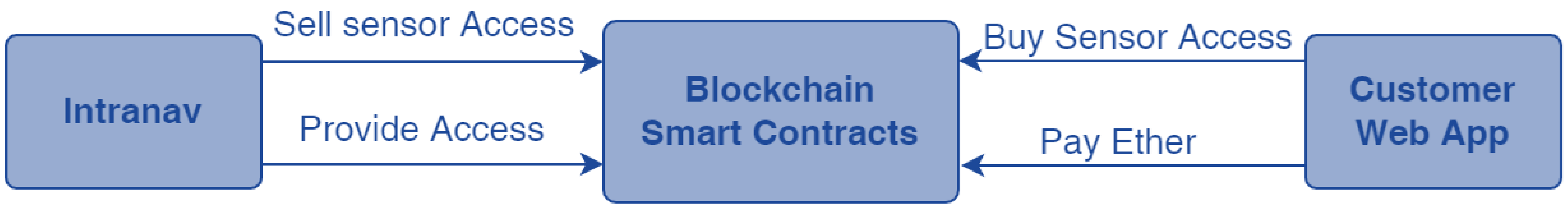
Ethereum is for more than payments. It's a marketplace of financial services, games and apps that can't steal your data or censor you.



Smart Contracts

What is Smart Contract?

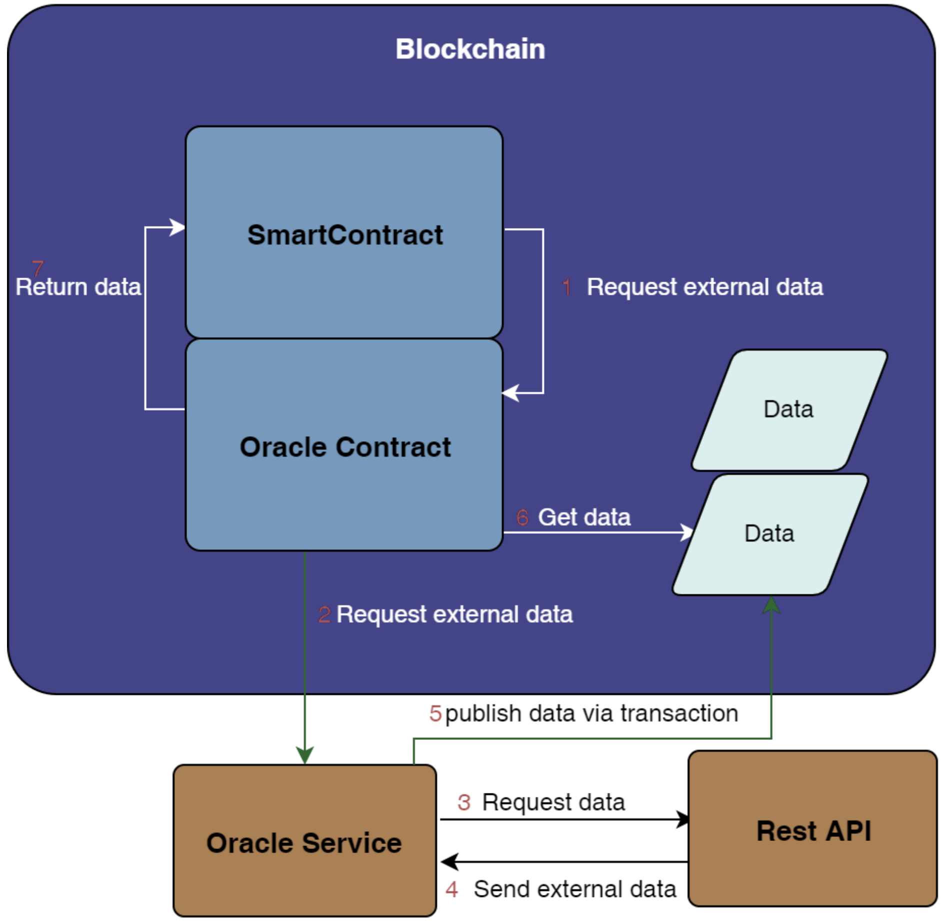
- It’s a digital contract
- Smart Contracts can be deployed on a blockchain
- Written in a Programming language (solidity for Ethereum).
- Limitation in size (24 KB).
- Can‘t use external API to get data.
- Each node needs to calculate(Mine) same result for same input for a contract method



Blockchain Oracle

How does an Oracle Work?

1. Inside Smart Contract call oracle function to get external data.
2. The Oracle contract requests the data from Oracle Service
3. The Oracle Service invoke a Rest API
4. The Oracle Service gets the data
5. The Oracle Service publishes the data on the blockchain
6. Oracle Contract callback function gets the data
7. The Oracle Contract returns the data
8. All nodes can mine the same result, since the data is published



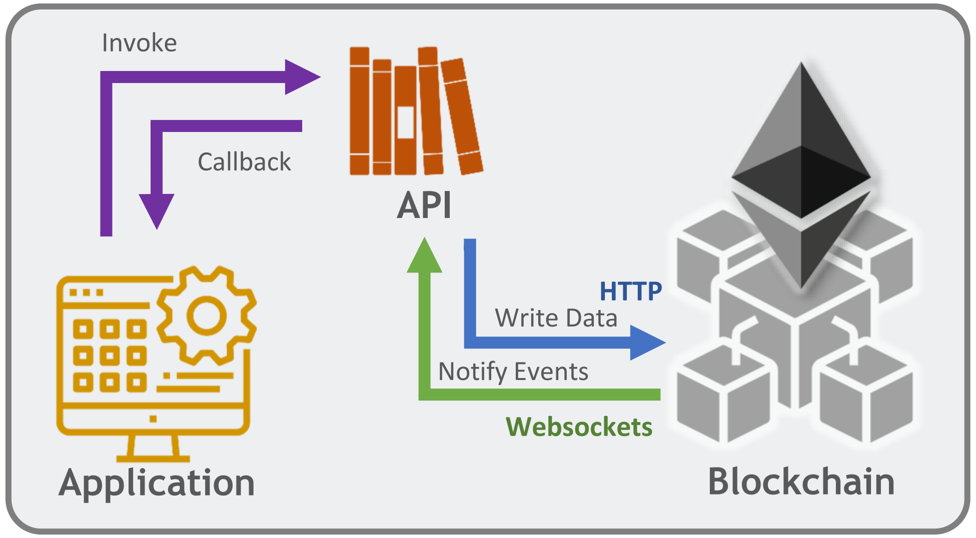
Communication with Blockchain

Description and Available APIs

JSON RPC API

Ethereum JSON-RPC APIs use a namespace system. RPC methods are clustered into several categories, depending on their usage. All method names are composed of the namespace, an underscore, and the actual method name within the namespace.

For example, the eth_call method resides in the eth namespace.
It will request data either from the node, execute an EVM function and return a response, or transmit data to the Ethereum network.



Different Languages and available API libraries

Language	API Library
.Net Framework (C#, F#)	Nethereum
Java, JavaScript	web3J, web3.js & Ethers.js
Golang	Geth (Go-Ethereum)
Others (If no API library exists)	JSON-RPC

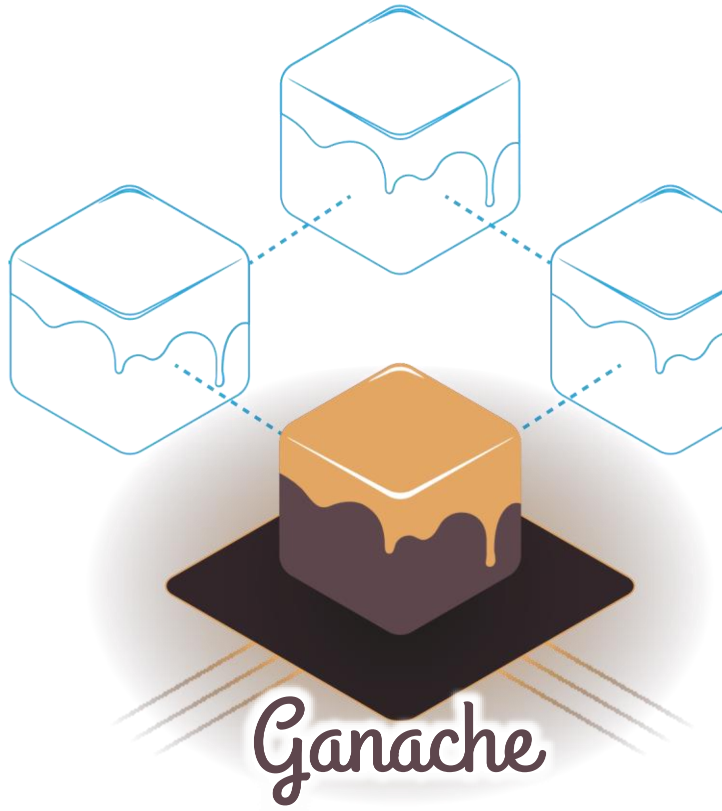
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
ccass
COMPETENCE CENTER FOR
APPLIED SENSOR SYSTEMS

Ganache

Ethereum Simulation Environment

What is Ganache?

Ganache is a personal blockchain for rapid Ethereum and Corda distr
application development. You can use Ganache across the entire dev
cycle; enabling you to develop, deploy, and test your dApps in a safe
deterministic environment.



Types of Ganache:

UI- Ganache UI is a desktop application supporting both Ethereum and Corda technology.
CLI- The command-line tool, ganache-cli (formerly known as the TestRPC), is available for Ethereum development.

How to Use Ganache CLI?

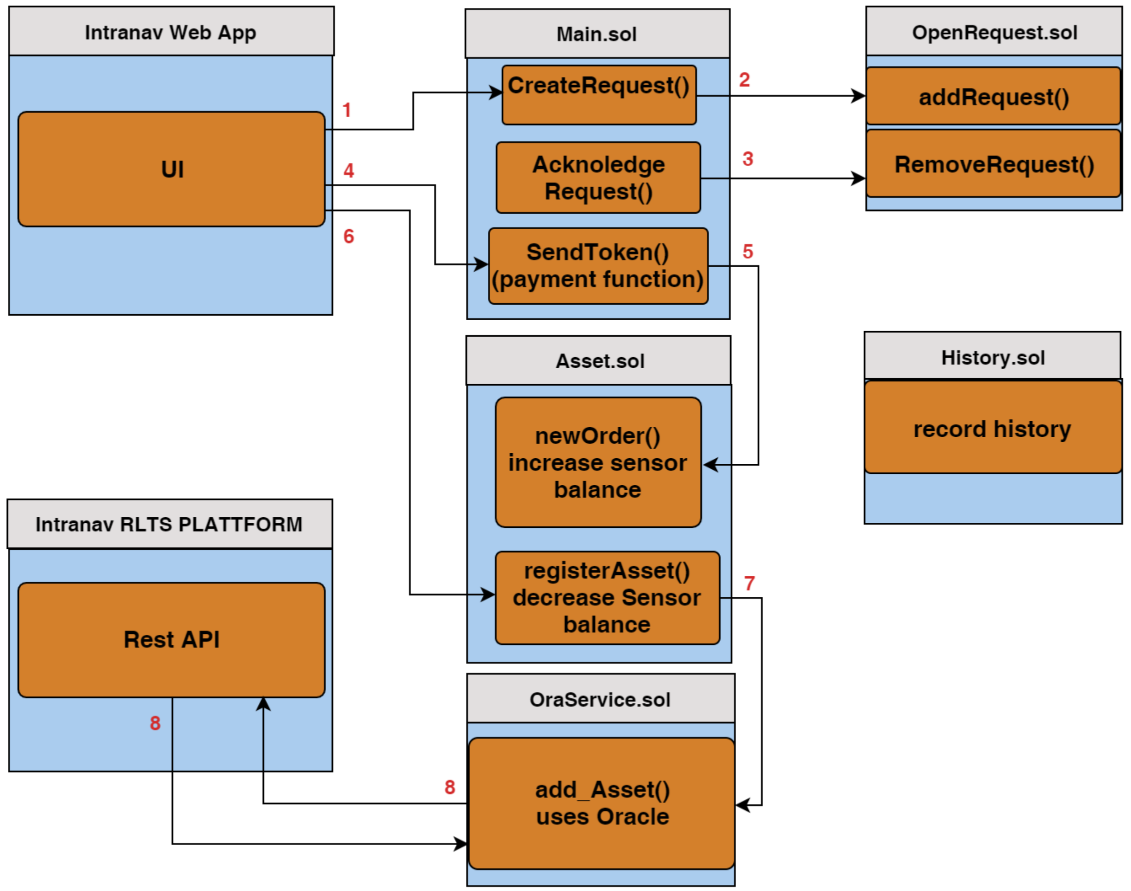
ganache-cli is written in JavaScript and distributed as a Node.js package via npm.
ganache-cli utilizes ganache-core internally, which is distributed with optional native dependencies for increased performance. If these native dependencies fail to install on your system ganache-cli will automatically fallback to ganache-core’s pre-bundled JavaScript build.

Smart Contracting Structure

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES
ccass COMPETENCE CENTER FOR APPLIED SENSOR SYSTEMS

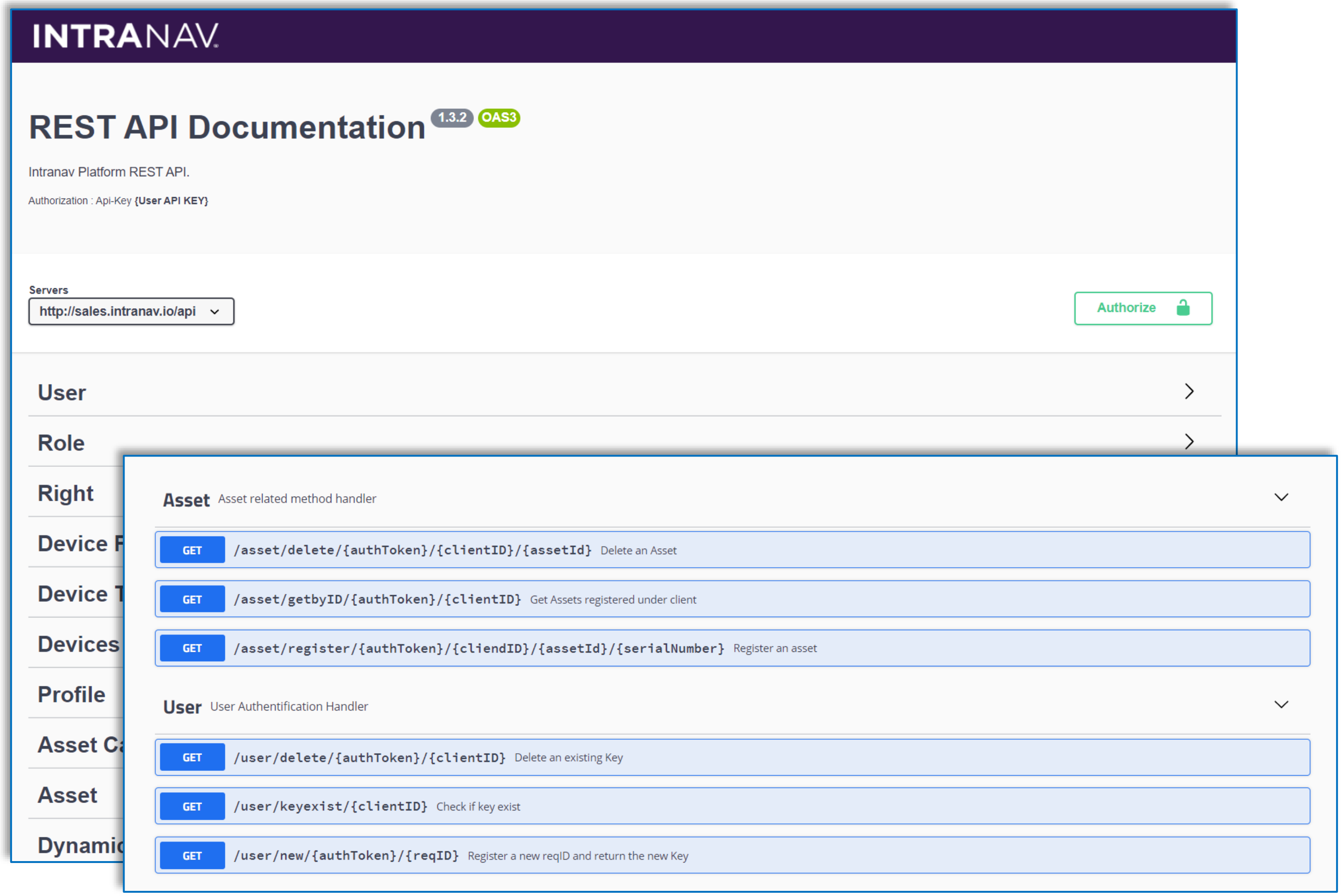
Contracting Process

1. The Customer creates the Request.
2. The Request will be inserted into open Requests.
3. Administrator can query the open requests and process accordingly.
4. Once acknowledged, the required amount will be calculated based on the request.
5. After successful payment in Ethereum, the clients quota increases with the new amount. Similarly, an authentication token will be requested from the REST API via Oracle Service.
6. Now the Customer can register an asset.
7. The Asset Smart Contract invoke a Oracle function.
8. The Oracle Service makes an Rest API call to add an asset



INTRANAV RTLS API Emulation

Sample API functions which can be integrated to the existing system



REST API Documentation 1.3.2 OAS3

Intranav Platform REST API.

Authorization : Api-Key {User API KEY}

Servers
http://sales.intranav.io/api

Authorize

User
Role
Right
Device F
Device T
Devices
Profile
Asset C
Asset
Dynamic

Asset Asset related method handler

GET	`/asset/delete/{authToken}/{clientID}/{assetId}`	Delete an Asset
GET	`/asset/getbyID/{authToken}/{clientID}`	Get Assets registered under client
GET	`/asset/register/{authToken}/{cliendID}/{assetId}/{serialNumber}`	Register an asset

User User Authentification Handler

GET	`/user/delete/{authToken}/{clientID}`	Delete an existing Key
GET	`/user/keyexist/{clientID}`	Check if key exist
GET	`/user/new/{authToken}/{reqID}`	Register a new reqID and return the new Key

Created using,

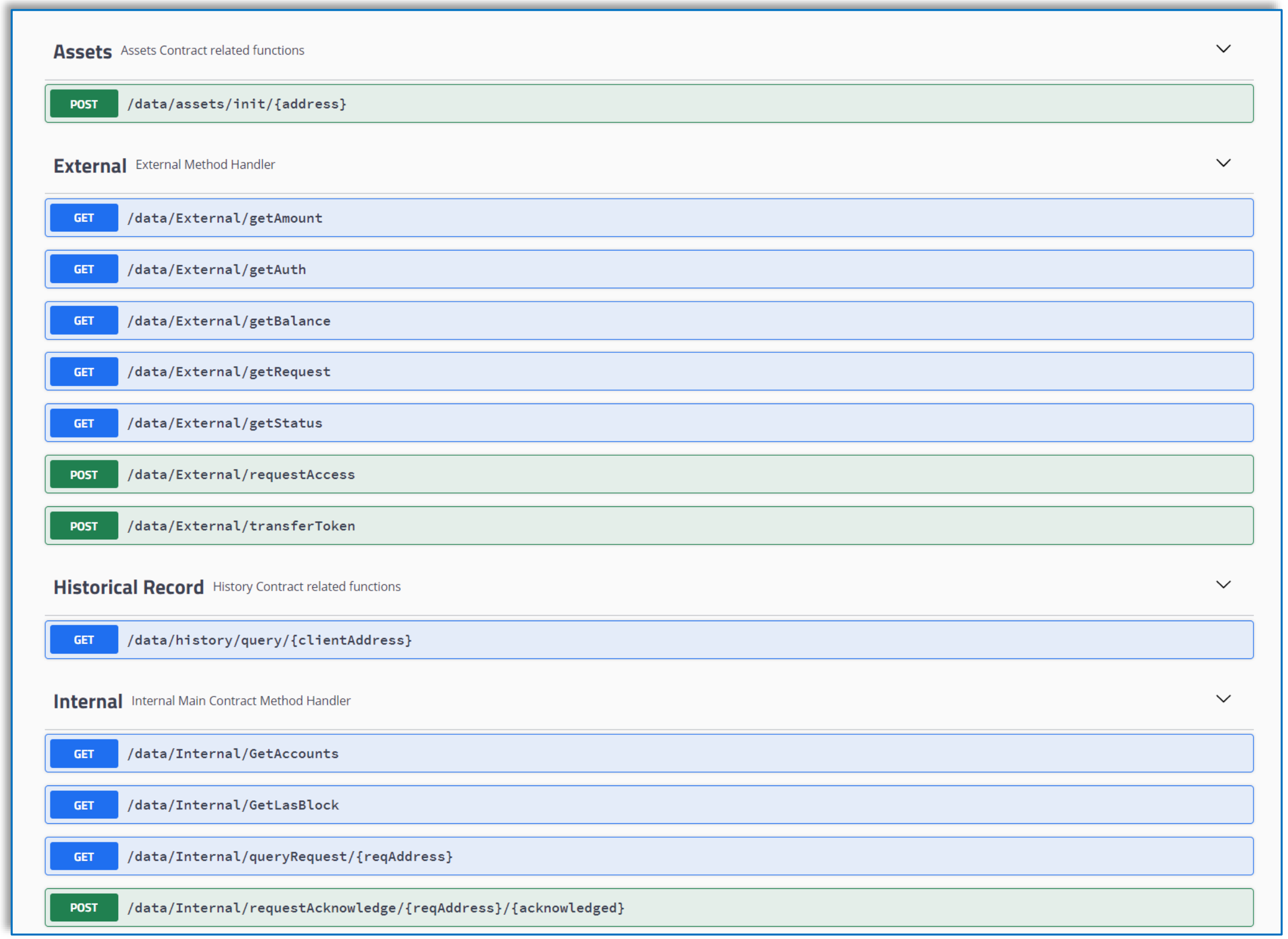
- **Language :** Java
- **Framework :** Openliberty
- **Type :** Microservice
- **Backend Communication :** None (Simulation Only)
- **Used libraries :**
  - **Java Security** – AES code generation
- **Source :**

  https://github.com/SachiHarshitha/HDa_TeamProject_SS21/tree/master/03_CompanyRestAPI

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
ccass
COMPETENCE CENTER FOR
APPLIED SENSOR SYSTEMS

Internal Process API

Internal Management API with All Access, Using Administrator Ethereum Account.


Assets Assets Contract related functions

POST /data/assets/init/{address}

External External Method Handler

GET /data/External/getAmount

GET /data/External/getAuth

GET /data/External/getBalance

GET /data/External/getRequest

GET /data/External/getStatus

POST /data/External/requestAccess

POST /data/External/transferToken

Historical Record History Contract related functions

GET /data/history/query/{clientAddress}

Internal Internal Main Contract Method Handler

GET /data/Internal/GetAccounts

GET /data/Internal/GetLasBlock

GET /data/Internal/queryRequest/{reqAddress}

POST /data/Internal/requestAcknowledge/{reqAddress}/{acknowledged}

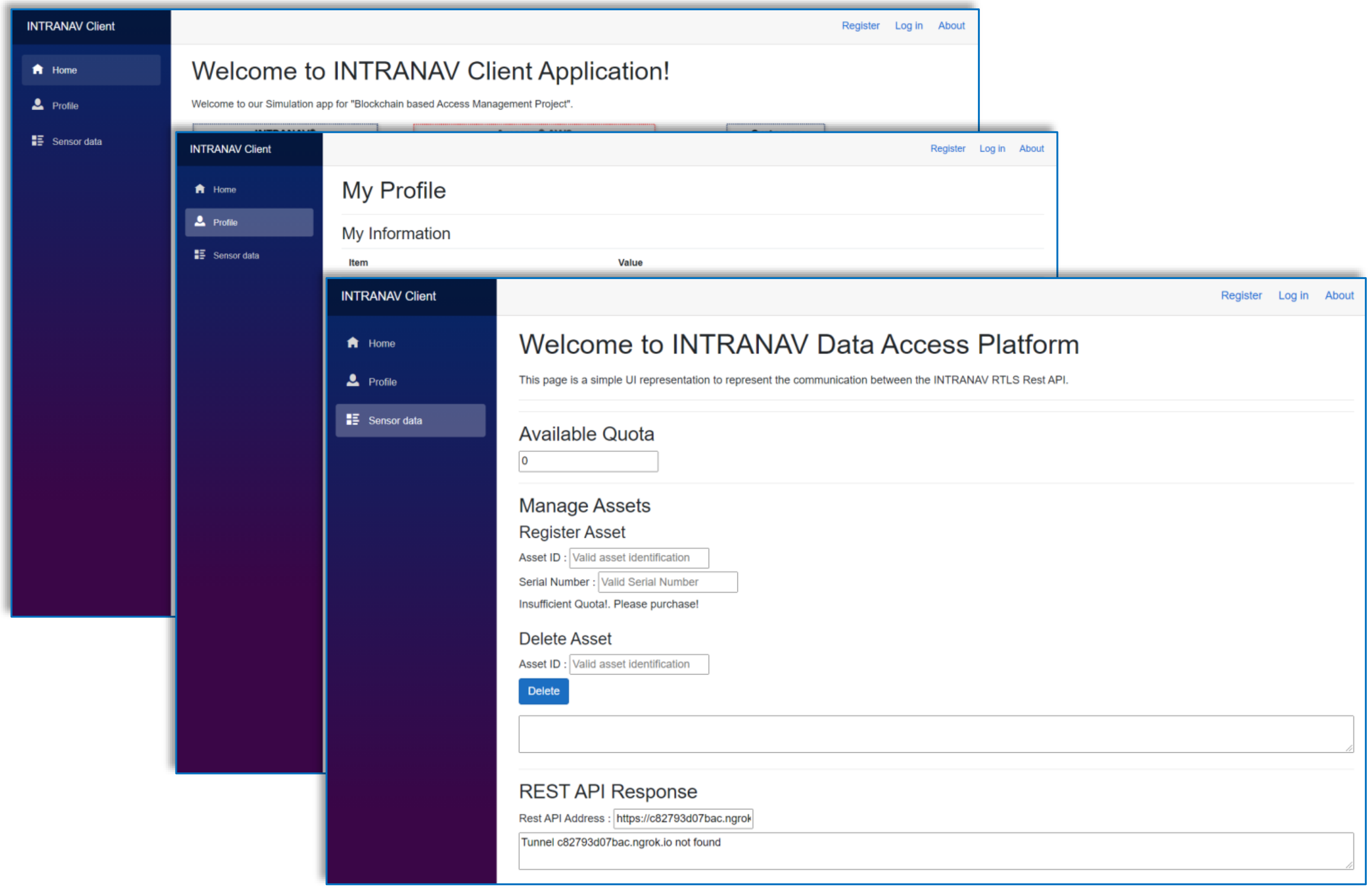
Created using,

- **Language :** Java
- **Framework :** Openliberty
- **Type :** Microservice
- **Backend Communication :** Direct
- **Used libraries :**
  - **web3j** – Blockchain to App
- **Source :**

  https://github.com/SachiHarshitha/HDa_TeamProject_SS21/tree/master/04_InternalRestAPI

Client Portal

Conceptual Client Portal Application which could be used to decouple the client only processes


INTRANAV Client

Register Log in About

Home

Profile

Sensor data

Welcome to INTRANAV Client Application!

Welcome to our Simulation app for "Blockchain based Access Management Project".

My Profile

My Information

Item	Value

Welcome to INTRANAV Data Access Platform

This page is a simple UI representation to represent the communication between the INTRANAV RTLS Rest API.

Available Quota

0

Manage Assets

Register Asset

Asset ID : Valid asset identification

Serial Number : Valid Serial Number

Insufficient Quota!. Please purchase!

Delete Asset

Asset ID : Valid asset identification

Delete

REST API Response

Rest API Address : https://c82793d07bac.ngrok

Tunnel c82793d07bac.ngrok.io not found

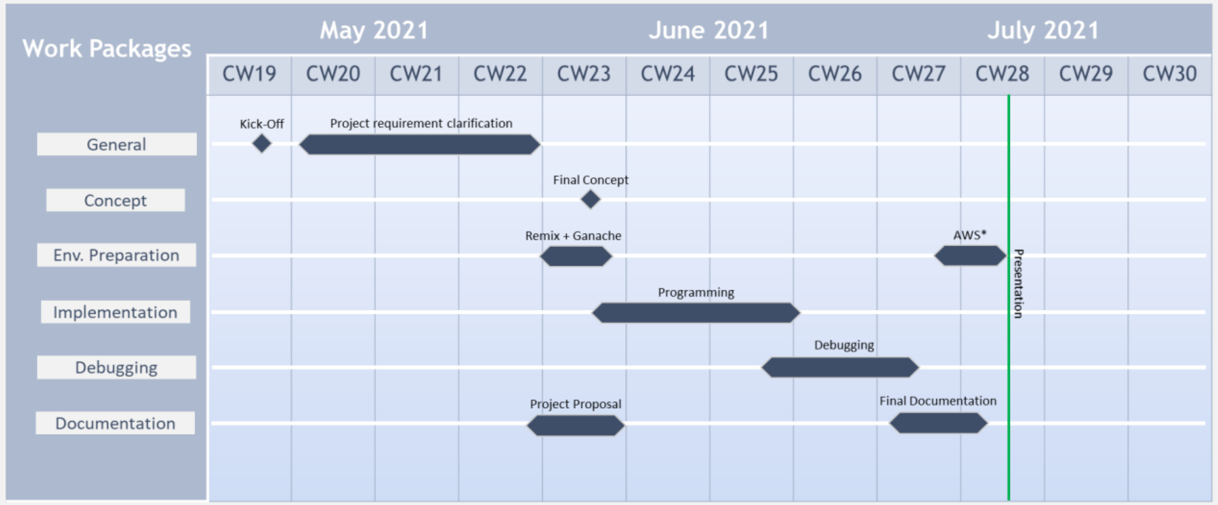
Created using,

- **Language :** C#
- **Framework :** .Net Core
- **Type :** Blazor Server Application
- **Backend Communication :** Direct
- **Used libraries :**
    - **Nethereum** – Blockchain to App
    - **RestSharp** – Rest API to App
- **Source :**

  https://github.com/SachiHarshitha/HDa_TeamProject_SS21/tree/master/05_ClientWebApp

Project Status

Timeline

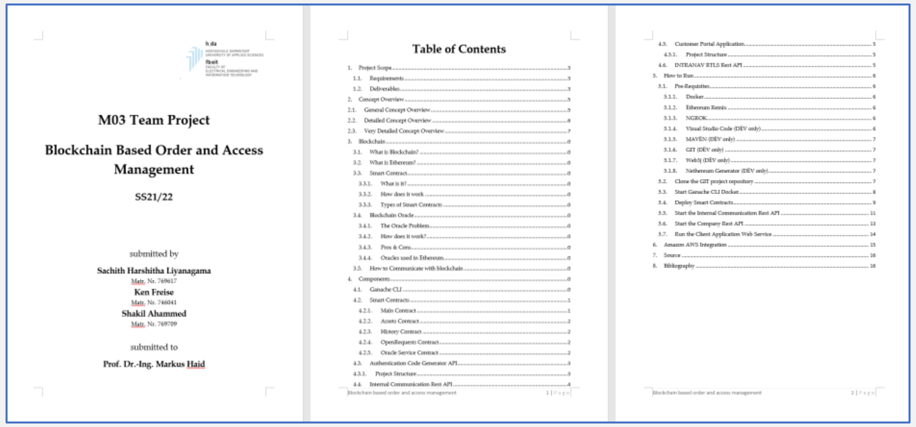


Project Path

Github : https://github.com/SachiHarshitha/HDa_TeamProject_SS21

Deliverables

01. Report



M03 Team Project

Blockchain Based Order and Access Management

SS21/22

submitted by

Sachith Harshitha Liyanagama
Matr. Nr. 769617
Ken Freise
Matr. Nr. 746041
Shakil Ahammed
Matr. Nr. 769709

submitted to

Prof. Dr.-Ing. Markus Haid

Table of Contents

Blockchain based order and access management 1 | Page

Blockchain based order and access management 2 | Page

02. Source Code

Can be found in project path.

03. Running Application Demonstration

Will be attached later.

Application Demonstration