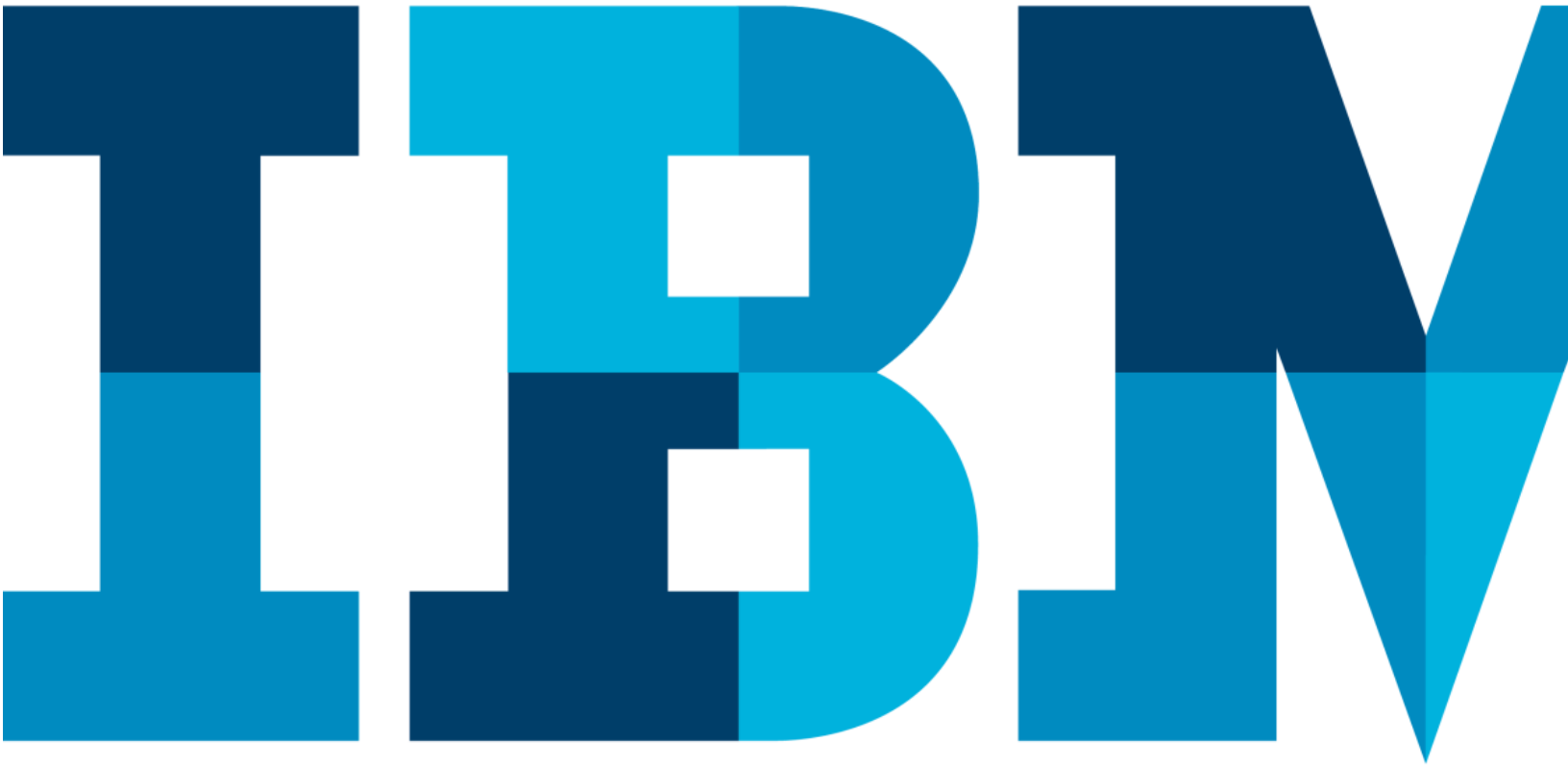
IBM Blockchain Platform Hands-On

Lab 4:

Verifiable Exchange with Private Data Collections



IBM

Table of Contents

Disclaimer 3
Overview of the lab environment and scenario 5
Simplified Commodity Trading Exchange 6
Trade Network 11
Lab Structure 12
1 Build and Start Fabric for the 'Trade Network' 13
2 Deploy the first version of the Smart Contract to test & prove the Trade Network 30
3 Private Data for the Offer and Accept Transactions 38
3.1 Invoking the Offer and Accept transactions 43
4 Work with the Cross Verify Functions 54
4.1 Understanding the Cross-Verify implementation 56
4.2 Performing the Cross Verification of Private Data 63
5 Add Demo Data and Private Query Transaction 70
5.1 Create some Demo Data for querying data 71
5.2 Executing Rich Queries against the Private Data Collections 74
We Value Your Feedback! 80
Appendix 1 - transaction List Info for 'exchangecontract' 81
Appendix 2 Access control considerations for Private data 83
Appendix 3 - Alternate Trade Network Fabric 84

Disclaimer

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results like those stated here.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Overview of the lab environment and scenario

This lab is the 4th lab in the series and shows how the IBM Blockchain Platform Extension for VS Code can be used to work with Private Data Collections. The lab uses a local custom fabric.

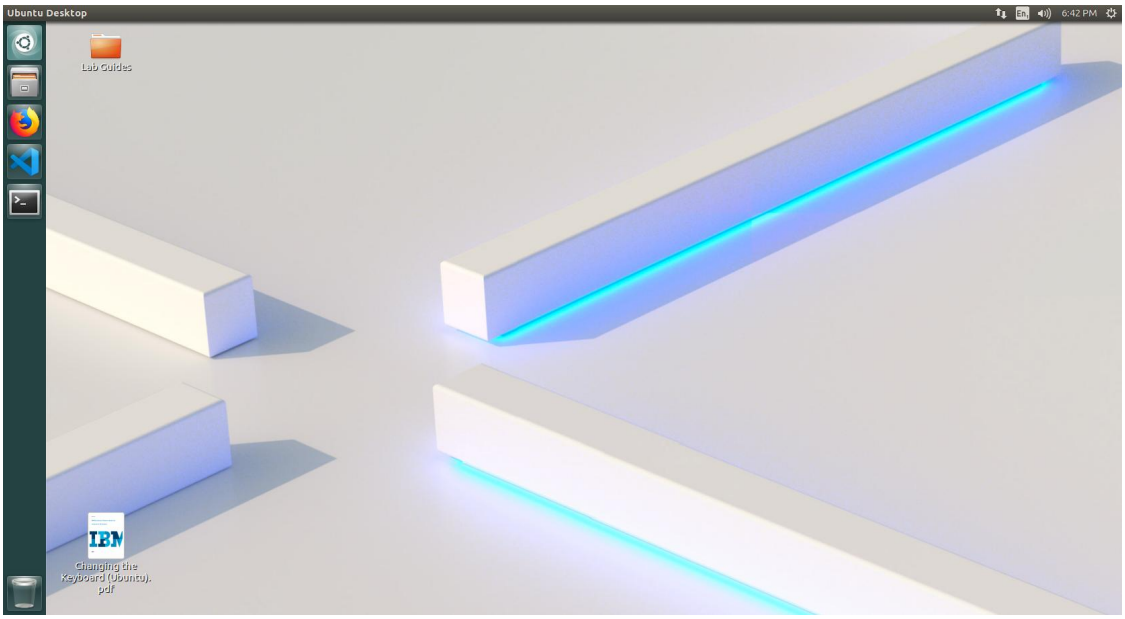
***Note**: The screenshots in this lab guide were taken using version **1.39.2** of **VS Code**, and version **1.0.12** of the **IBM Blockchain Platform** extension. If you use different versions, you may see differences from those shown in this guide.*

Start here. Instructions are always shown on numbered lines like this one:

__ **1.** If it is not already running, start the virtual machine for the lab. Your instructor will tell you how to do this if you are unsure.

__ **2.** Wait for the image to boot and for the associated services to start. This happens automatically but might take several minutes. The image is ready to use when the desktop is visible as per the screenshot below.

Note: If it asks you to login, the userid and password are both "**blockchain**".



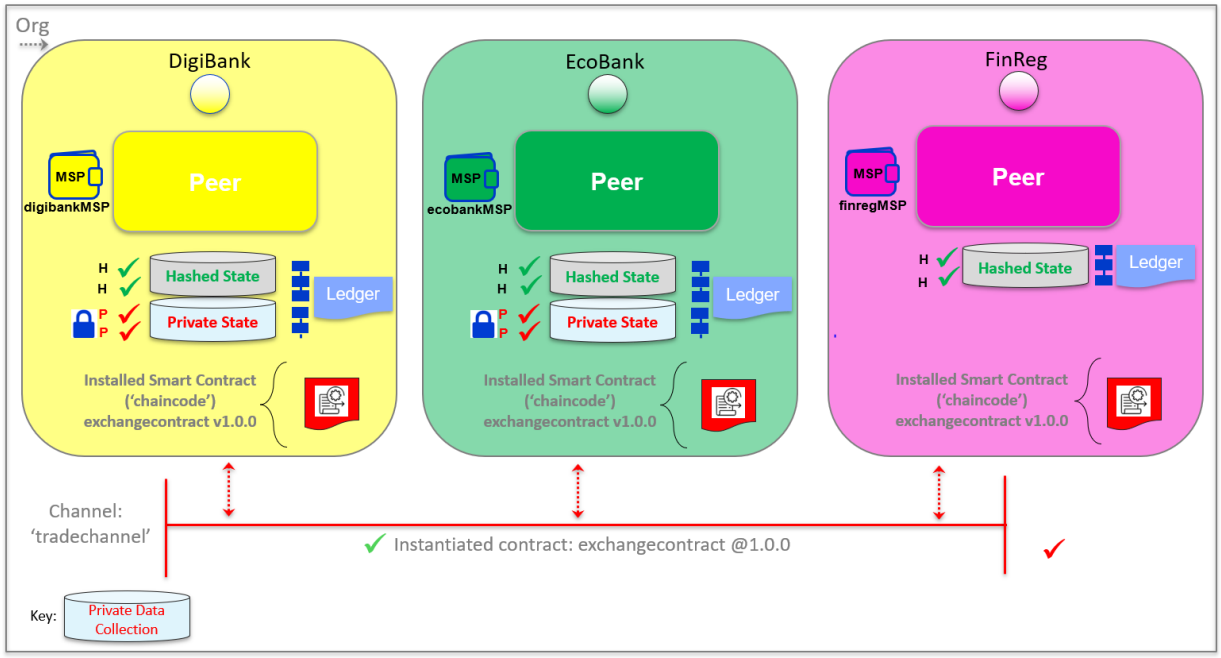
Simplified Commodity Trading Exchange

DigiBank and **EcoBank** participate (as investing banks) in a Commodity Exchange network – the buying and selling **Commodity Contracts** (legal contracts) for investment purposes). A commodity exchange is a regulated marketplace that facilitates the purchase and sale of such **Commodity Contracts** whose values are tied to the price of commodities (e.g., oil, corn, silver, gold). These contracts represent the total value or price of tradeable commodities. Each advertised commodity has a Contract ID in this lab. So in summary: a Contract is put up for sale – i.e. it is advertised at a 'market' price, then offers (and counter offers perhaps) are made, before finally an offer is accepted by the seller and a deal is made. It then remains to cross-verify the offer details against the original offer and write that status to the ledger.

In this lab example we see that Ecobank and Digibank have private data collections when it is likely that both banks know all the data! But imagine a scenario where there are many more banks trading. Digibank would not be the only bank making an offer, and these multiple offers would be kept private and confidential so "Bigbank" for instance would not be aware of the offer that Digibank made.

An overview of the exchange network on the blockchain and organisations involved, is shown below:

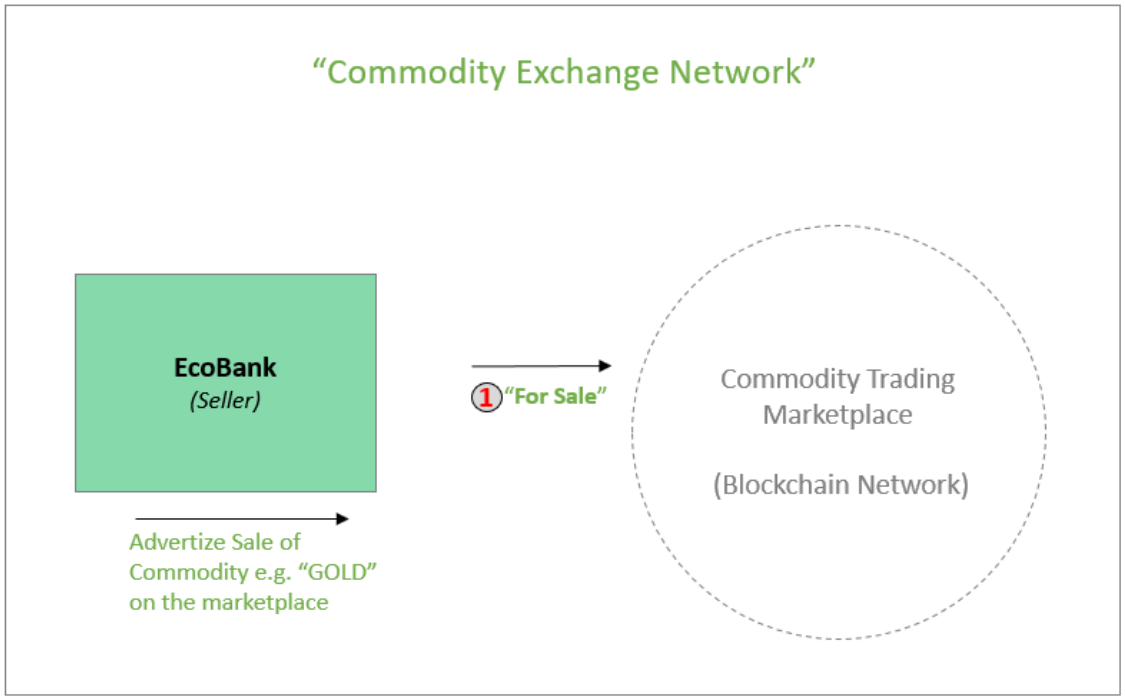
Commodity Trading Exchange: Overview



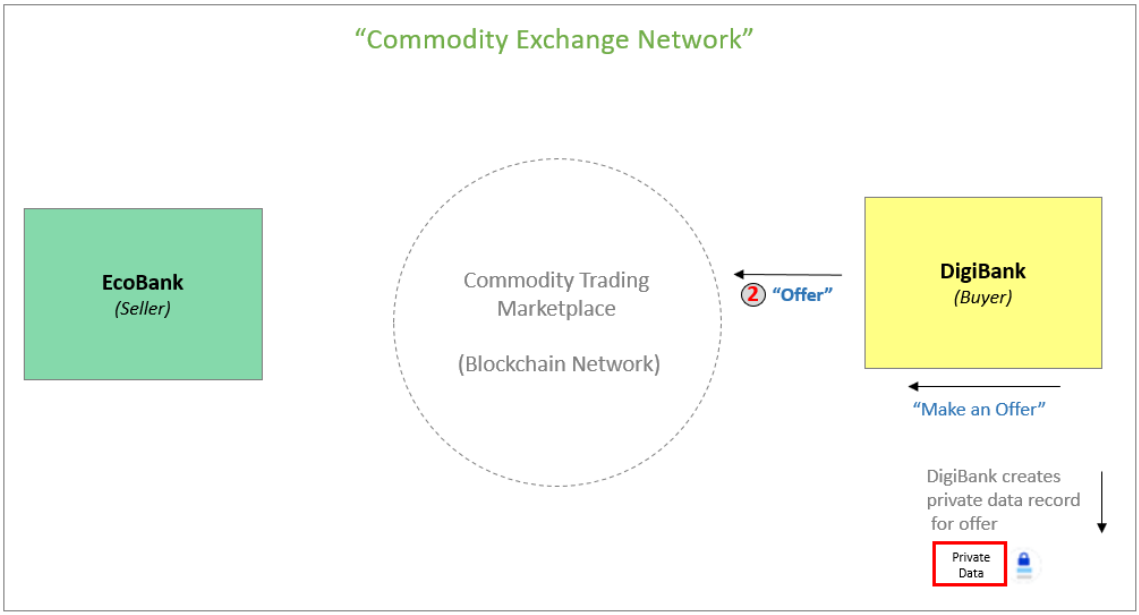
Notice in the above diagram, the regulator **FinReg** does not store any private data of its own – it does however have a copy of the ledger including the hashed state ledger. Its role is to audit records – e.g. third-party verification or dispute resolution of private data, shared with it. The hash state of the private data on the ledger, serves as evidence of the original private data transaction; the third party can compute the hash of the private data and see if it matches the state.

The smart contract reflects the transactions in this network – lets examine the transaction in the lab:

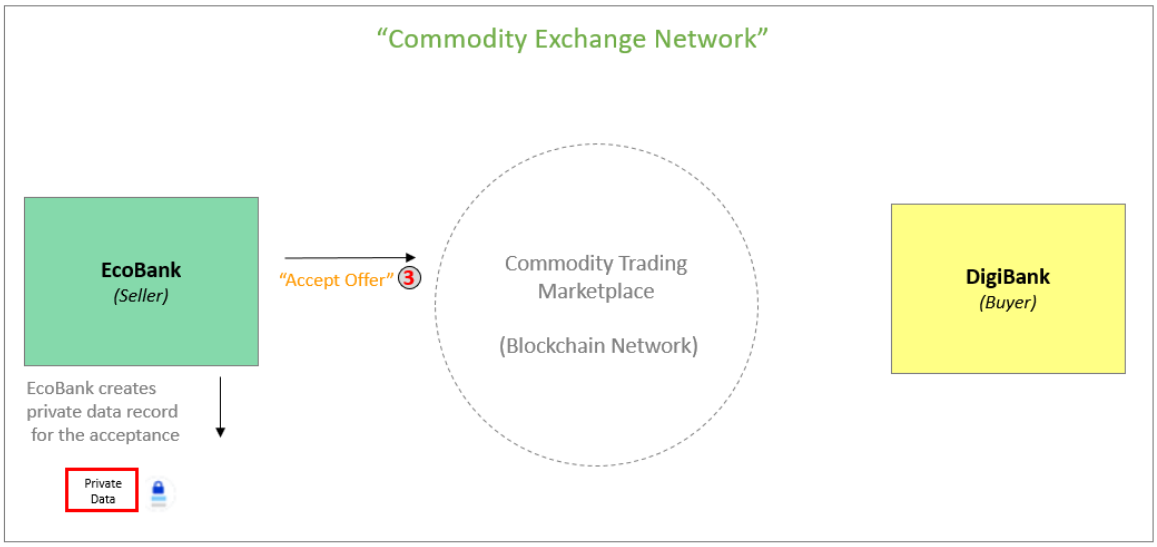
1. **EcoBank** advertises or 'broadcasts' a commodity contract for sale on the marketplace



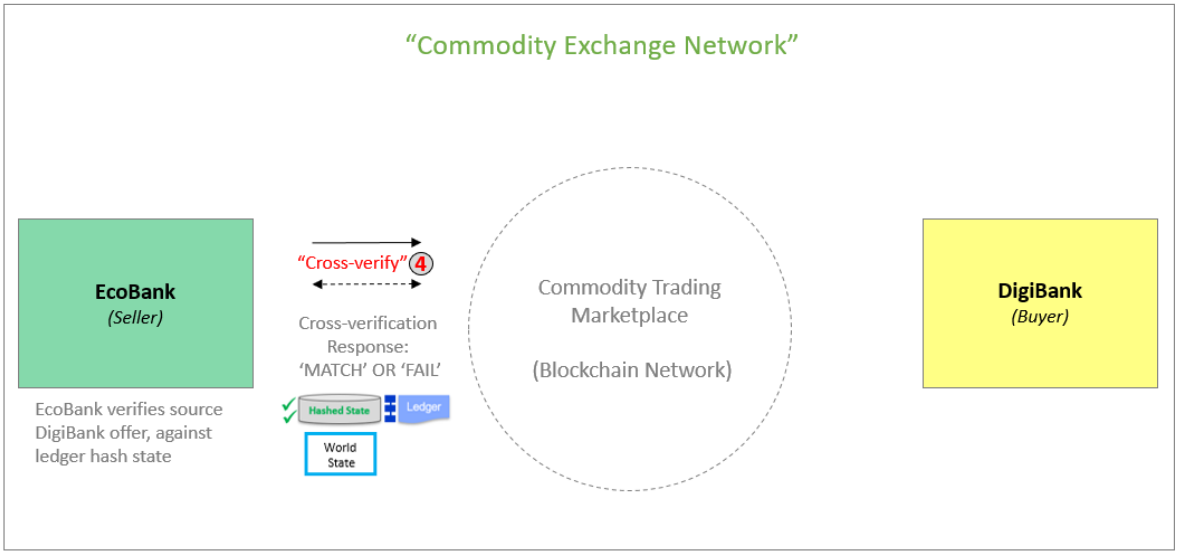
2. **DigiBank** makes an offer to EcoBank. Note that DigiBank writes a record of this offer, to its own private data store. A cryptographic 'hash' of the record is also recorded on the blockchain (channel world state).



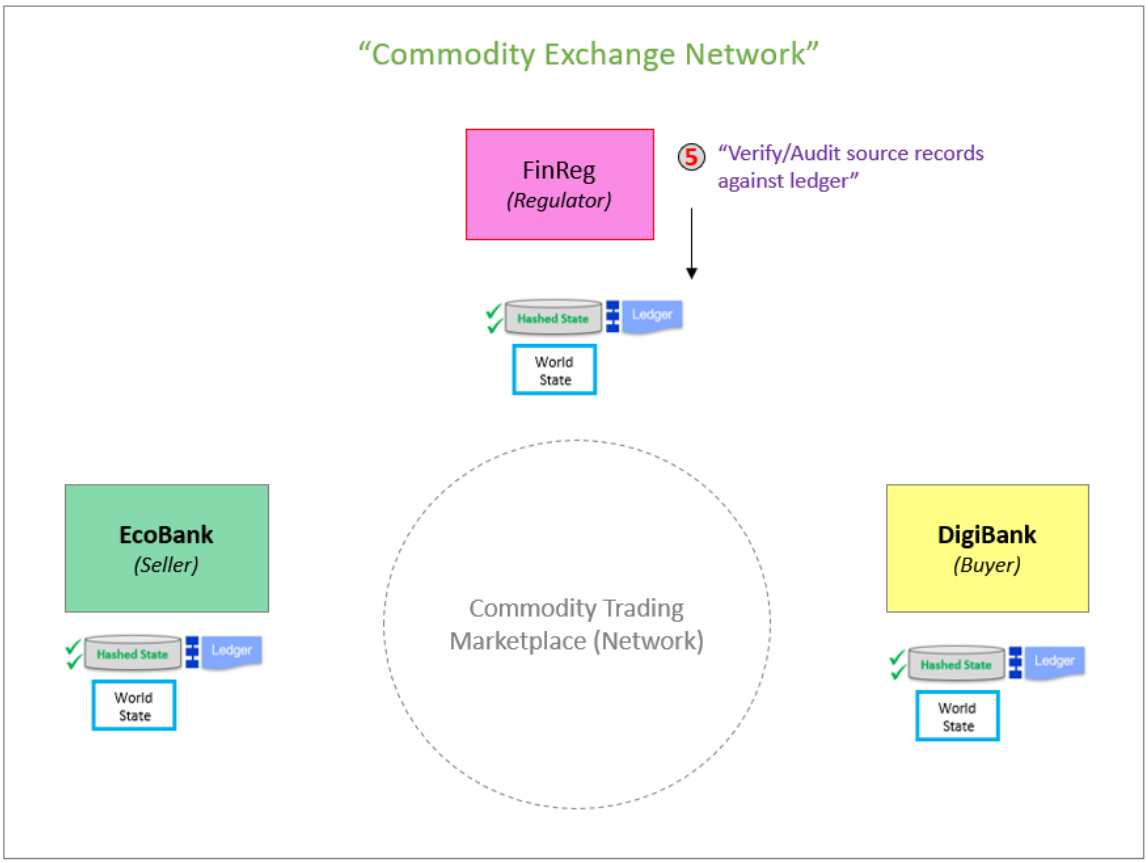
3. **EcoBank** receives the offer and informs DigiBank that it accepts the offer; EcoBank writes its own 'accept with offer' record to its own private data store – the offer on the ledger is as yet UNVERIFIED – meaning, it needs to be cross-verified.



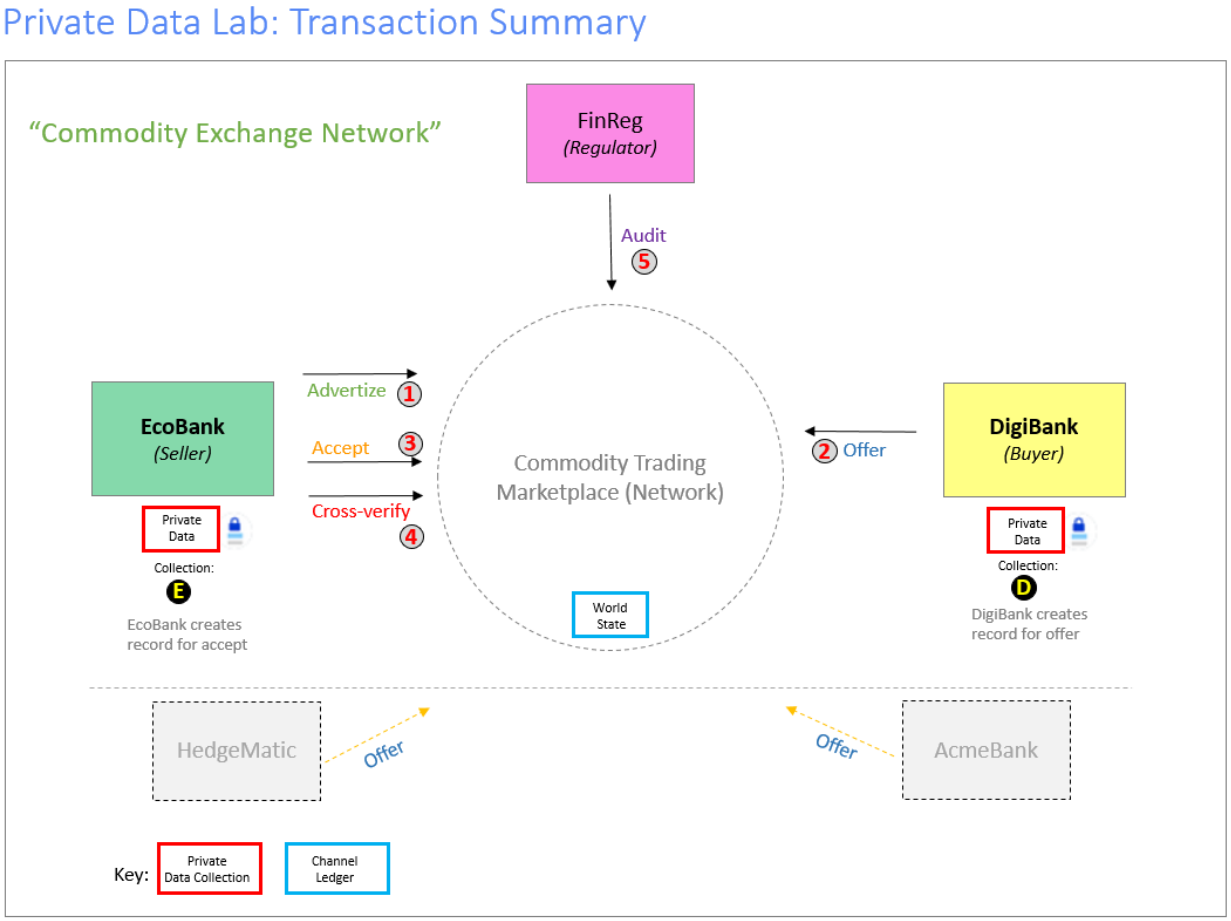
4. **EcoBank** calculates a hash of the source offer private data and verifies this hash, against the private data hash that was written by DigiBank in step 2. The smart contract compares the hashes and if they match, will update the accept/offer to 'CROSSVERIFIED' – this status attribute is not actually private – it is shared as a general status on the ledger that the organisations share.



5. **FinReg**, a 3rd party regulator, sometime later, carries out audit checks and takes source offer or accept data, and cross-verifies the records, against the hashes originally written to the ledger.



The following diagram contains a consolidated transaction summary:



Note that we focus on 3 organisations in this lab exercise; but remember, there could eventually be more (reference the grey boxes in the above diagram) already joined the network and be on the same channel.

FinReg, the regulator – will, later in the lab, require to validate historical offers or accepts, to see they are the genuine, source data that each organisation (DigiBank, EcoBank) recorded, independently.

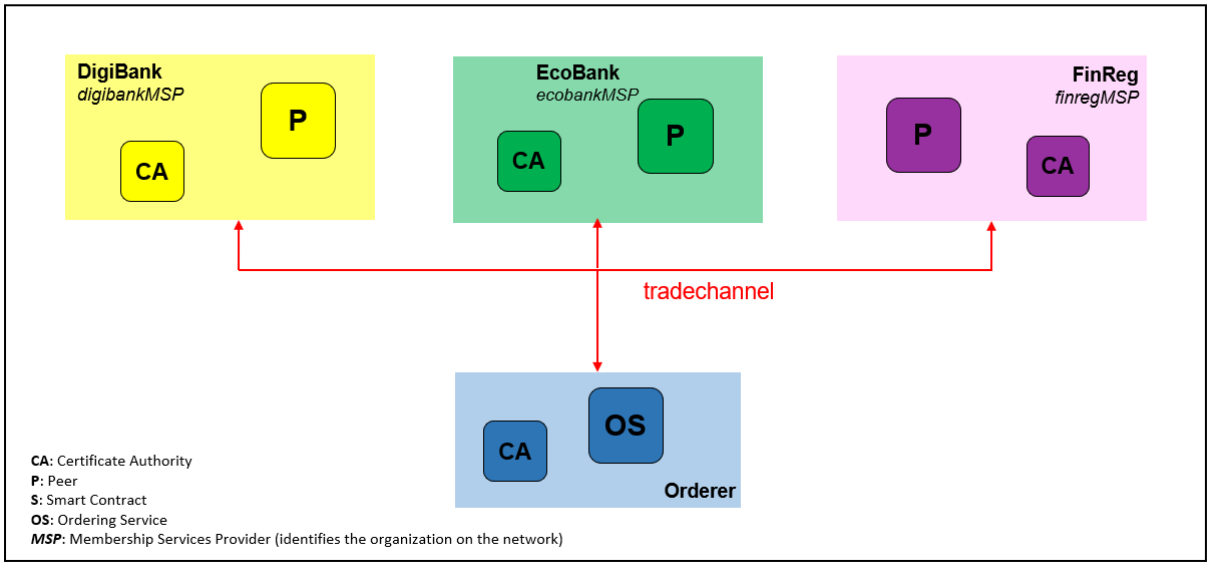
Trade Network

The lab uses a custom Hyperledger Fabric network with 3 Organisations to illustrate the Private Data features of Hyperledger Fabric. It comprises a set of Docker Containers built with Ansible scripts.

The Ansible tool is an open-source is a configuration and deployment tool. The VM contains Ansible scripts to build the custom network for the lab – these scripts run inside a Docker container. The Lab requires no knowledge of Ansible, just an awareness that it is being used.

The scripts and the build process are currently an evaluation example, but a similar feature may be integrated with the VS Code extension in the future to allow more realistic topologies to be available to developers.

Custom Network



The diagram illustrates the Custom Network showing the channel used is **tradechannel.** Each Peer will be using CouchDB as the State Database to enable rich queries to be run in the Lab.

Lab Structure

This lab is structured into 6 parts (one is optional, to complete if time allows).

Part 1 of this lab will take you through Building and Starting the Fabric for the Trade Network.

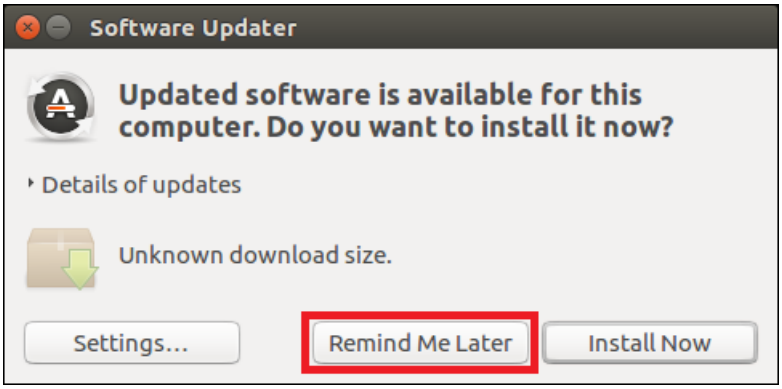
Part 2 of this lab will deploy the first version of the Smart Contract that is used to test and prove the Trade Network Fabric

Part 3 of this lab will focus on the Offer and Accept transactions and the writing of the initial Private Data.

Part 4 of this lab will show the Cross-Verify transactions allowing parties to verify the hashes of data of Private Data collections.

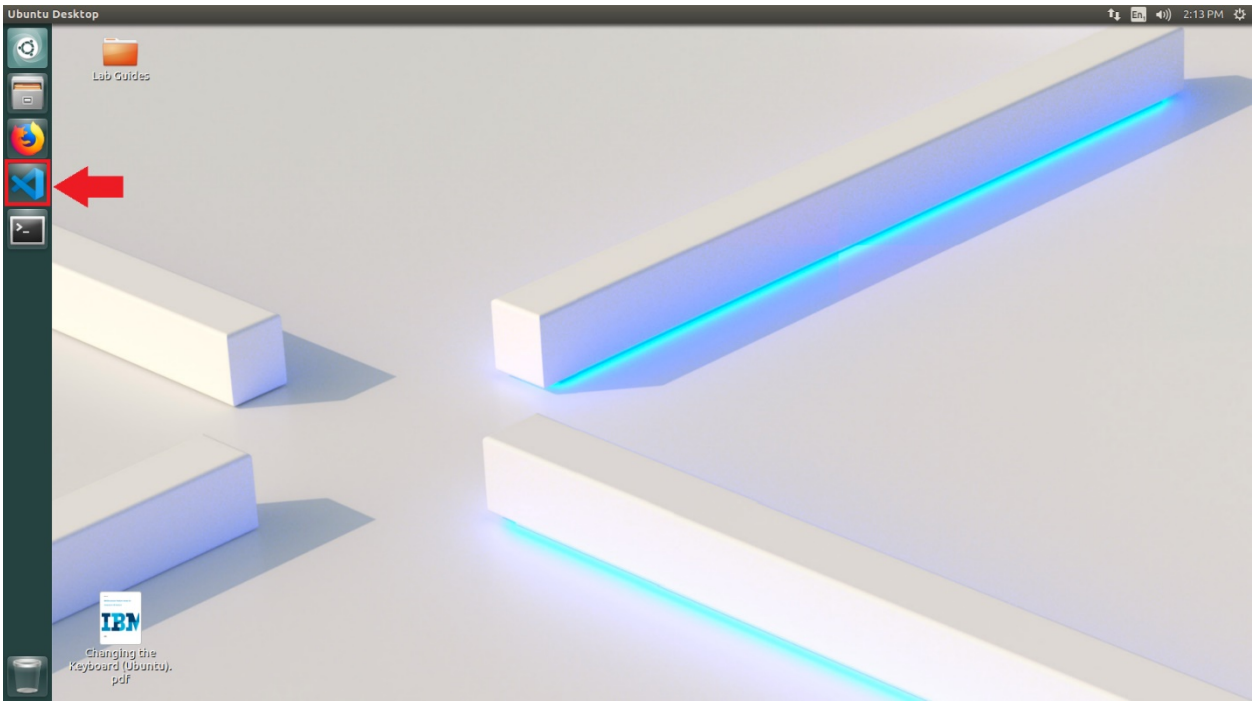
Part 5 adds additional sample private data for queries, and works with rich query transactions, running against the Private Data Collections

Note *that if you get an "Software Updater" pop-up at any point during the lab, please click "****Remind Me Later****":*

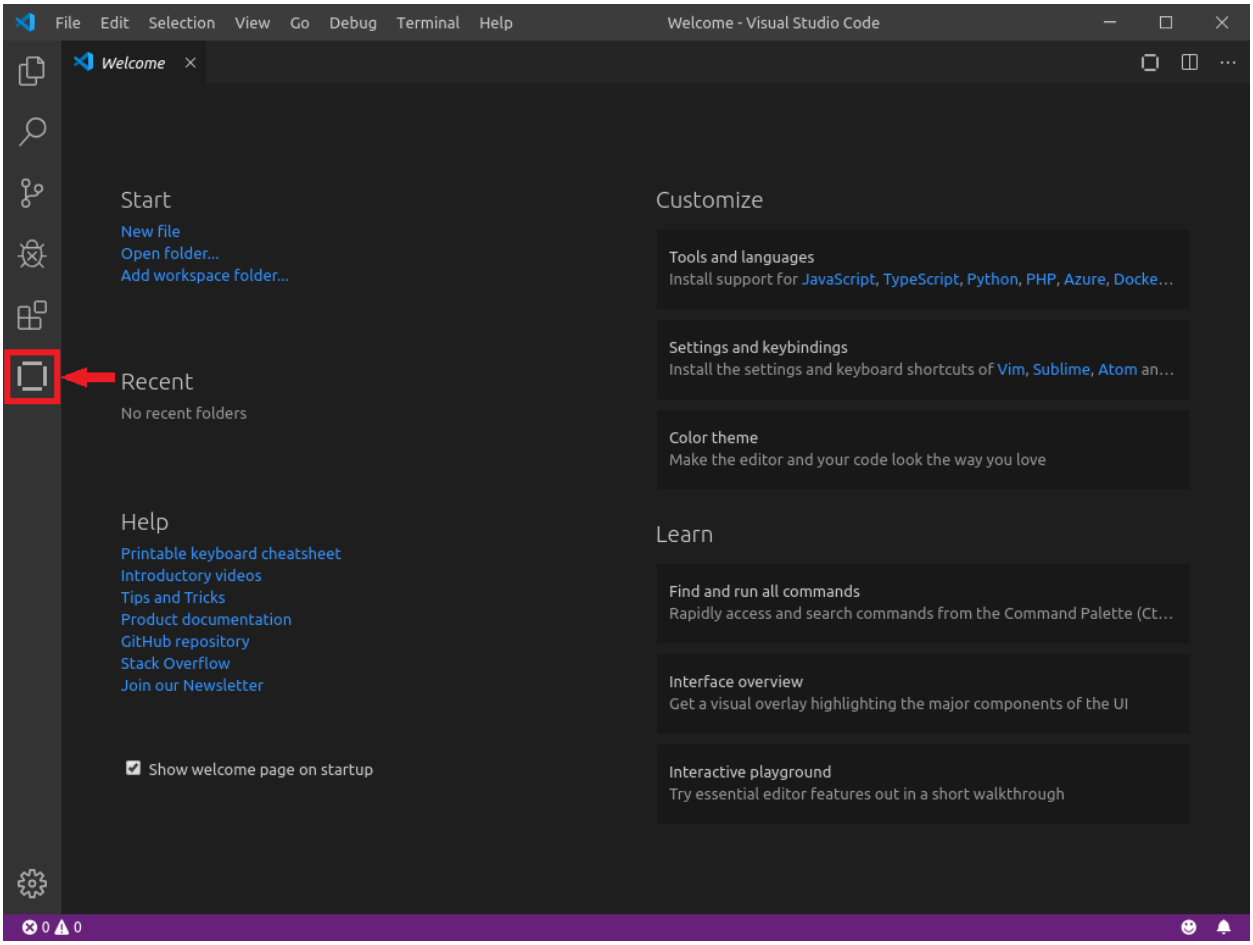


1 Build and Start Fabric for the ‘Trade Network’

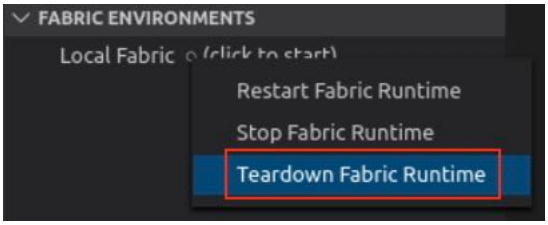
__ **3.** VS Code may already be running from a previous lab exercise, but if not, launch VS Code by clicking on the VS Code icon in the toolbar.



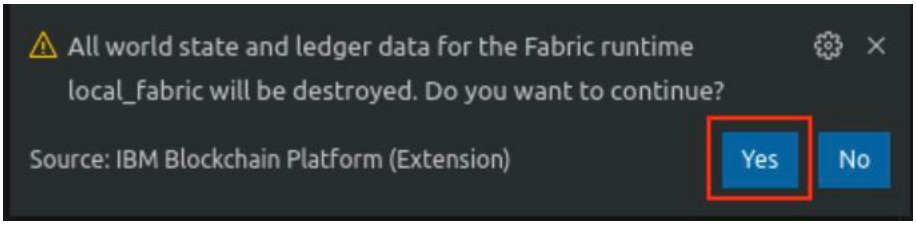
__ **4.** When VS Code opens, click on the IBM Blockchain Platform icon in the Activity Bar in VS Code as shown below.



__ **5. Right click** on the **Local Fabric** environment and click the option the **Teardown Fabric Runtime:**



Click **Yes** in the bottom right corner to confirm the teardown.

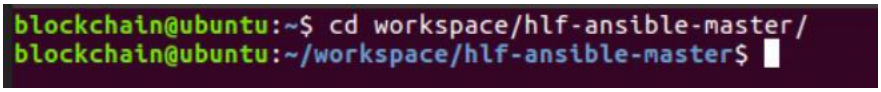


We are now going to start the custom Hyperledger Fabric network. This VM includes a script to automate the process.

__ **6.** On the Ubuntu Dock **click** the **Terminal** icon to open a new terminal window:

__ **7.** Using the following command in the terminal, change to the folder containing the ansible build scripts:

```
cd workspace/hlf-ansible-master/
```

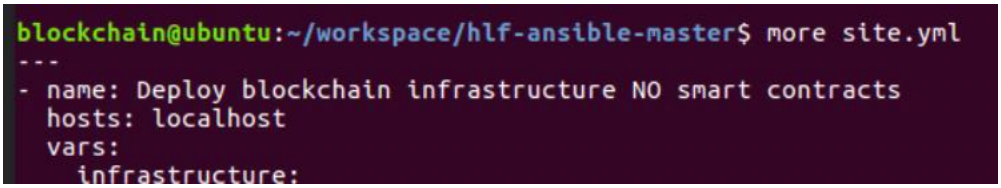


The Custom Fabric will be built based on a "playbook" file in yaml format. The playbook describes the network we will use in the lab and is consumed by the Ansible scripts described in the introduction.

Briefly examine the playbook in the terminal window.

__ **8.** Type the following command:

```
more site.yml
```

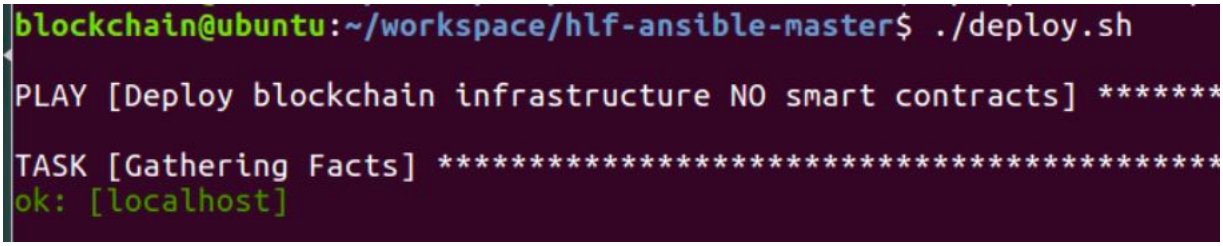


(When using the "more" command, Press the spacebar for "Next Screen".)

Note the definition of **ecobankMSP** and the **ids** associated with Ecobank – you will use them later in this section.

Issue the following command to run the deploy script which runs the docker container to build the Trade Network fabric. (The command takes about 2 minutes to complete and writes many lines of output in the terminal.)

```
./deploy.sh
```



Successful completion of this command will look similar to the following:

Don't worry about the red Fatal message – the script can optionally deploy a Smart Contract but in this lab the Smart Contract will be manually deployed later.

> ***Note***
>
> If you see a red error ending with "Bind for 0.0.0.0:17054 failed port is already allocated" then the Local Fabric in VS Code is still present and needs a teardown as described in Step 5.

__ **9.** Run the following command to verify that the 11 expected containers are running. "docker ps" is the command to display running containers, and the format parameter is just used to simplify the output.

```
docker ps --format 'table {{.Names}}:\t {{.Ports}}'
```

```
blockchain@ubuntu:~/workspace/hlf-ansible-master$ docker ps --format 'table {{.Names}}:\t {{.Ports}}'
NAMES:                          PORTS
orderer.example.com:            7050/tcp, 0.0.0.0:17050->17050/tcp
ca.orderer.example.com:         7054/tcp, 0.0.0.0:16054->16054/tcp
peer0.finreg.example.com:       0.0.0.0:19051-19052->19051-19052/tcp
couchdb0.finreg.example.com:    4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp
ca.finreg.example.com:          7054/tcp, 0.0.0.0:19054->19054/tcp
peer0.digibank.example.com:     0.0.0.0:18051-18052->18051-18052/tcp
couchdb0.digibank.example.com:  4369/tcp, 9100/tcp, 0.0.0.0:6984->5984/tcp
ca.digibank.example.com:        7054/tcp, 0.0.0.0:18054->18054/tcp
peer0.ecobank.example.com:      0.0.0.0:17051-17052->17051-17052/tcp
couchdb0.ecobank.example.com:   4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp
ca.ecobank.example.com:         7054/tcp, 0.0.0.0:17054->17054/tcp
```

__ **10.** In order to have full access to some configuration files, file protections need to be modified. Run the following 2 commands to modify the file protection – if requested for the password enter ***blockchain***

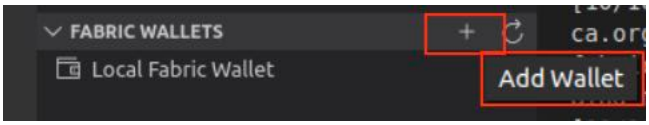
```
sudo chown -R blockchain:blockchain wallet/
sudo chown -R blockchain:blockchain nodes/
```

```
blockchain@ubuntu:~/workspace/hlf-ansible-master$ sudo chown -R blockchain:blockchain wallet/
blockchain@ubuntu:~/workspace/hlf-ansible-master$ sudo chown -R blockchain:blockchain nodes/
blockchain@ubuntu:~/workspace/hlf-ansible-master$
```

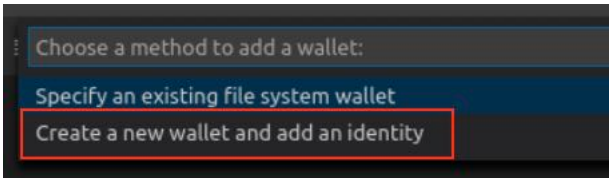
The network is now created and running, it is time to create wallets and import identities into them. This will allow us to access the network from within VS Code.

We will first create the wallet and import identities for **EcoBank**

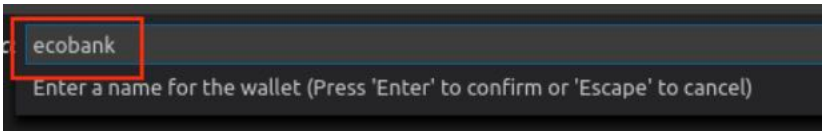
__ **11.** Back in VS Code, hover the mouse over the '**+**' sign in the Fabric Wallets panel and click **Add Wallet.**



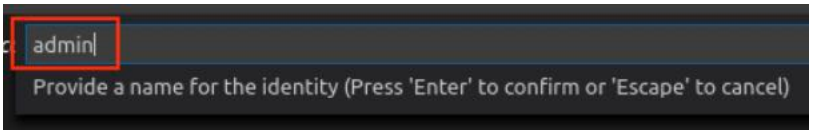
__ **12.** At the top of the screen click the option to **Create a new wallet and add an identity**



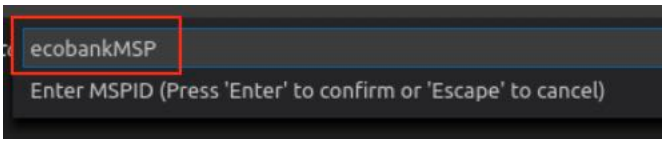
__ **13.** Specify **ecobank** as the name of the wallet (it is important to name this exactly with all lowercase letters)



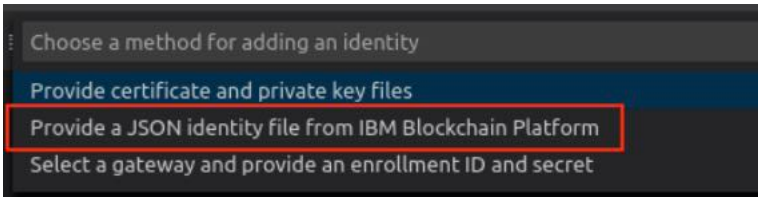
__ **14.** Specify **admin** as the name of the identity



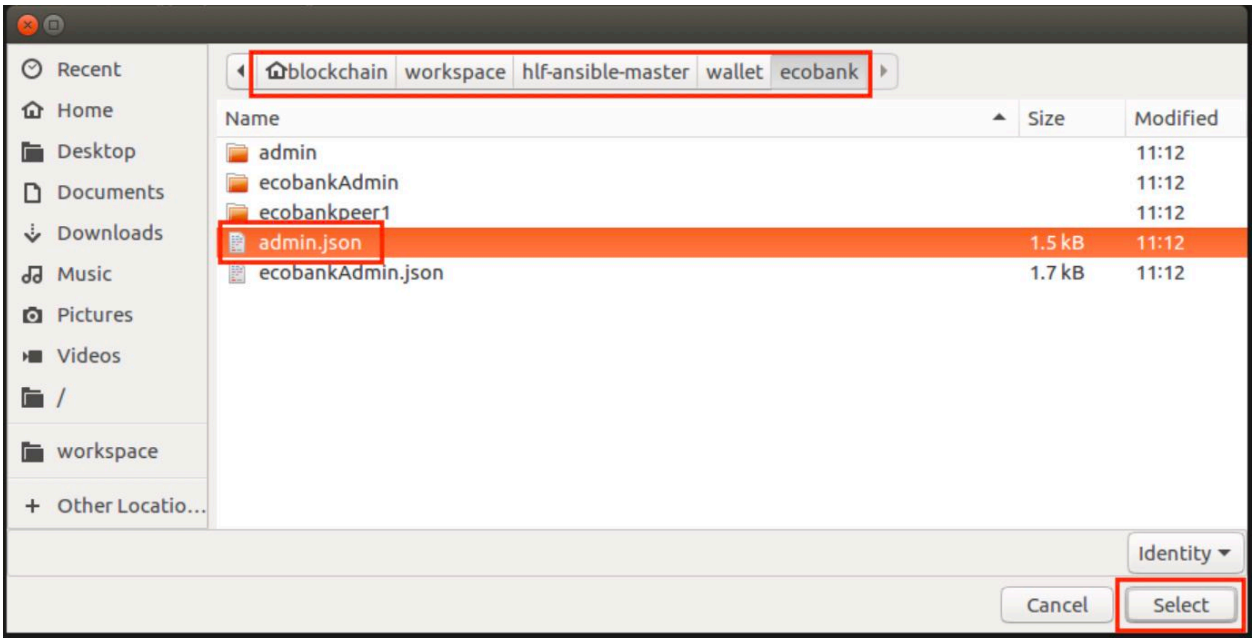
__ **15.** Specify **ecobankMSP** as the MSPID



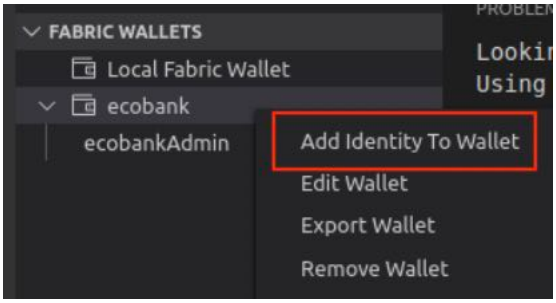
__ **16.** Select the option to Provide a JSON identity from IBM Blockchain Platform



__ **17.** Click **Browse** and then navigate to the location:
"Home" > workspace > hlf-ansible-master > wallet > ecobank
Click the file **admin.json** to highlight it, then click **Select**

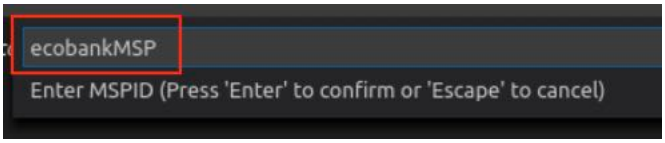


__ **18.** Right click the ecobank wallet icon on the **ecobank** wallet to add another identity

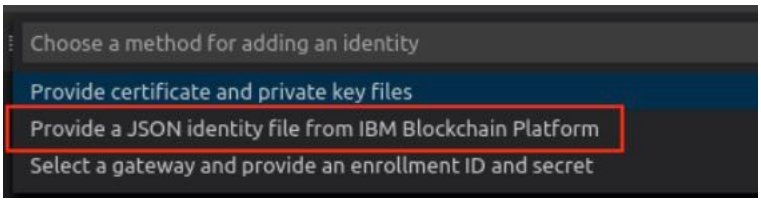


__ **19.** Specify **ecobankAdmin** as the identity name and press enter

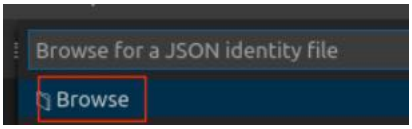
__ **20.** Specify **ecobankMSP** as the MSPID

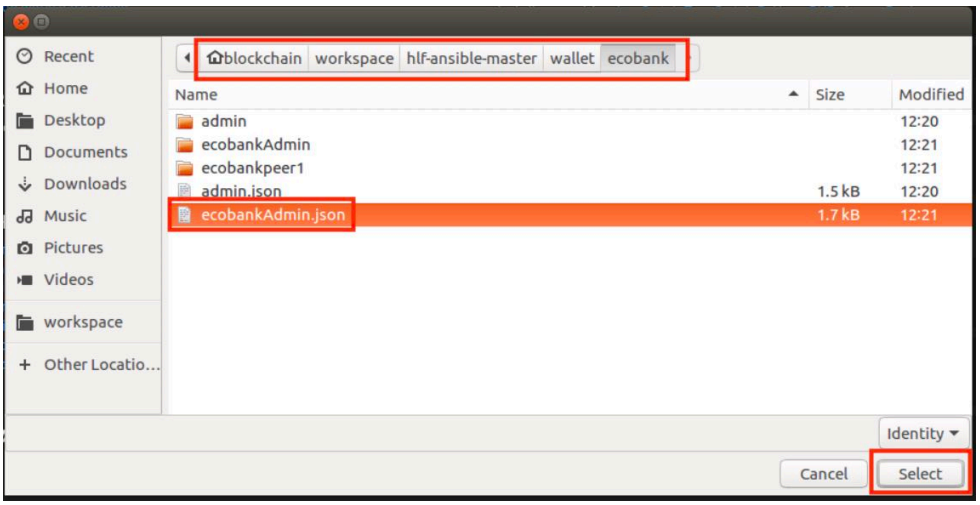


__ **21.** Select the option to Provide a JSON identity from IBM Blockchain Platform

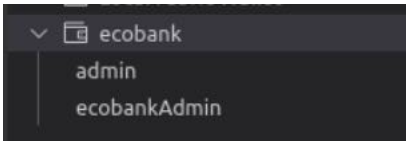


__ **22.** Click **Browse** and then navigate to the location:
"Home" > workspace > hlf-ansible-master > wallet > ecobank
Click the file **ecobankAdmin.json** to highlight it, then click **select**





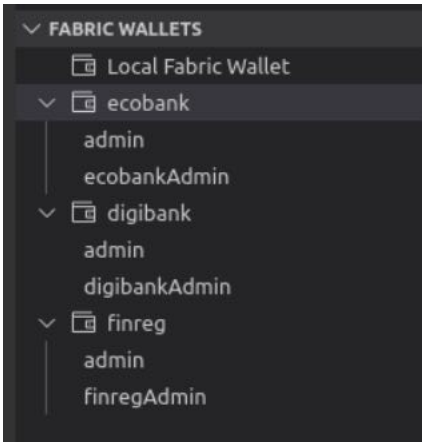
The newly created wallet and two imported identities will be shown in the Fabric Wallets panel:



__ **23.** Using Steps *12 – 23* as a guide create a wallet called **digibank** and import the IDs **admin** and **digibankAdmin** . The MSPID will be **digibankMSP**. Similar to the other wallet, remember to be exact with the names used. The folder to browse for the JSON file will be:
"Home" > workspace > hlf-ansible-master > wallet > digibank

__ **24.** Using Steps *12 – 23* as a guide create a third wallet called **finreg** and import the IDs **admin** and **finregAdmin** . The MSPID will be **finregMSP**. Similar to the other wallets, remember to be exact with the names used. The folder to browse for the JSON file will be:
"Home" > workspace > hlf-ansible-master > wallet > finreg

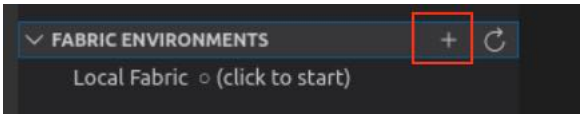
When all the wallets are created and the identities imported, they will display as follows:



The wallets are now created, and the identities imported.
In order to install and instantiate smart contracts it is necessary to create ***Fabric Environments*** for each of the 3 main organisations in the consortium.

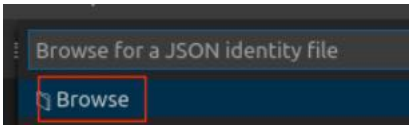
We will first create the Fabric Environment for EcoBank.

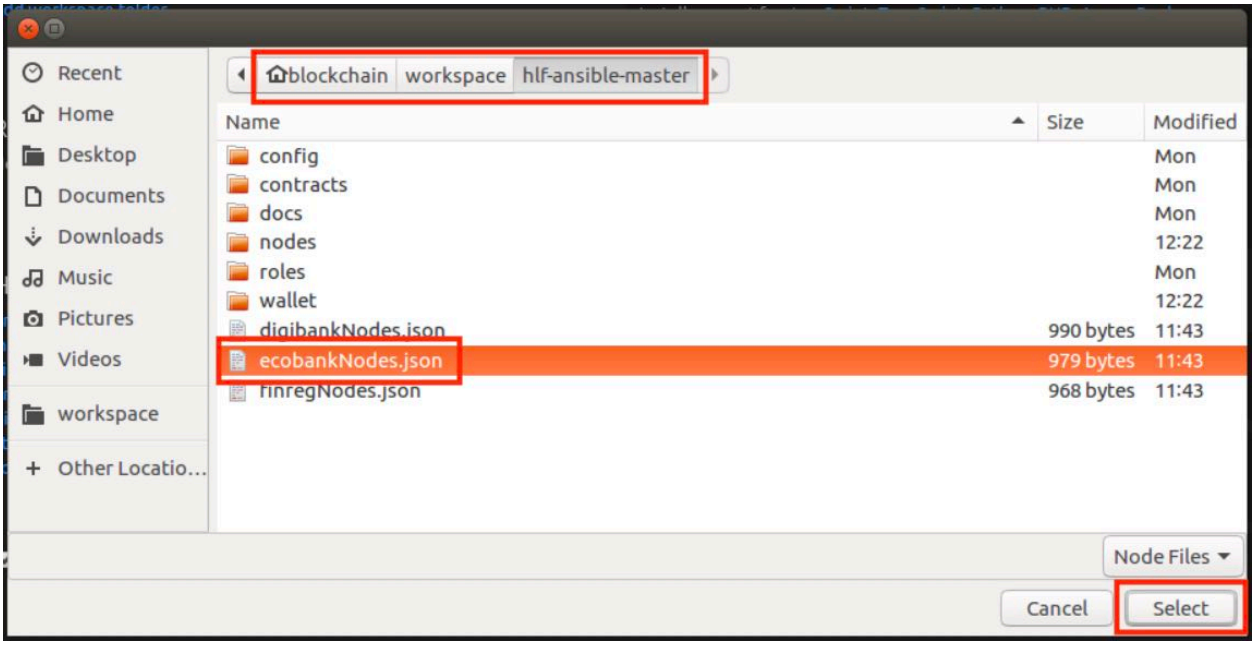
__ **25.** Import "Nodes" file to create a Fabric Environment for EcoBank.
On the Fabric Environments Panel click the '+' icon to add a new environment.



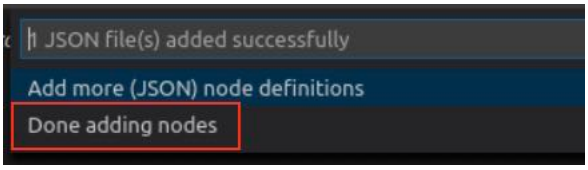
__ **26.** At the top of the screen type **ecobank** as the name of the new environment and press enter.

__ **27.** Click **Browse** and then navigate to the location:
"Home" > workspace > hlf-ansible-master
Click to highlight **ecobankNodes.json** click **Select**



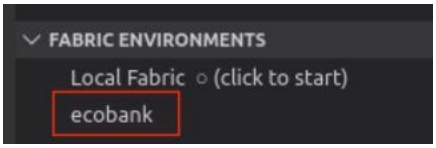


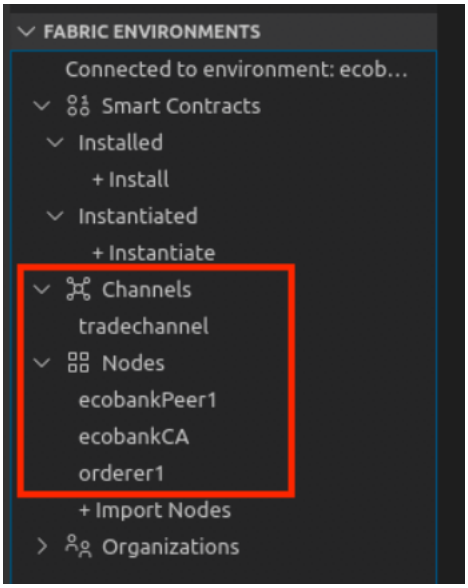
__ **28.** The JSON file you selected contains definitions for Peer, Certificate Authority and Orderer, so there are no more files to import for EcoBank. At the top of the screen 1 file is shown as imported – click **Done adding nodes**



Note: The imported Node file included the name of the wallet and the identity to use, so when clicking this environment it will connect immediately.

__ **29.** Click on the newly created **ecobank** environment to check that it connects as expected, and expand the **Channels** and **Nodes** twisties.





__ **30.** Hover over the Fabric Environments panel, and click the icon to disconnect from the Ecobank environment

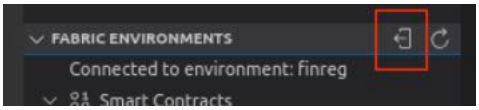
__ **31.** Using steps 25 – 30 as a guide, create a Fabric Environment for **digibank** using the file "Home" > workspace > hlf-ansible-master > **digibankNodes.json**.

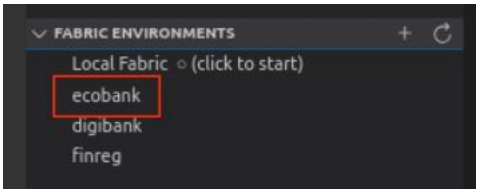
__ **32.** Again, using steps 25 – 30 as a guide, create a Fabric Environment for **finreg** using the file "Home" > workspace > hlf-ansible-master > **finregNodes.json**.

These environments will now be used to create additional (non-administrator) IDs to allow more realistic testing of the smart contract. These IDs are
Eva for EcoBank
David for DigiBank and
Fran for FinReg

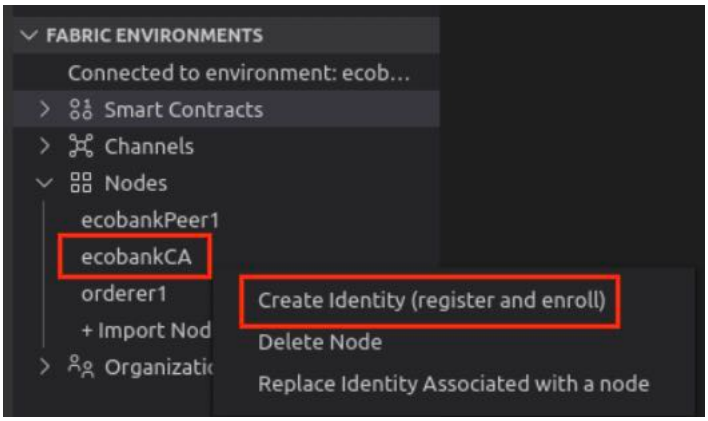
We will start by creating the ID for Eva.

__ **33.** Disconnect from any connected Fabric Environment and click on **ecobank** to connect to the EcoBank environment.



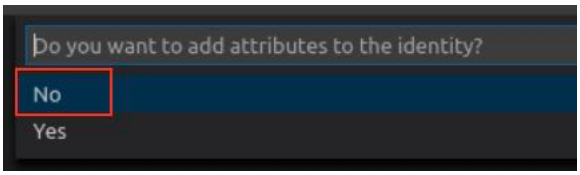


__ **34.** Expand the **Nodes**, right-click on the **ecobankCA** and then click **Create Identity (register and enrol)**

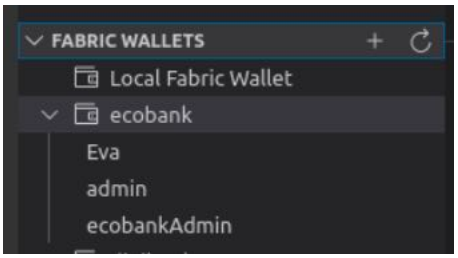


__ **35.** Specify **Eva** as the identity

__ **36.** There are no attributes required for this lab – click **No**



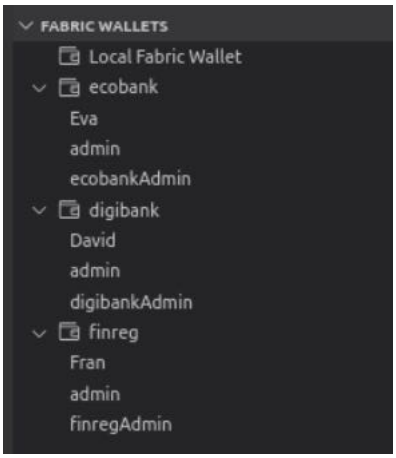
The Identity **Eva** has been added to the **ecobank** wallet



__ **37.** Using steps *33* – *36* as a guide, connect to the **digibank** environment and Create and Identity **David**

__ **38.** Using steps *33 – 36* as a guide, connect to the **finreg** environment and Create and Identity **Fran**

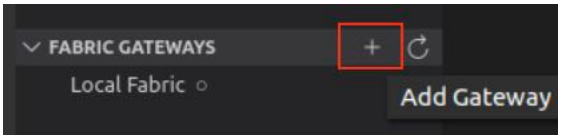
The complete list of wallets and identities for the 3 organisations is shown below



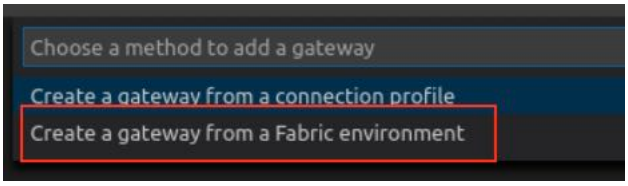
The identities we have just created will connect to the network using ***Gateways***.

We'll first add the gateway for Ecobank.

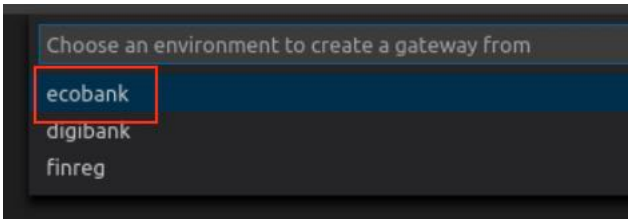
__ **39.** Add the Gateway for **ecobank**
Hover over Fabric Gateways and click the '+' to add a gateway



__ **40.** The simplest way to create a Gateway is to base the definition on an existing Environment. Click **Create a gateway from a Fabric environment**

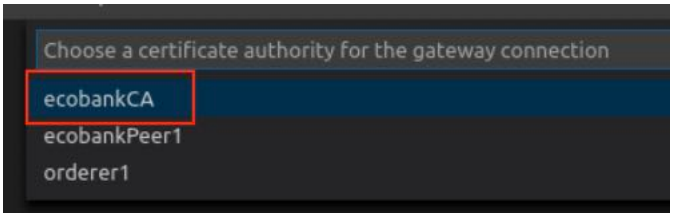


__ **41.** Click **ecobank** as the environment to copy from

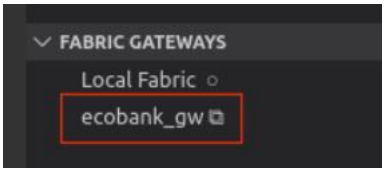


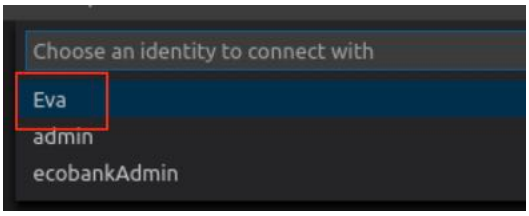
__ **42.** Use the suggested name **ecobank_gw** and press **enter**

__ **43.** **Click** the **ecobankCA** as the certificate authority

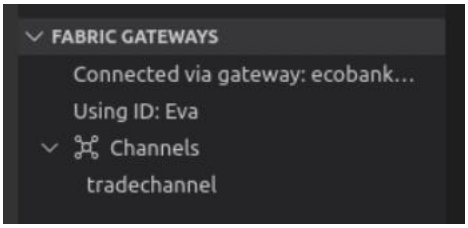


__ **44.** **Click** on the new gateway **ecobank_gw** and choose **Eva** as the identity to connect with

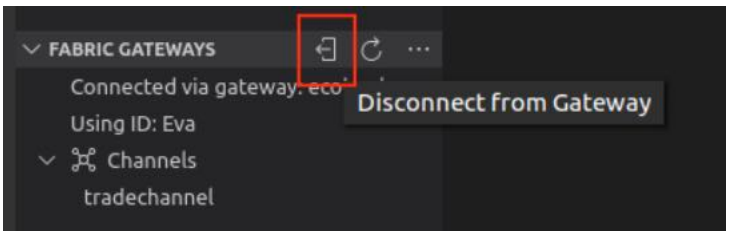




__ **45.** Verify that Eva can see the **tradechannel**



__ **46.** Hover over the Fabric Gateways panel and **click** the **Disconnect** icon to disconnect from the gateway



__ **47.** Using steps *39 – 46* as a guide, add a **digibank** gateway called **digibank_gw** and connect with the identity **David.** Verify that David can see the tradechannel channel.

__ **48.** Using steps *39 – 46* as a guide, add a **finreg** gateway called **finreg_gw** and connect with the identity **Fran**. Verify that Fran can see the tradechannel channel.

Review

In this section you have:

- Used a playbook (site.yml) to create a network
- Created wallets and imported administrative users
- Created environment definitions that allowed the administrators to aperate the network
- Created additional non-administrative users for more realistic testing
- Created gateway definitions that allowed the non-administrative user IDs to be used to test transactions when the smart contract was deployed.

2 Deploy the first version of the Smart Contract to test & prove the Trade Network

The network has been created and a first version of the smart contract can be deployed and tested. The process is to package the Smart Contract, then install it on peers in the network, and finally instantiate it once on the channel. The instantiation step takes a few moments to build the new chaincode container.

The smart contract contains code that handles private data, something which was introduced to Hyperledger Fabric as far back as version1.2. It was introduced to enable organisations to keep data private from other organisations on a channel, whether as one organisation or in a private arrangement with another organisation. This functionality was designed, among other things, to prevent the need to create a separate channel to achieve the same end.

Let's briefly describe two key entities essential to understanding Fabric Private Data:

The first is a **Private Data collection** – the second, is a **Private Data collection definition file**. **Private Data collections** allow an organisation – or a subset of organizations on a channel - the ability to endorse, commit, or query private data without having to create a separate channel. Collections consist of **private data** sent peer-to-peer to only the organisations entitled to see it (by policy, defined in a collection definition file) – and – a **hash of the data** is also endorsed, ordered, and written to the ledgers of every peer on the channel. The hash serves as evidence of the transaction, i.e. for state validation or audit/compliance purposes.

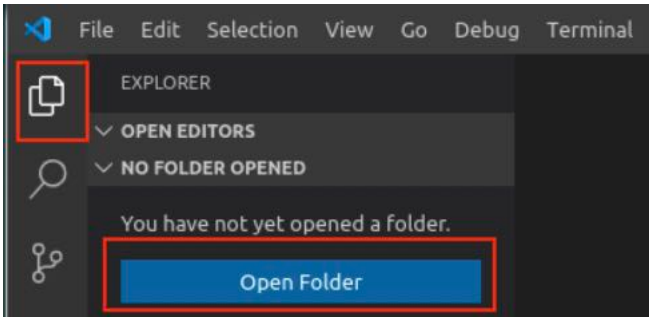
The second is **Private Data collection definition files**. These are policy-based definitions that describe which organisation(s) belong to a Private Data collection – it could be one, two or more organisations (as policy dictates), that govern who can access private data in a given collection, on a channel. It is commonplace for the definition file to contains one or more collections (each has a name and the participating organisations in that stanza), as well as properties used to control dissemination of private data at endorsement time and, optionally, whether the data will be purged / its longevity. The collection definition then gets deployed to the channel, supplied as a policy file when instantiating/upgrading the chaincode package.

When instantiating this smart contract you will be supplying the definition of the Private Data Collections.

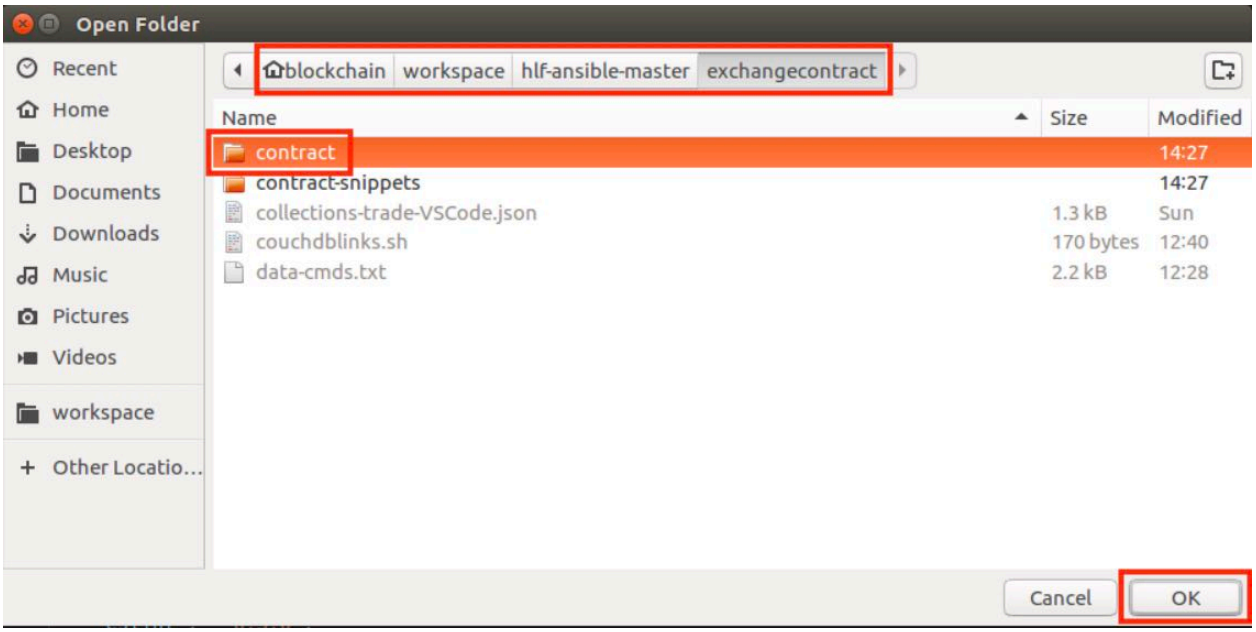
The definition file for this lab is shown below:

Complete details of the syntax and meaning of all the fields is available in the Fabric Documentation, but note that the two Collections defined in this lab exercise have collection names of **CollectionD** for Digibank and **CollectionE** for Ecobank. (The "Policy" section in the JSON file is the same format as that used for Endorsement Policies)

__ **49.** Click the Explorer icon in VS Code and **Open Folder**

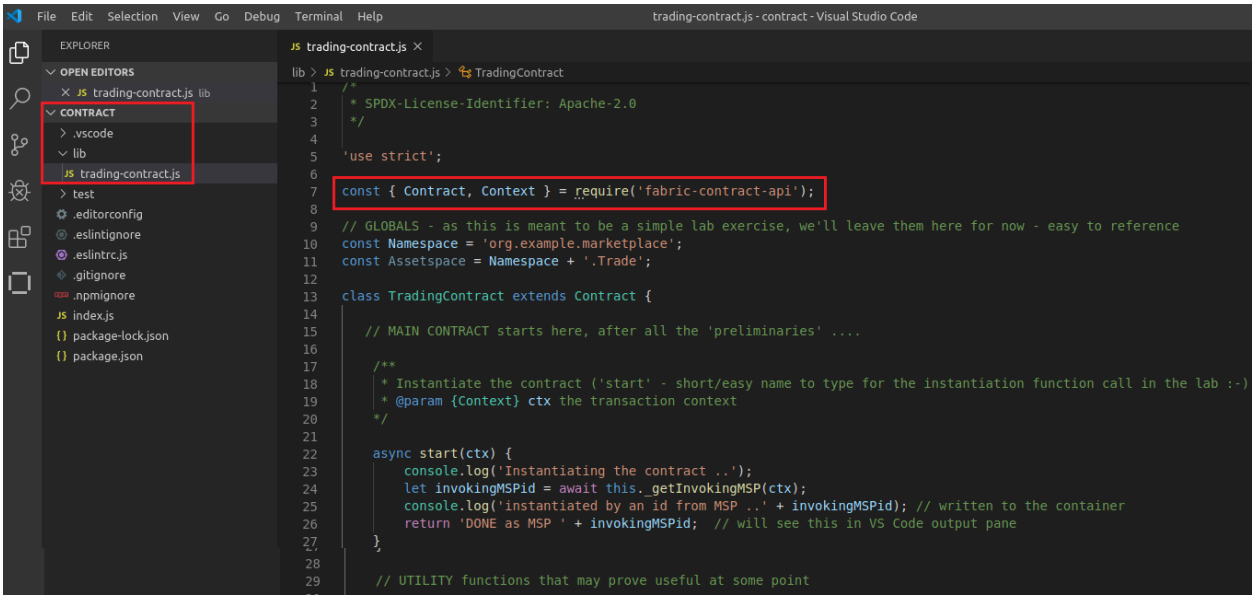


Navigate to the location:
"Home" > workspace > hlf-ansible-master > exchangecontract
Click to highlight the **contract** folder and click **OK**

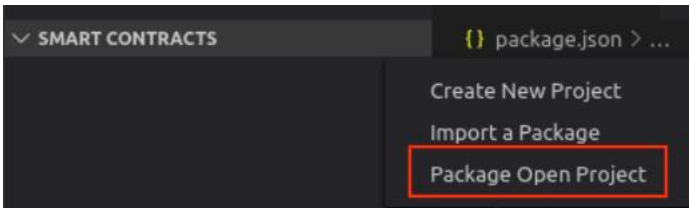


__ **50.** VS Code will display the **Contract folder** tree. Expand the twisty for the **lib** folder and click **trading-contract.js** to view it.

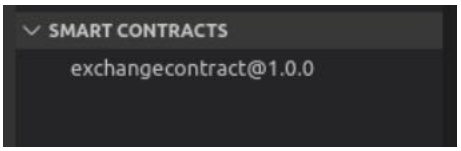
Note 1: Notice the location of the source 'trading-contract.js' base contract under 'lib' in Explorer - you will need it later to add additional transactions.
Note 2: This Smart Contract includes the Fabric new programming model Contract API. (`fabric-contract-api`)



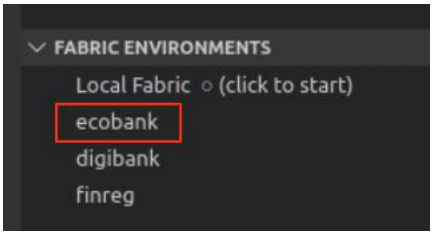
__ **51.** Click the icon  to return to the IBM Blockchain Platform extension, hover over the and under **Smart Contracts** panel, click the Ellipses icon to select “More actions” and then select **Package Open Project**



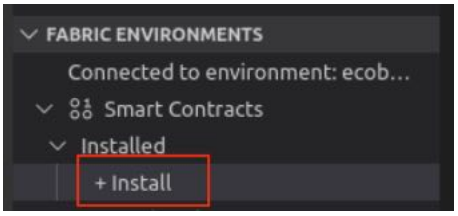
This will cause the smart contract you just imported to be packaged into a CDS file that can be installed on a peer. The package will then appear in the Smart Contracts list.



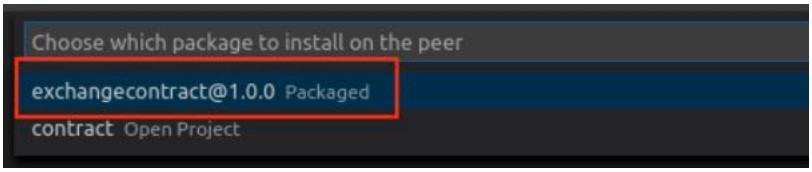
__ **52.** On the Fabric Environments panel click on **ecobank** to connect to the Ecobank environment:

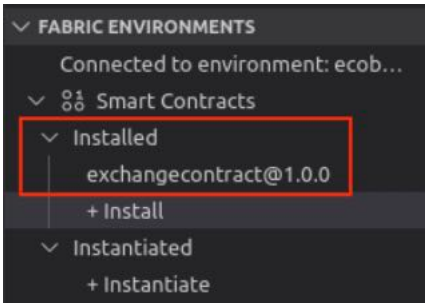


__ **53.** Click **+Install** to install a contract on the peer



Select **exchangecontract@1.0.0** The contract will appear under the installed list

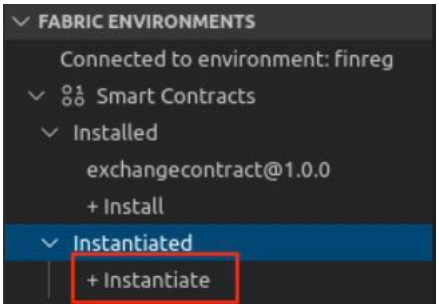


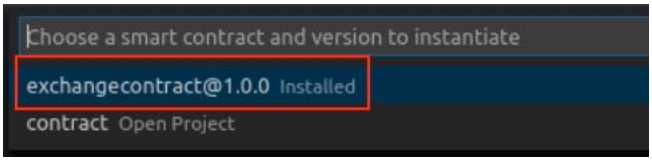


__ **54.** Disconnect from the Ecobank Fabric Environment, and using Steps *52 -53* as a guide, install the same smart contract in the **digibank** environment.

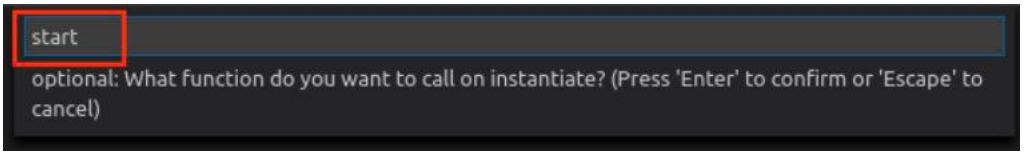
__ **55.** Disconnect from the Digibank Fabric Environment, and using Steps *52 -53* as a guide, install the same smart contract in the **finreg** environment.

__ **56.** While still connected to the finreg environment, click **+Instantiate** to instantiate the contract on the finreg peer, and select **exchangecontract@1.0.0**

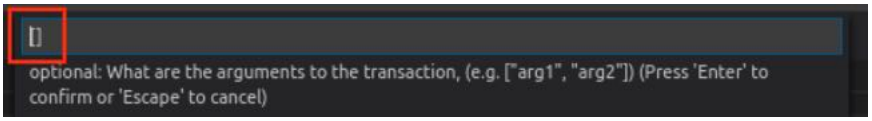




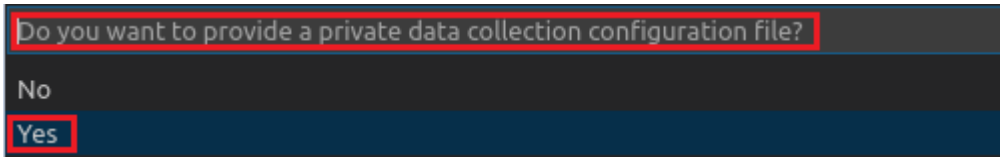
__ **57.** Specify **start** as the function to be used with instantiate



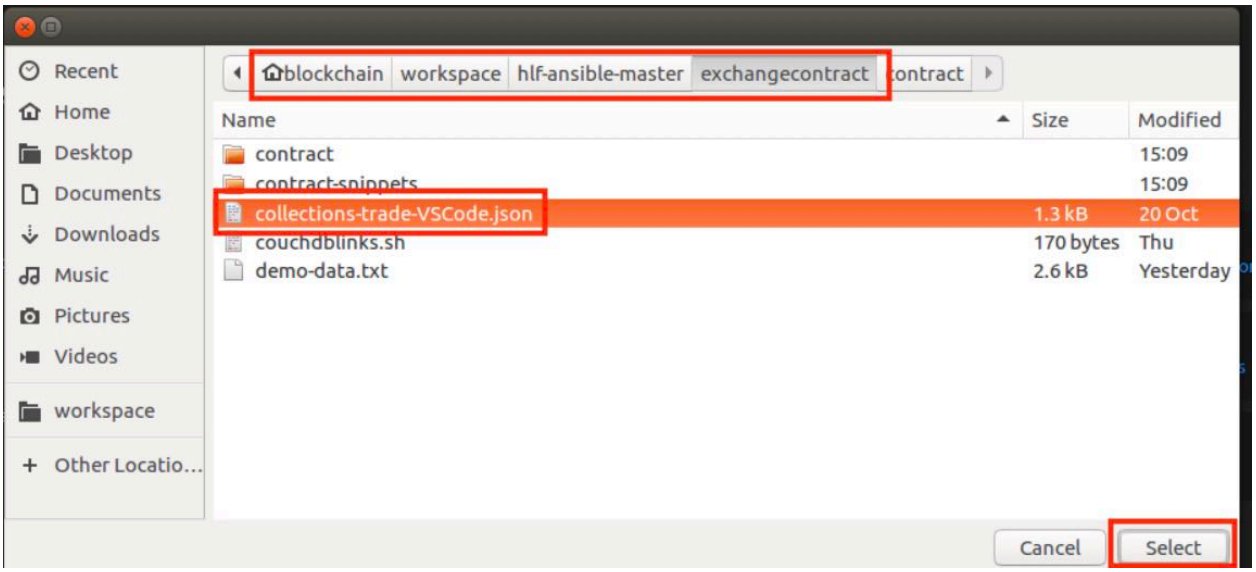
__ **58.** There are no parameters to pass to the start function – just press **enter** with the default empty array **[]**



__ **59.** When asked if you 'want to provide a private data collection configuration file?' – select **Yes**

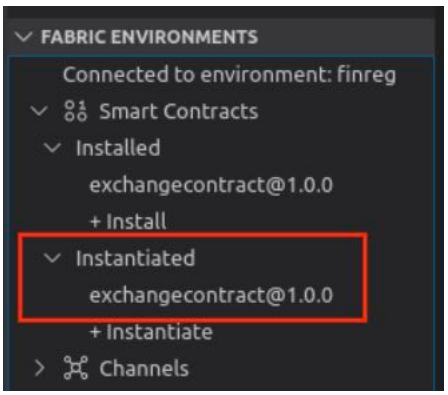


__ **60.** Click **Browse** and navigate to the folder:
"Home" > workspace > hlf-ansible-master > exchangecontract
and select the file **collections-trade-VSCode.json**.



This will take a minute or so to complete.

When the contract is instantiated it will show as follows



The smart contract has been instantiated on the **tradechannel** channel.

This is the end of Part 2 of the Lab.

Review

In this part of the Lab you have:

- Packaged the base contract
- Installed the base contract on peers for the 3 organisations
- Instantiated the Smart Contract on the FinReg peer (starting a chaincode container)
- Instantiated the Smart Contract with the definition of the Private Data Collections

3 Private Data for the Offer and Accept Transactions

INTRODUCTION

In this section, we will focus on the logic for the **offer** and **accept** transactions in our private data scenario. We will additionally us an **advertise** transaction which will allow a commodities contract to be offered for sale on the blockchain network.

Part 3 of the lab is to execute these transactions so that we create records in both the channel ledger and most importantly in the private data collections. After an initial **advertize** function is executed, the next sequence is to invoke the new **offer / accept** functions – these are executed by identities from:

- DigiBank (the **buyer**, making the offer) and
- Ecobank (the **seller**, who chooses what offer to accept)

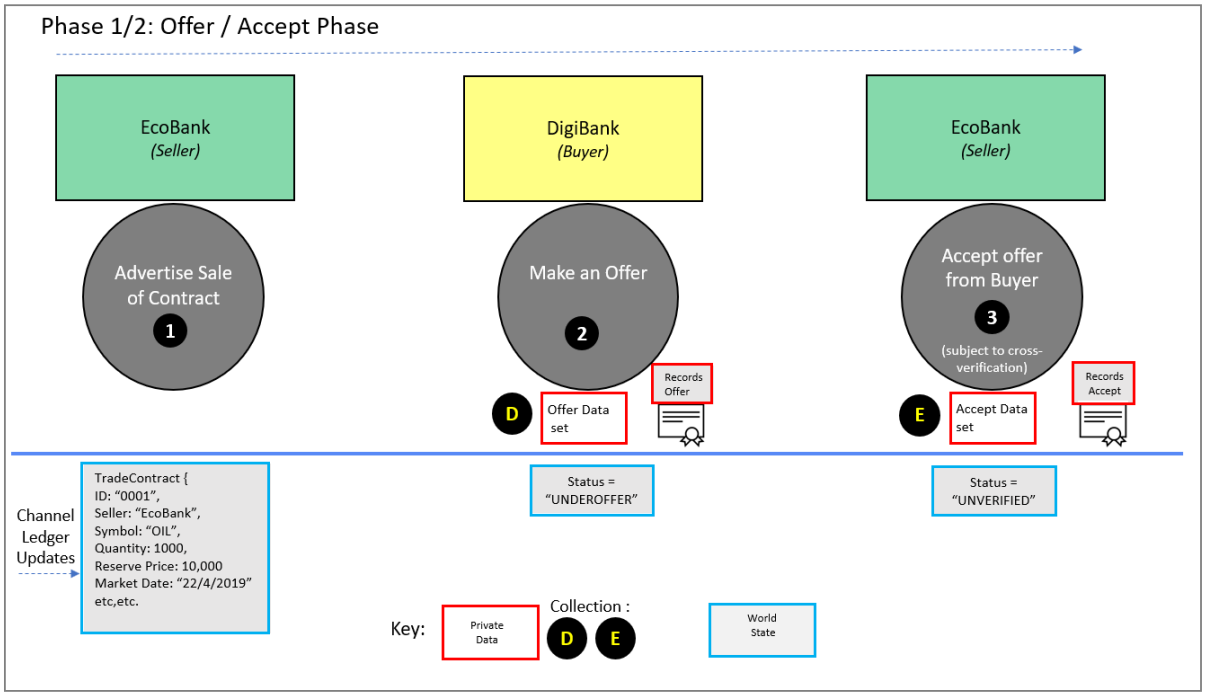
Both the offer and the accept transactions generate a request and create a private data record for the invoking identities' organisation. Note that the functions will also update the channel ledger with 'public' data like 'status' or 'date'. Later on, the offer / accept pattern will need to undergo a 'cross-verification' process – that will be done in Part 4.

For a complete list of the function names, their objectives and a brief description of each, please see the Appendix.

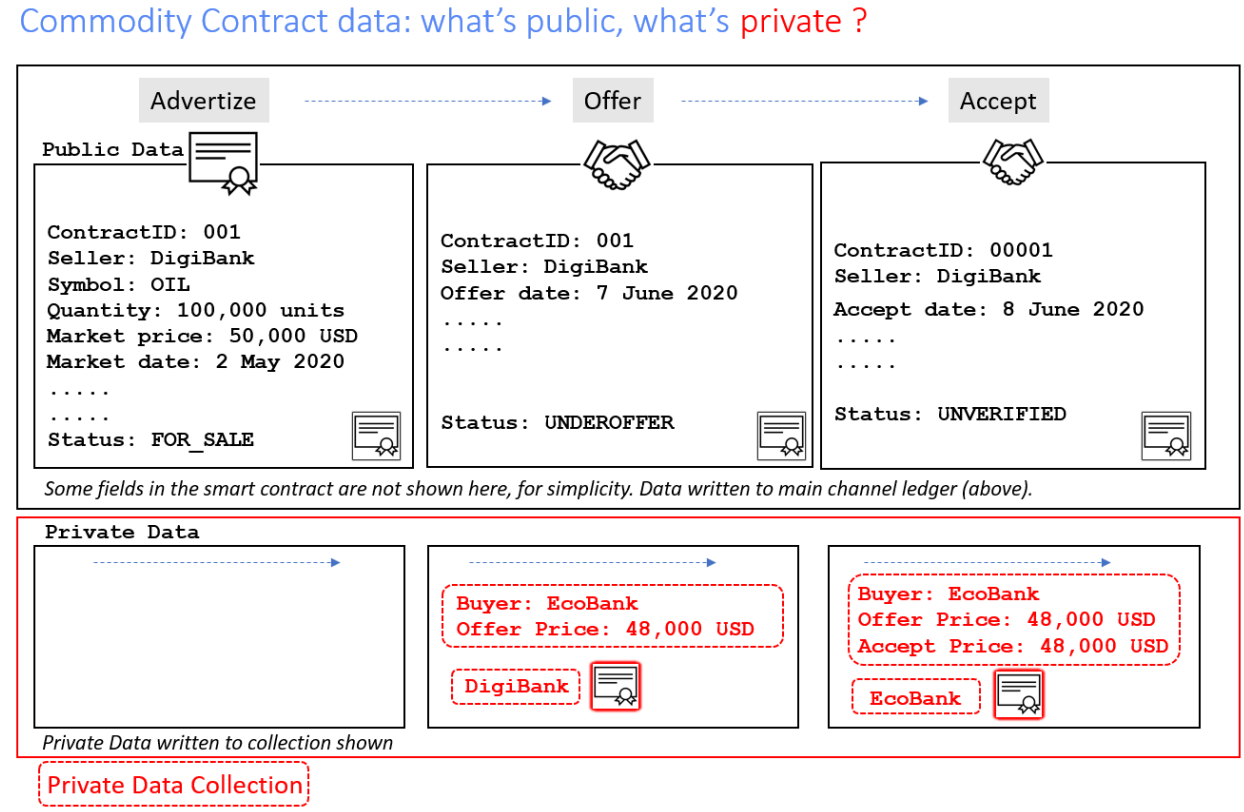
In the offer/accept phase of the scenario the following transactions occur:

1. Seller **EcoBank** *advertises* the nominal sale price / info on the marketplace and it is recorded on the blockchain - this is written to the ledger and all would-be buyers get notified (via applications, out-of-band).
2. Buyer **DigiBank**, makes an *offer* to buy the contract – it formalises this offer by generating an offer request. The offer price is confidential, and so is written to its (DigiBank's) own private data store (i.e. one organisation in the collection) and shared only with Ecobank via an out-of-band application. Its status is 'UNDEROFFER' on the ledger (world state).
3. **EcoBank** who received the offer price out-of band – *accepts* the offer. It generates an accept approval request and it stores this in its own Private Data collection (one organisation). Its status (written to the channel ledger state) at this time is now set to 'UNVERIFIED'.

Verify Pattern



The private data – and the 'public' (channel ledger) data being recorded, is best captured in the diagram below:



Offer / Accept Phase – Introduction

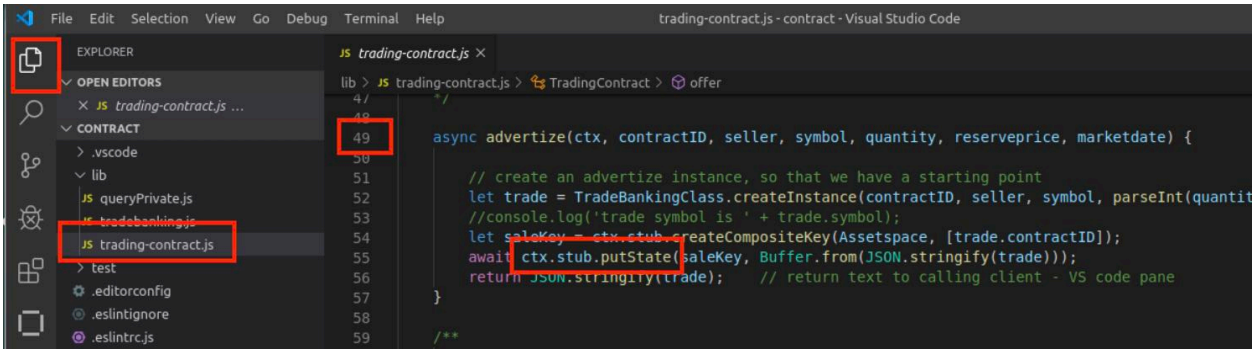
The first task is to examine the offer and accept transactions mentioned earlier. These are the main transactions that were added in the base contract, along with two helper methods called **readOffer** and **readAccept** which can be used to verify data written to private data collections (in the lab).

Input to the **offer** and **accept** transactions are passed as 'transient data'; in the VS Code extension you're prompted to provide this. Transient data is not persisted in the transaction that is stored on the channel ledger; this keeps the data confidential. Transient data is passed as binary data and then decoded and written to the local private data store.

Note: It is good and common practise to 'salt' this transient data with a random element, especially if it contains more predictable private data. See the appendix 'Access Control and Salting of Private Data' for more information.

Let's briefly explore the functions starting with **advertize**.

__ **61.** Click the **Explorer** icon, and open the **trading-contract.js** from the folder view and find the **advertize** function at **line 49**.



The **advertize** transaction creates a saleable Commodity contract (identified by a contract ID) on the channel ledger which is traded on the marketplace. This uses the Fabric **putState() API** that writes state information to the ledger. This transaction function is called by someone from EcoBank (the seller).

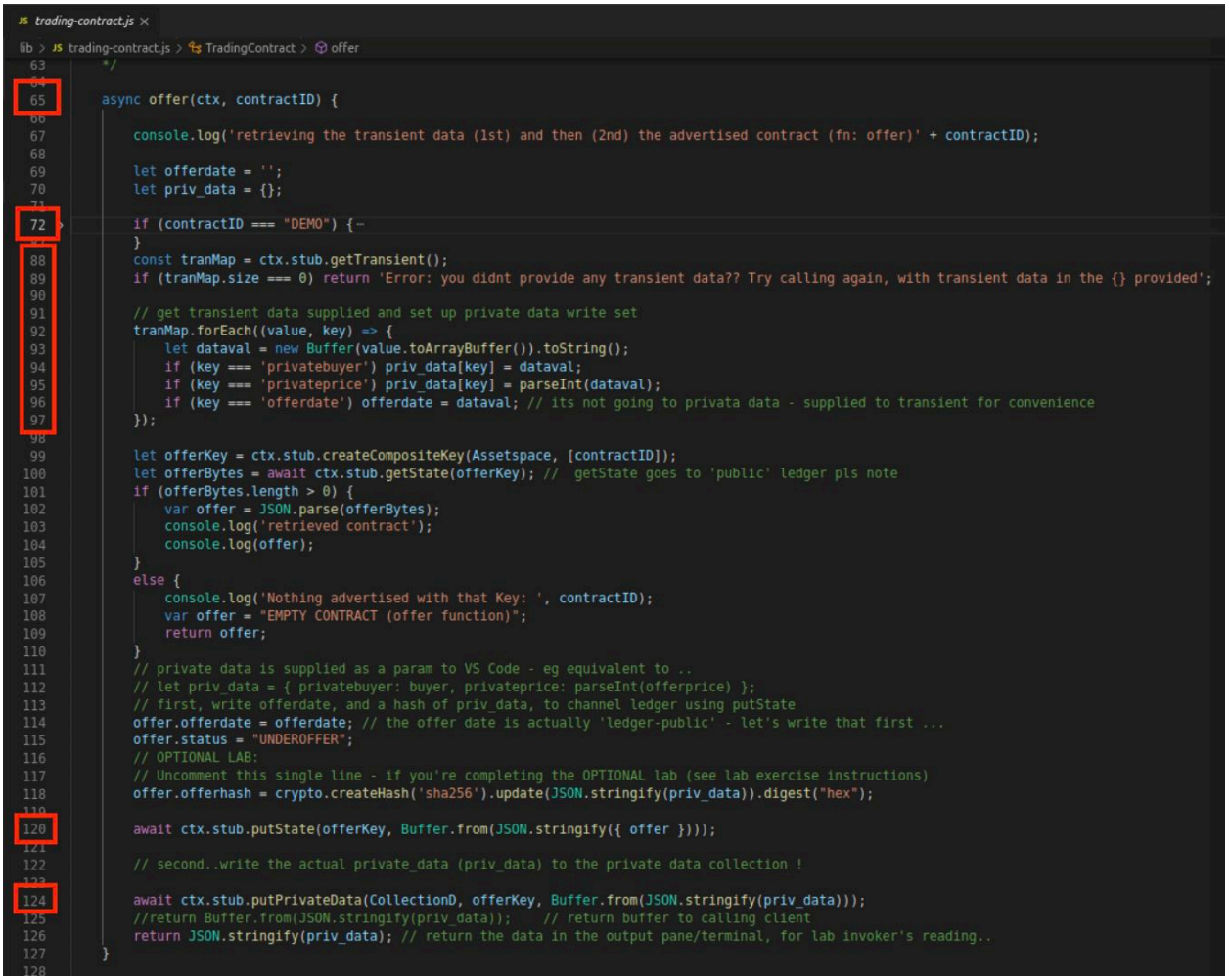
__ **62.** Scroll to the **offer** transaction at **line 65.**

You can ignore the “DEMO” clause between lines 72 to 87, which can be used to create sample data.

The offer transaction takes a contract ID as a parameter and reads in the ‘transient data’ as private data - supplied when the transaction is invoked from the VS Code extension or a client app. Transient data is passed as binary data and then decoded in the function starting with the **getTransient** method.

Lines 88-97 show the private data elements being committed to DigiBank’s private collection using the chaincode API **PutPrivateData()** in **line 124**

Line 120 causes the non-confidential data to be written to the main ledger using **putState()** – data like ‘Status’ or an ‘Offer Date’ – which is intentionally visible to others on the channel.



__ **63.** Scroll to the implementation of the **accept** transaction at **Line 157**
The accept method has the same format as the offer function, decoding the transient data **(lines 179-190)** then writing Private Data at **line 212** and writing main channel data at **line 208**.

The **accept** transaction represents an accepting party (EcoBank, the seller) completing the sale, by accepting an offer – in this scenario from DigiBank. Similar to the **offer** transaction, it also writes private data – but this time to EcoBank's own private collection. It writes an accept price privatelyin addition to the, as well as the offer data set that was agreed with DigiBank. It also makes use of **putPrivateData()** to write confidential data and **putState()** to update the main channel ledger with non-confidential data as before.

__ **64.** Review the additional helper functions in the contract:
The read-only transaction **readOffer** is a helper function, to enable you to verify what was written to private data earlier.
The read-only transaction **readAccept** is a helper function, to enable the seller identity, to verify what was written in the to the private collection, when created in the 'accept' call earlier.
The remaining functions in the smart contract - like **_getInvokingMSP** are utility functions, used invariably by the main transaction functions.

3.1 Invoking the Offer and Accept transactions

At this point we can now go and create some private data on each of the collections we are using.

However, we will first launch the CouchDB web interface for each organisation into a separate Firefox tab which will enable us to view the data in the tradechannel world state, and the private collections.

Note also that some of the parameter lists that you need to 'paste' into VS Code (to complete a task), can be copied and pasted from the file **demo-data.txt** which is located under the **workspace/hlf-ansible-master/exchangecontract** folder.

__ **65.** From a terminal window, use the following two commands to navigate to the **exchangecontract** folder and launch CouchDB sessions in Firefox using a bash script:

```
cd ~/workspace/hlf-ansible-master/exchangecontract

./couchdblinks.sh
```

```
blockchain@ubuntu:~/workspace/hlf-ansible-master$
blockchain@ubuntu:~/workspace/hlf-ansible-master$ cd ~/workspace/hlf-ansible-master/exchangecontract
blockchain@ubuntu:~/workspace/hlf-ansible-master/exchangecontract$ ./couchdblinks.sh
starting Firefox with tabs for CouchDB utils
blockchain@ubuntu:~/workspace/hlf-ansible-master/exchangecontract$
```

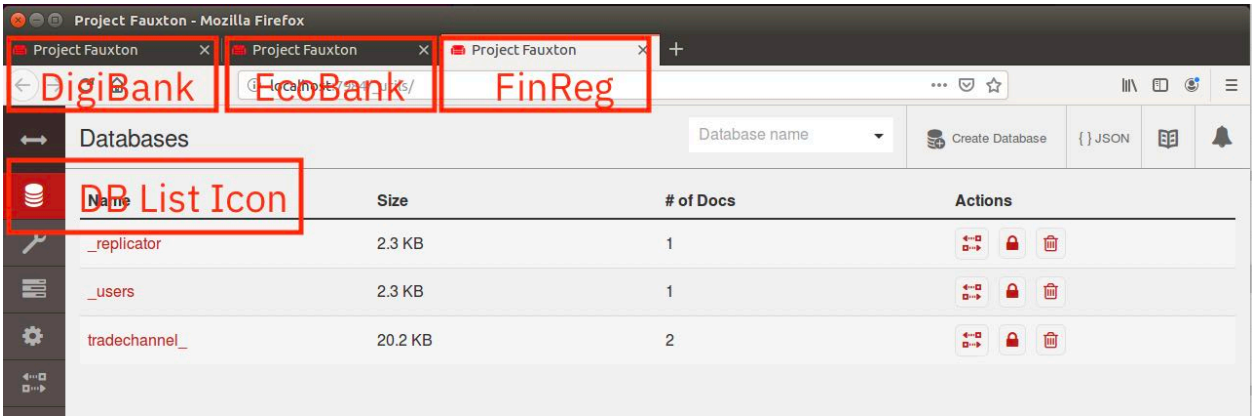
When the script is complete you should see a Firefox browser window with three tabs displayed. Note that the script may take a couple of minutes to complete, and there will be a pause between tabs opening.

Note: If the tabs have not opened after three minutes close the firefox window and re-run the command.

Each tab represents the view for a different organization:

- Digibank is displayed on localhost:6984/_utils
- EcoBank is displayed on localhost:5984/_utils
- Finreg is displayed on localhost:7984/_utils

Note: In a production scenario direct access to the CoucbDB Web interface would be blocked for security, but it is useful during development and testing.



In the steps in this section of the lab, some of the parameters are quite long. There is a text file available to make the copy and paste of the parameters easier.

__ **66.** From the terminal window issue the command to open the text file in gedit

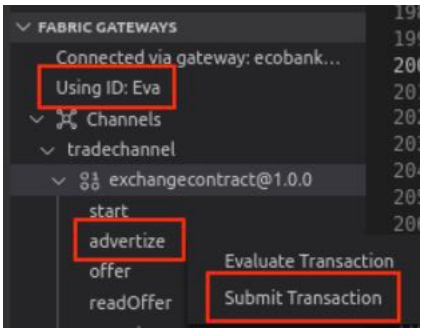
```
gedit demo-data.txt &
```

```
blockchain@ubuntu:~/workspace/hlf-ansible-master/exchangecontract$ gedit demo-data.txt &
```

You can copy and paste from this text file in the steps that follow.

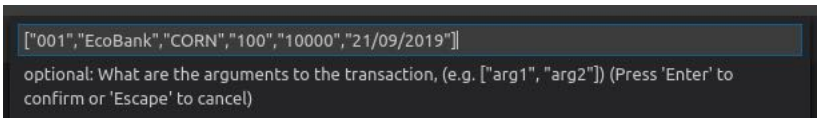
__ **67.** Switch back to the IBM Blockchain Platform VS Code extension, and in the Fabric Gateways panel click **ecobank_gw** and connect it using the identity **Eva**

__ **68.** Expand Channels and tradechannel and then right click the **advertize** transaction and click **Submit transaction**.



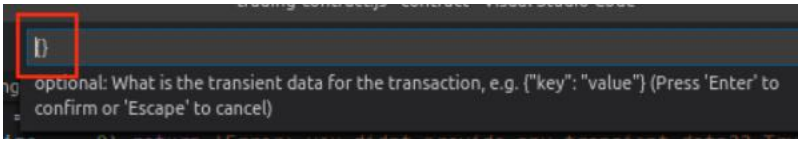
__ **69.** Next, enter the following parameters for arguments when prompted – overwrite the '[]' brackets offered in the prompt

["001","EcoBank","CORN","100","10000","21/09/2019"]



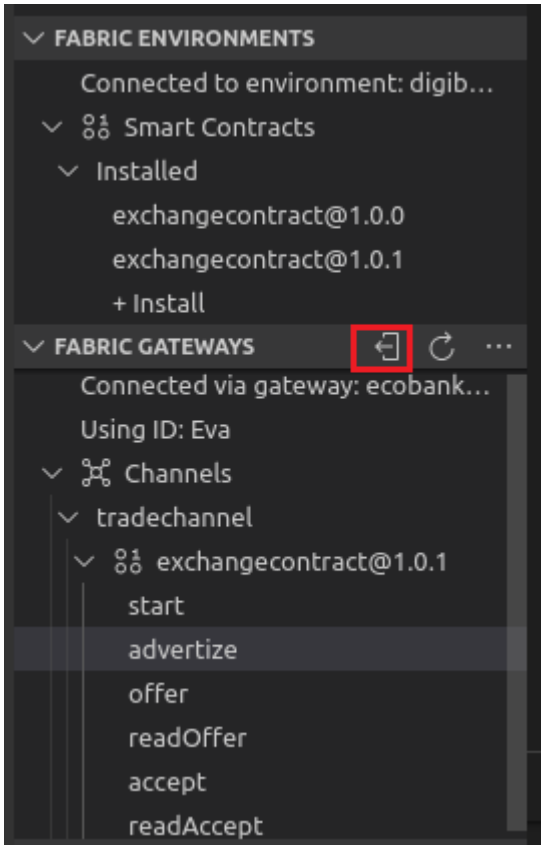
As you will recall from the advertise() implementation, the parameters represent the contract ID, seller, symbol, quantity, reserve price and market date respectively.

__ **70.** There is no transient data for this function, just press **enter** leaving the empty curly braces **{}**



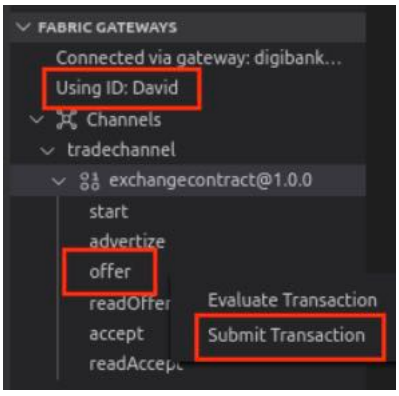
the transaction will now be submitted, and should return with a SUCCESS message

__ **71.** Next, we will make an offer for the advertised commodity with a Contract ID of "001" – to do this, we must first disconnect from the EcoBank gateway – **click** on the **disconnect** icon



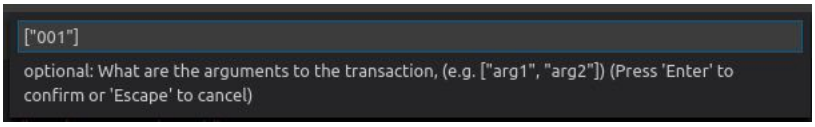
__ **72.** Next, click on the DigiBank gateway (**digibank_gw**) – when prompted, select **David** as the identity

__ **73.** Right-click on the **offer** transaction and click **Submit Transaction**



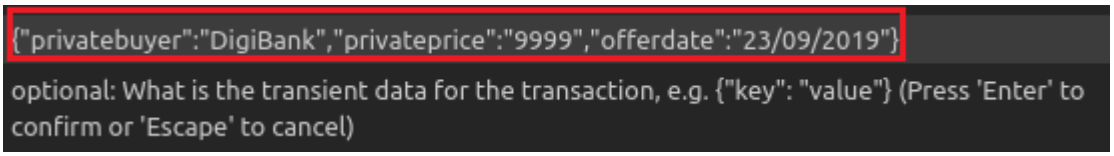
__ **74.** When prompted for arguments, enter the following parameter (overwriting any existing '[]' data) – and press **enter**

["001"]



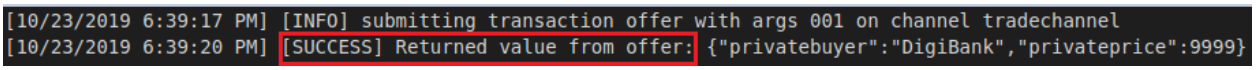
__ **75.** Next, you will be asked to supply 'transient data'. Our private offer is confidential and so we want to use this field to supply this information so that it is not captured on the ledger. Enter or paste the following overwriting the '{}' text presented – **notice that it is wrapped in curly brackets this time!**

{"privatebuyer":"DigiBank","privateprice":"9999","offerdate":"23/09/2019"}



__ **76.** Check the output pane at the bottom for a SUCCESS message confirming that the offer data was submitted successfully.

Note: We are logging the private information to the console for debug and demo purposes – you would not do this in a live application!

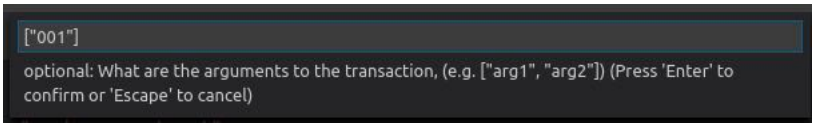


To verify what was written to the private data collection, we have a helper function called **readOffer** which we can call, and verify the collection returns us the data that was written earlier.

__ **77.** Right-click on transaction **readOffer** and click **Evaluate Transaction**

__ **78.** When prompted for parameters, enter the following:

["001"]



__ **79.** There is no transient data for this function, just press **enter** leaving the empty curly braces **{}**

The transaction will now be submitted, and should return with a SUCCESS message

```
[10/31/2019 9:42:46 AM] [INFO] evaluateTransaction
[10/31/2019 9:43:04 AM] [INFO] evaluating transaction readOffer with args 001 on channel tradechannel
[10/31/2019 9:43:04 AM] [SUCCESS] Returned value from readOffer: {"privatebuyer":"DigiBank","privateprice":9999}
```

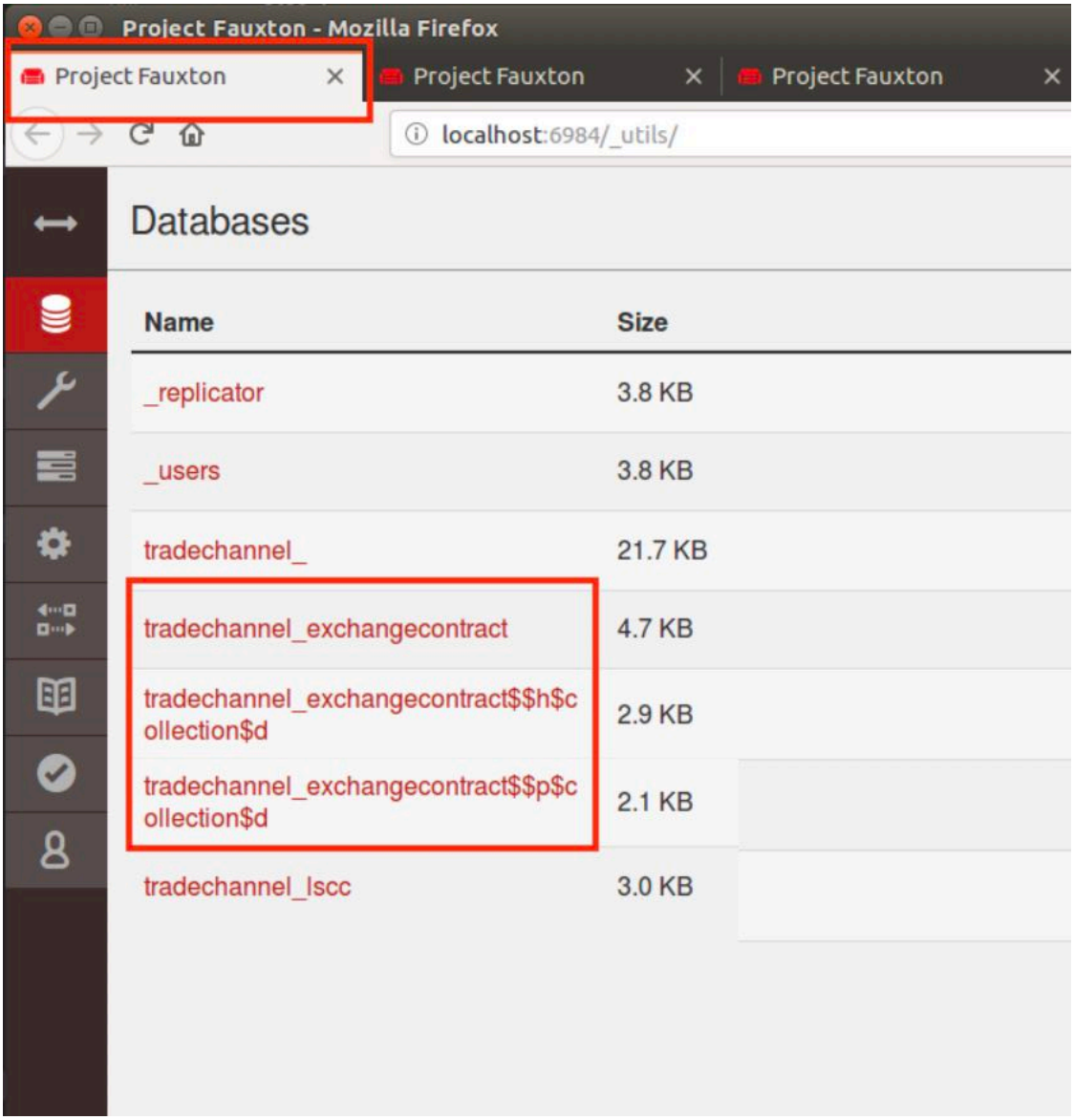
Notice that David can view this confidential information.

We can also review the 'private data footprints' in CouchDB – earlier, we launched 3 Firefox browser tabbed sessions, which will list currently databases and can click through to the individual records we've created at this time.

__ **80.** Switch to the **firefox** window

__ **81.** Click on the DigiBank CouchDB tab in Firefox – this is the URL running on **port 6984** and is the **first tab**. Refresh the page to see the update3d information.

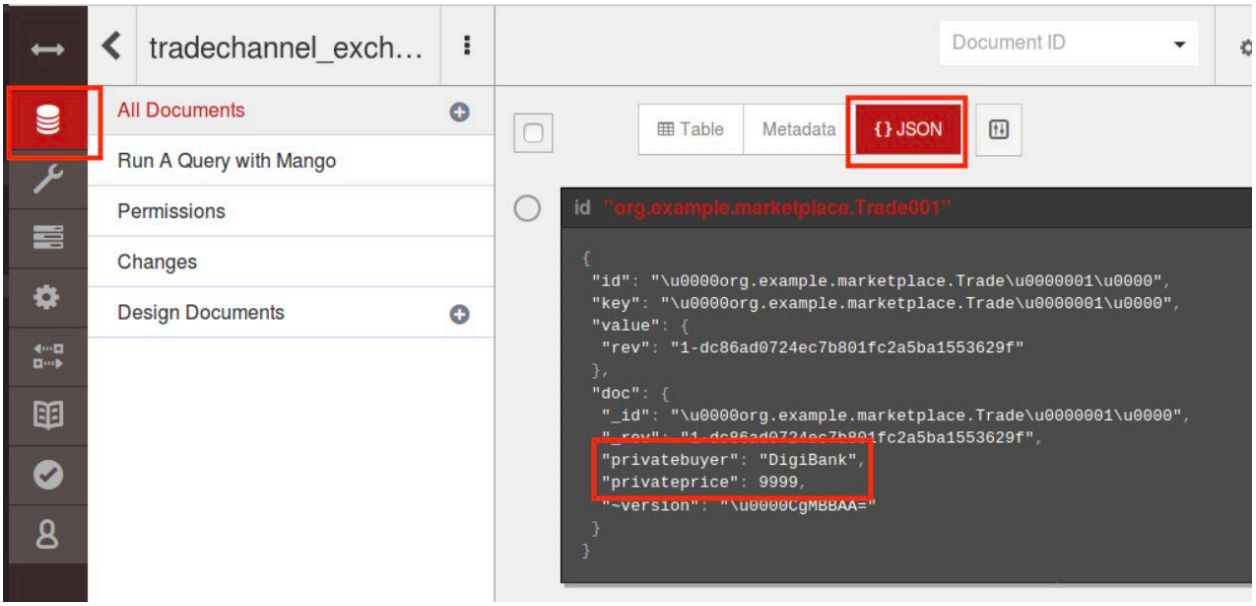
__ **82.** Review the databases created:
tradechannel_exchangecontract the world state database for the exchangecontract on the tradechannel
tradechannel_exchangecontract$$h$collection$d the private collection hashstore for CollectionD
tradechannel_exchangecontract$$p$collection$d the private collection for Collection D (which is only available in Digibank's CouchDB)



__ **83.** Click on the private collection tradechannel_exchangecontract$$p$collection$d

__ **84.** Click on the **{} JSON** view and you can see a record of the private data that was written for trade “001”.

When you have reviewed the data, click the **All DBs** icon to return.

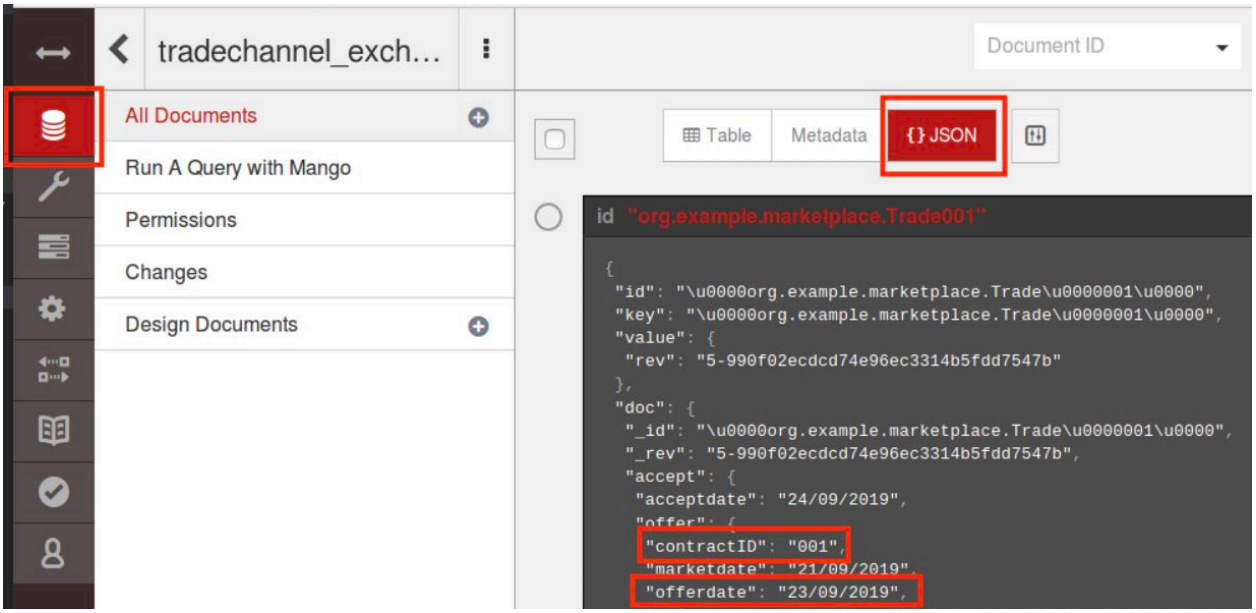


__ **85.** Back in the main database list – click on the world state database **tradechannel_exchangecontract**

__ **86.** Click on the **{} JSON** view and you can see the record for `"contractID": "001"`

Notice that the offer date is shown, but the private data is not.

Again, when you have reviewed the data, click the **All DBs** icon to return.



__ **87.** Still using the **first tab** for the **Digibank** CouchDB open the collection hash database **tradechannel_exchangecontract$$h$collection$d** and verify that the key and value is unreadable.

__ **88.** Using the **second tab** for the **Ecobank** CouchDB, look at the database list and notice that Ecobank does not have the private database (**tradechannel_exchangecontract$$p$collection$d**)

This is expected because the data is confidential to Digibank.

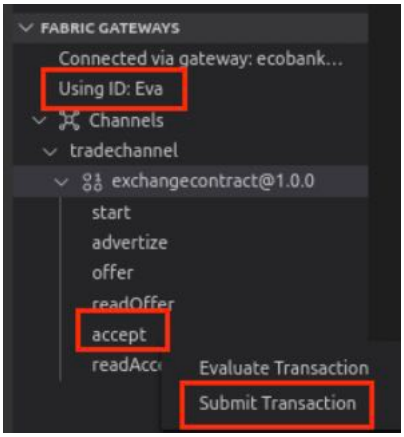
Having verified the databases in CouchDB we can proceed with the transaction flow with Ecobank (Eva) accepting the offer from Digibank.

__ **89.** Return to the VS Code editor and in the Fabric Gateways panel, click the Disconnect icon to disconnect from DigiBank's gateway.

__ **90.** In the Fabric Gateways panel connect to **ecobank_gw** and choose **Eva** as the identity

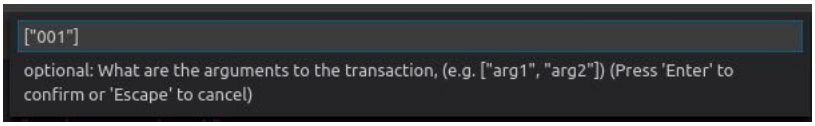
__ **91.** Expand the transaction list as before, and **right click** the **accept** transaction and click **Submit Transaction.**

We will now perform an accept transaction, as Eva**.** This will create some private data, for an approved accept transaction in EcoBank's private data collection.



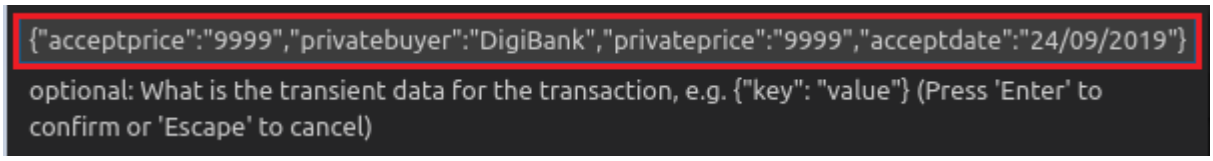
When prompted to enter arguments enter the following:

```
["001"]
```



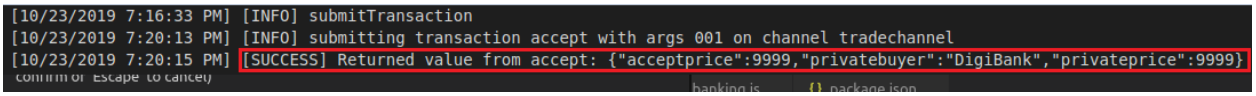
__ **92.** Enter or paste the following transient data for this transaction, replacing the '{}' provided with the following one-liner. Remember that you can copy and paste from the text file in gedit if necessary:

{"acceptprice":"9999","privatebuyer":"DigiBank","privateprice":"9999","acceptdate":"24/09/2019"}



The transaction is now submitted.

__ **93.** Review the output pane at the bottom for results – you should see a SUCCESS message similar to this:



Notice that the 'acceptdate' value is not part of this SUCCESS message. This is because we've made the 'acceptdate' a 'public' field, so that gets written to the channel ledger. The data set shown above (first 3 JSON values) is private data only viewable by EcoBank.

__ **94.** Return to Firefox and click on the **second tab** for the **Ecobank CouchDB** running on **Port 5984**

__ **95.** Click the **All DBs** icon and open the database for the private collection CollectionE **tradechannel_exchangecontract$$p$collection$e**

__ **96.** Click on the **{} JSON** format icon

Notice that the record for Trade001 has the private data for the accept transaction.

We are now going to try and read Ecobank private data with a Digibank ID which should fail, proving that the data is confidential to Ecobank.

__ **97.** Return to VS Code andin the Fabric Gateways panel click the **Disconnect** icon to disconnect from the current gateway.

__ **98.** Connect to **digibank_gw** with the identity **David.**

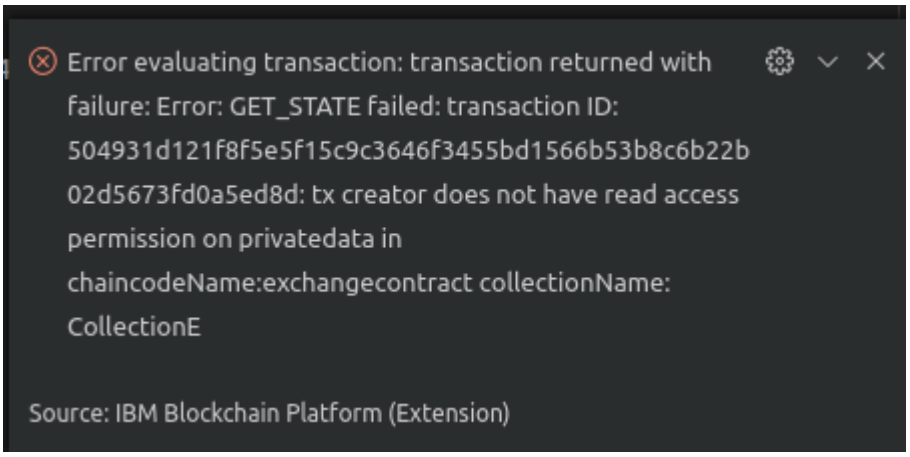
__ **99.** Right-click on the **readAccept** transaction and click **Evaluate Transaction.** When prompted enter the following in the parameters

```
["001"]
```

__ **100.** There is no transient data for this function, just press **enter** leaving the empty curly braces **{}**

The evaluate should return an error.

__ **101.** Expand the popup message on the bottom right in VS Code and you'll see a message that the transaction failed. This is because the Digibank Identity used to invoke the transaction cannot access the private collection.



__ **102.** Now **disconnect** from the DigiBank Gateway in the VS Code extension.

Review

- In this part of the Lab you have understood how to add private data transaction functions to a smart contract.
- You've instantiated the smart contract with a Collection Policy describing two private data collections - one each for EcoBank and DigiBank,
- You have used the new functions to create private data in those collections.
- You have seen that the transactions executed simultaneously create a private data hash store, containing the public hash, corresponding to the original private data stored off-chain.
- You have seen that Private Data is indeed Private – David from Digibank could not see the Ecobank collection.

4 Work with the Cross Verify Functions

In this section we will upgrade our smart contract in include a crossVerify transaction implementation, which will allow the smart contract to verify a calculated hash of source data against the private data hash record.

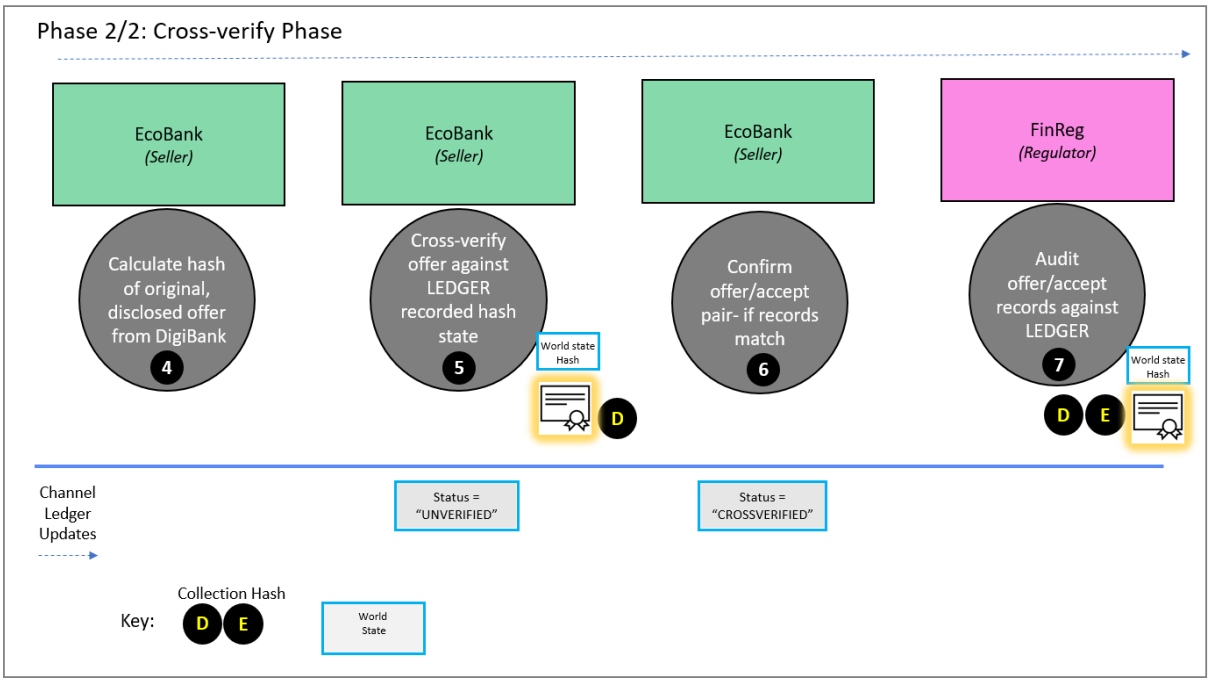
An identity from a proving organisation (for example, a Regulator) will invoke this cross-verify function and return a MATCH / NO MATCH response.

It's important to note that the verifying party only has access to the data hash store and not the private collection containing the confidential information.

Here are the steps to the cross-verify process:

1. **EcoBank** calculates a hash of the accepted offer and cross-verifies with the written hash of the offer for the contract in question, and which was written to the 'public' channel ledger at the same time the original private data transaction took place.
2. **EcoBank** cross-verifies they match.
3. If there is a match, the offer/accept pair is verified and the channel ledger record for the contract, is now set to 'CROSSVERIFIED' - At this point, the exchange can be completed, and the resultant sale transfer can be initiated
4. Later, the regulator **FinReg** wishes to cross-check the original offer and accept transactions recorded to each organisation's private data store, matches what is stored in the channel ledger.

Verify Pattern



Note that as we upgrade the smart contract to include the crossVerify method, we will also implement a query transaction type we will use in the subsequent section of the lab.

4.1 Understanding the Cross-Verify implementation

__ **103.** Click the Explorer icon in the VS Code editor, and return to the **trading-contract.js** file.

__ **104.** Scroll down to **line 241,** where you find the code comment

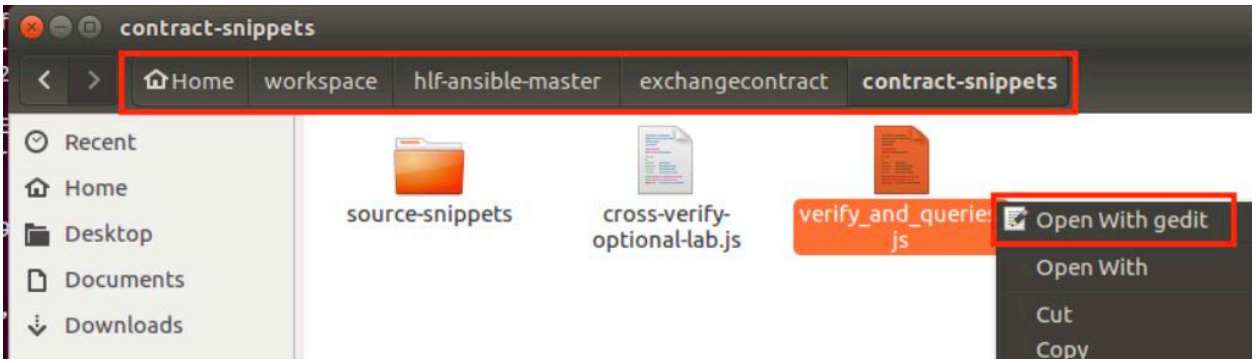
```
// UTILITY functions that may prove useful at some point
```

```
233             console.log('No private data with that Key: ', readKey);
234             return 'No private data with that Key: ' + readKey;
235         }
236         return pdString;
237     }
238
239
240
241     // UTILITY functions that may prove useful at some point
242
243     /**
244      * Get invoking MSP id - or any other CID related values
245      * @param {Context} ctx the transaction context
246      */
247     async _getInvokingMSP(ctx) {
```

This is where you will paste in the remaining functions of the contract.

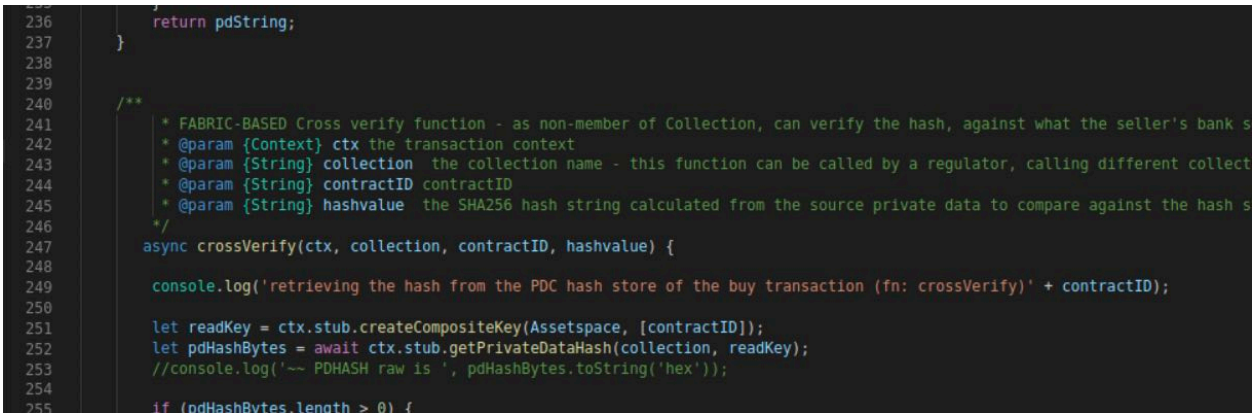
__ **105.** Open the Ubuntu File Explorer

__ **106.** Navigate to the following folder:
Home > workspace > hlf-ansible-master > exchangecontract > contract-snippets
Right click on `verify_and_queries.js` and select **Open with Gedit**



__ **107.** In the gedit session, highlight all the code by pressing **CTRL+A** to select, then press **CTRL+C** to copy to the clipboard

__ **108.** Back in the VS Code Explorer session, position the cursor at **line 239** and paste in the contents you copied to the clipboard using **CTRL+V**. Scroll back to Line 239 to check it was pasted OK.



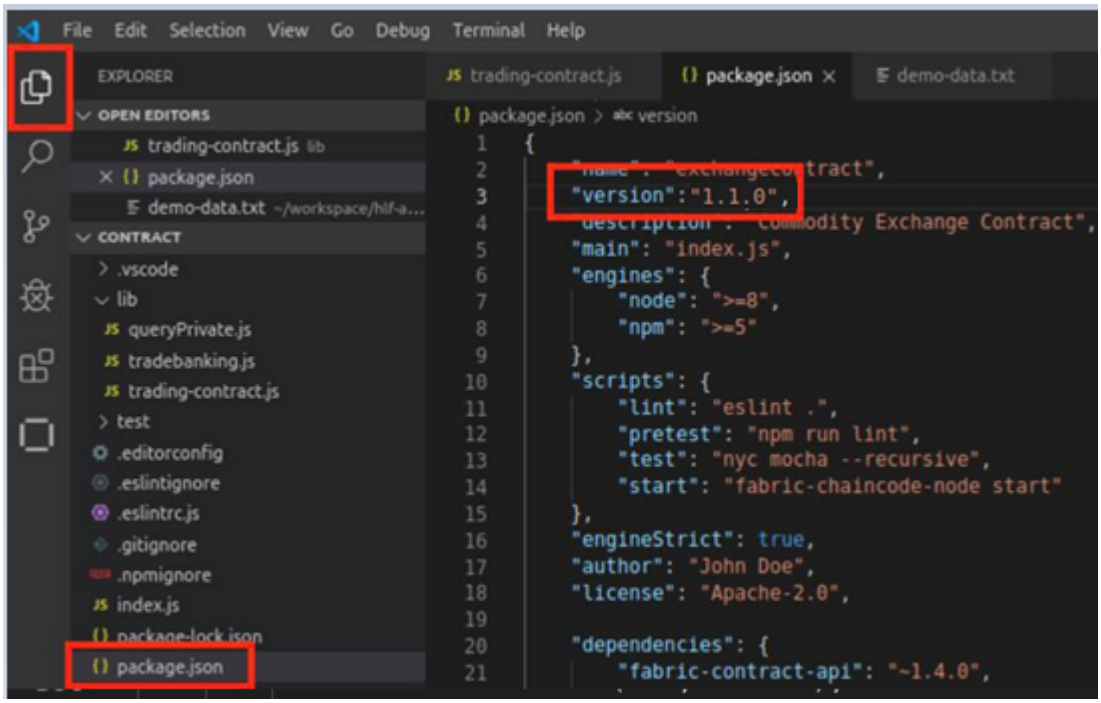
__ **109.** Select all the code in the window with **CTRL+A**.

Right-click and select **Format Selection** to format the code to fix the indentation.

The cross-verify code functionality and logic has now been added to the **trading-contract.js** edit session.

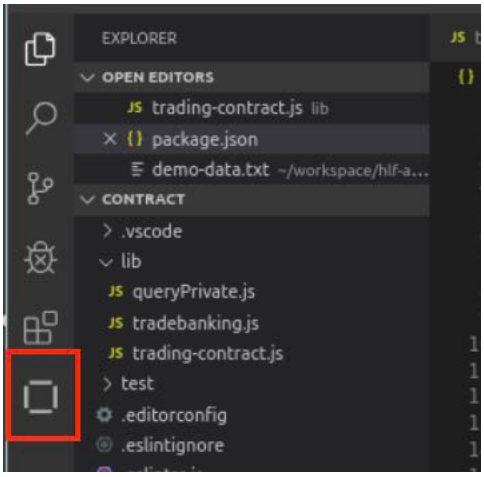
__ **110.** Save the file by pressing **CTRL+S**.

__ **111.** Still in the Explorer view, click on the **package.json** file and change the version number to “1.1.0”. Press **CTRL+S** to save the file.

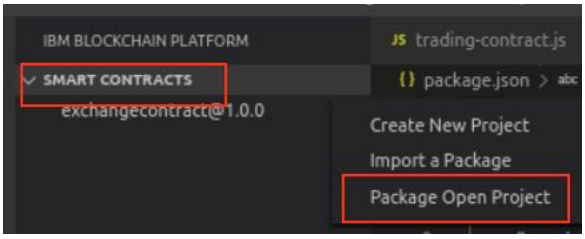


This will allow us to create a smart contract package with a new version number, and therefore allow us to upgrade our instantiated contract on the channel.

__ **112.** Click on the IBM Blockchain Platform extension icon.



__ **113.** Click on the ellipsis to the right of the Smart Contracts panel and select **Package Open Project**.



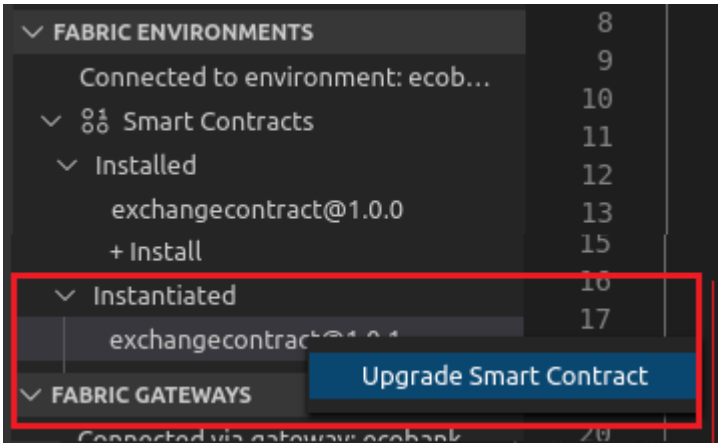
__ **114.** In the Fabric Environments view, click the Disconnect icon to disconnect from any connected environment, then connect to the **digibank** environment.

Click **+Install** and install the **exchangecontract@1.1.0** smart contract. Once completed, you'll get a confirmation it was performed successfully.

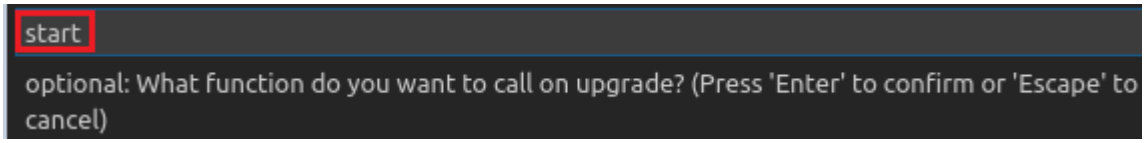
__ **115.** Repeat step 114 and install the new contract version onto the **finreg** environment.

__ **116.** Repeat step 114 and install the new contract version onto the **ecobank** environment.

__ **117.** Still connected to EcoBank's Fabric Environment **right click** the instantiated **exchangecontract@1.0.0** contract and click **Upgrade Smart Contract.** Select exchangecontract@1.1.0 as the smart contract to upgrade to.

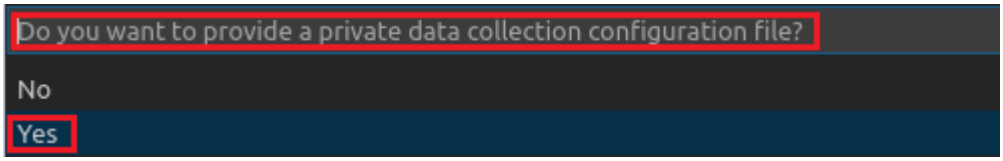


__ **118.** Enter **start** as the function to call on upgrade.

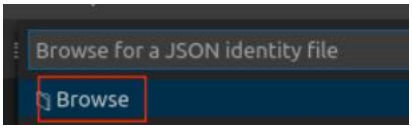


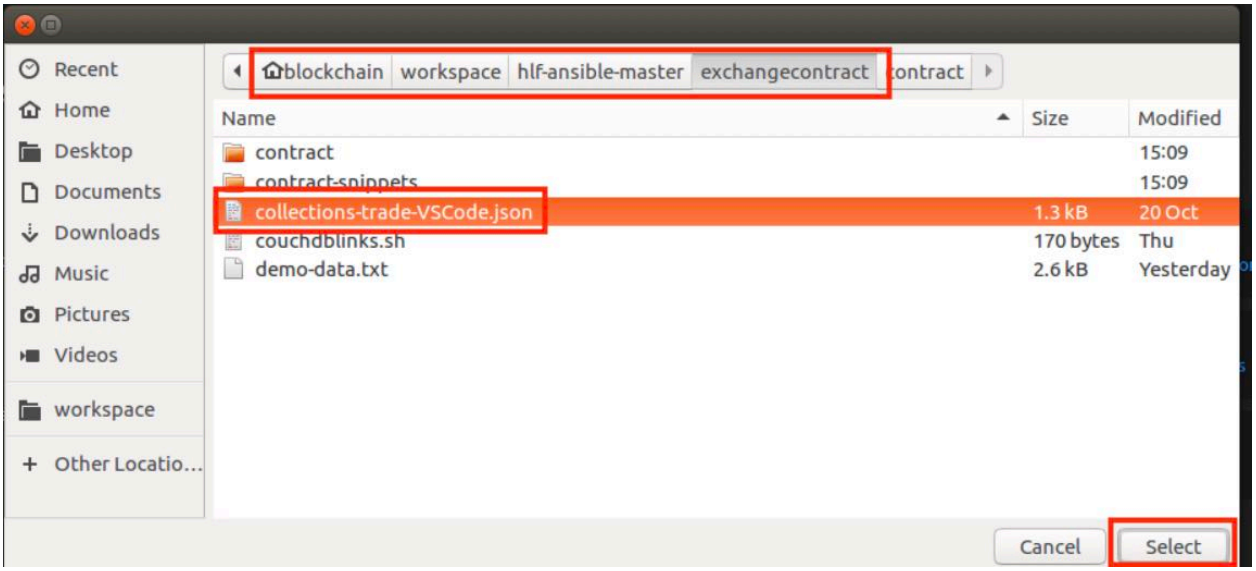
__ **119.** Press Enter to accept the default arguments to the function as there are none.

__ **120.** When asked if you 'want to provide a private data collection configuration file' – select 'Yes'

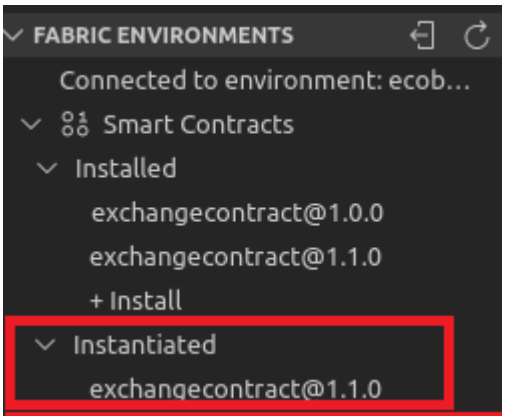


__ **121.** Click **Browse** and navigate to the folder
Home > workspace > hlf-ansible-master > exchangecontract
and select the file **collections-trade-VSCode.json**.





Upgrading may take a minute or so. When the process has completed it will show in the Fabric Environments view as follows:

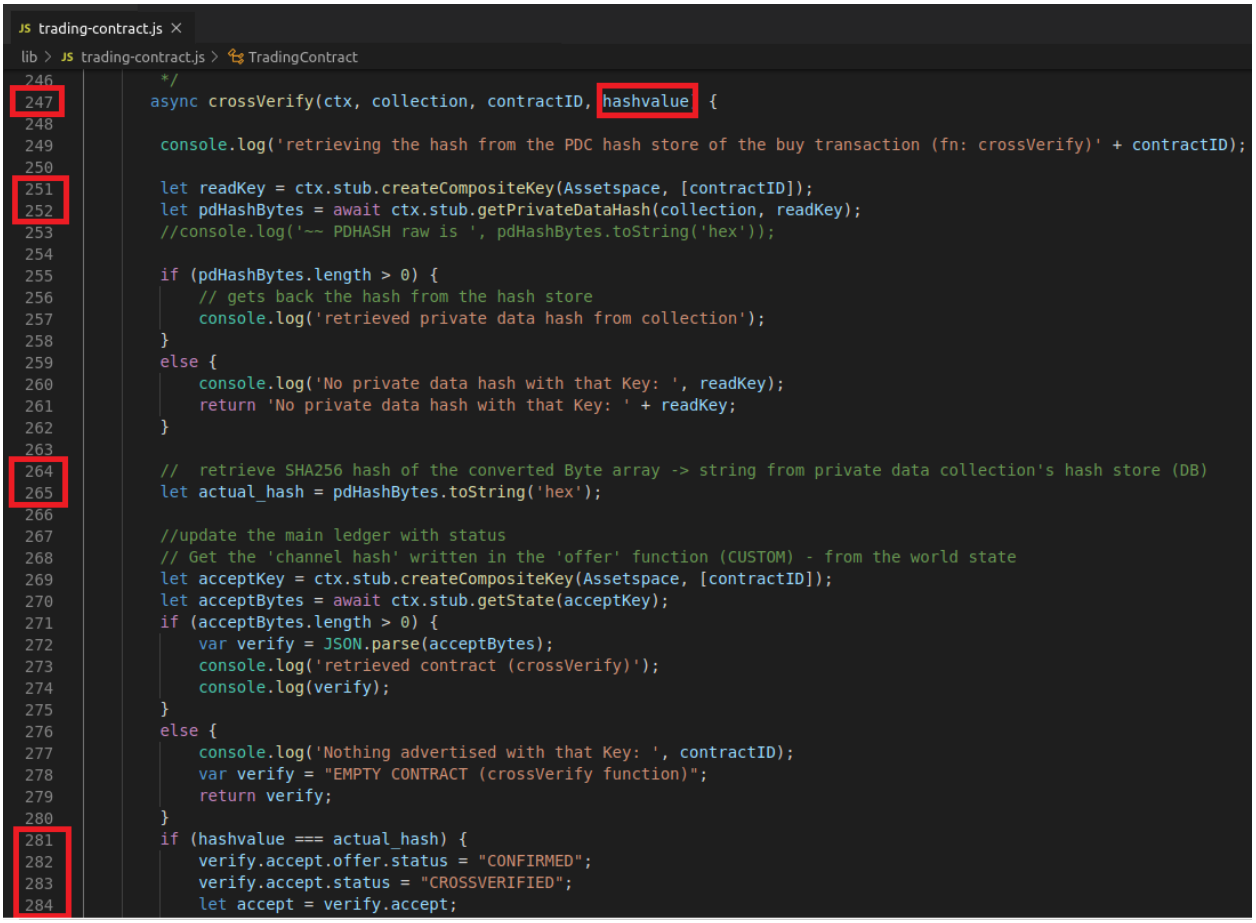


The smart contract has been instantiated on the tradechannel channel.

Before we proceed to invoke the cross-verification transactions, it helps to have a bit more explanation of what transaction functions were added by the copy/paste actions, and subsequent upgrade of the smart contract.

__ **122.** In the trading-contract.js editor croll to line 247.

Let's look at the first transaction – **crossVerify()**.

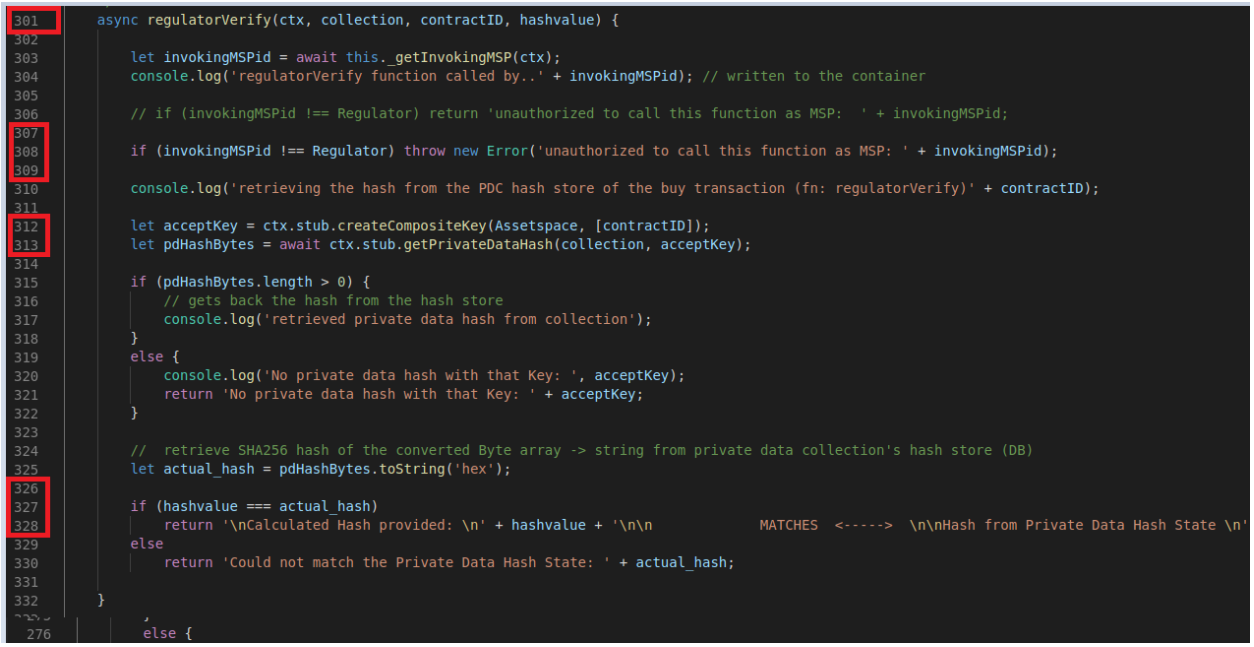


Lines 251-252 takes the supplied parameter (Contract ID) and finds the hashed key for this ID in the hashed data store using **getPrivateDataHash**

Line 264-265 converts the encoded Byte Array to a hexadecimal SHA256 hash

Line 281 compares the calculated hash (you do this in the 'perform' lab below) that's supplied as a parameter (hashvalue) – to the converted hash from line **265**
Depending on the comparison, it will either MATCH or FAIL MATCH. If a match is made lines **282-285** show that the status on the main channel ledger is updated to 'CROSSVERIFIED'

Line 301 is the **regulatorVerify** transaction – this is a 'specialist' transaction for use by a regulator.



```
301  async regulatorVerify(ctx, collection, contractID, hashvalue) {
302
303      let invokingMSPid = await this._getInvokingMSP(ctx);
304      console.log('regulatorVerify function called by..' + invokingMSPid); // written to the container
305
306      // if (invokingMSPid !== Regulator) return 'unauthorized to call this function as MSP:  ' + invokingMSPid;
307
308      if (invokingMSPid !== Regulator) throw new Error('unauthorized to call this function as MSP: ' + invokingMSPid);
309
310      console.log('retrieving the hash from the PDC hash store of the buy transaction (fn: regulatorVerify)' + contractID);
311
312      let acceptKey = ctx.stub.createCompositeKey(Assetspace, [contractID]);
313      let pdHashBytes = await ctx.stub.getPrivateDataHash(collection, acceptKey);
314
315      if (pdHashBytes.length > 0) {
316          // gets back the hash from the hash store
317          console.log('retrieved private data hash from collection');
318      }
319      else {
320          console.log('No private data hash with that Key: ', acceptKey);
321          return 'No private data hash with that Key: ' + acceptKey;
322      }
323
324      //  retrieve SHA256 hash of the converted Byte array -> string from private data collection's hash store (DB)
325      let actual_hash = pdHashBytes.toString('hex');
326
327      if (hashvalue === actual_hash)
328          return '\nCalculated Hash provided: \n' + hashvalue + '\n\n            MATCHES  <----->  \n\nHash from Private Data Hash State \n'
329      else
330          return 'Could not match the Private Data Hash State: ' + actual_hash;
331
332  }
      ,
 276      else {
```

Once again, on line 301, we see the parameters are the collection name, the contract ID and a calculated hashvalue to compare against the ledger state as written by **PutPrivateData()** in the offer/accept phase.

Lines 307-308 show that this transactioncan ONLY be called by someone that is in the Regulator organisation (there is a transactionthat checks the calling identity's MSP id), so identities from other organisations will not be able to execute this specialist transaction

Line 312-313 once again show the use of the **getPrivateDataHash** transaction

Lines 326-328 show what actions are taken dependent on whether there is a MATCH or failed MATCH between the hashes.

Further transactions added are also helper transactions like **ShowTransient** (show inputs for a given Transient set), invokeBadCollection (what you see when an attempt to write private data to an invalid or non-existent collection) and an **initLedger** transaction that is called once as **David** (Digibank) and **Eva** (EcoBank) to create some sample/demo private data in their respective collections (data is used for querying later).

4.2 Performing the Cross Verification of Private Data

The next step is to perform the verification: EcoBank had accepted the offer details provided by DigiBank, but now want to verify it against hash record of what DigiBank had originally created in their own collection.

__ **123.** In VS Code, click the **terminal** pane at the bottom of the screen. (If you cannot see this, click the VS Code menu “View->Terminal”.)

When the prompt appears, paste in the following line exactly (including the escape characters)

```
echo -n "{\"privatebuyer\":\"DigiBank\",\"privateprice\":9999}" |shasum -a 256
```

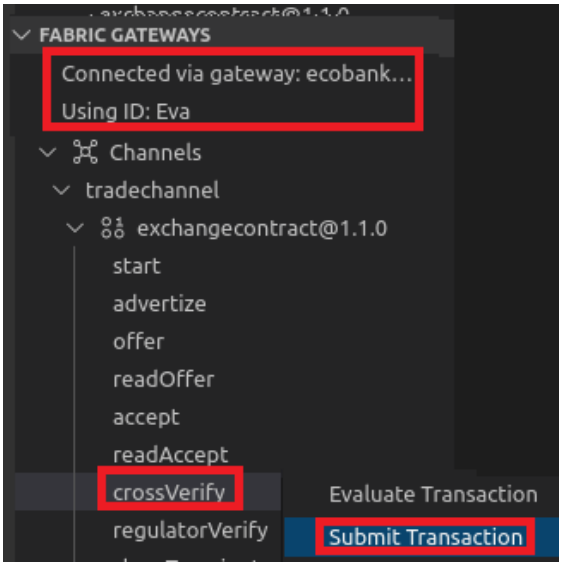
This will calculate a SHA 256 hash value of the source data EcoBank had agreed with DigiBank.

The command above returns a hash value beginning 22616. For convenience, we will provide this verification hash in the parameter string which you will shortly pass into the new smart contract transaction

__ **124.** In the **Fabric Gateways** panel disconnect from click **ecobank_gw** and connect with identity **Eva**

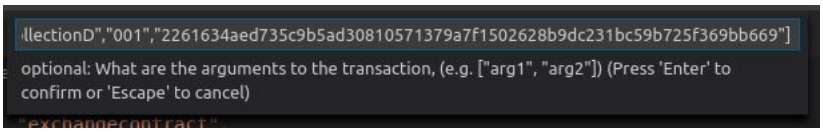
__ **125.** Expand the **Channels/exchangecontract@1.1.0.** Right-click **crossVerify** and click **Submit Transaction.**

Note that we are running ‘Submit Transaction’ and not ‘Evaluate Transaction’ because we will be updating the status on the channel ledger for the trade contract “001” to be ‘CROSSVERIFIED’ if the verify pattern returns a TRUE result or ‘MATCH’.



__ **126.** When prompted, paste in the following parameter list as a one-liner in the VS Code parameter field – replacing the existing '[]' text (again this is available in the text file in gedit)

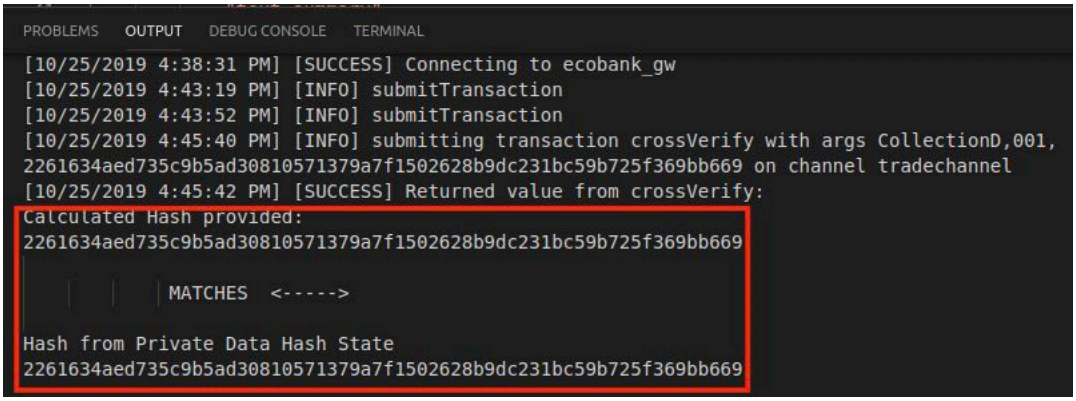
```
["CollectionD","001","2261634aed735c9b5ad30810571379a7f1502628b9dc231bc59b725f369bb669"]
```



__ **127.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

__ **128.** Wait for the transaction to complete, then select the Output pane and eview the messages.

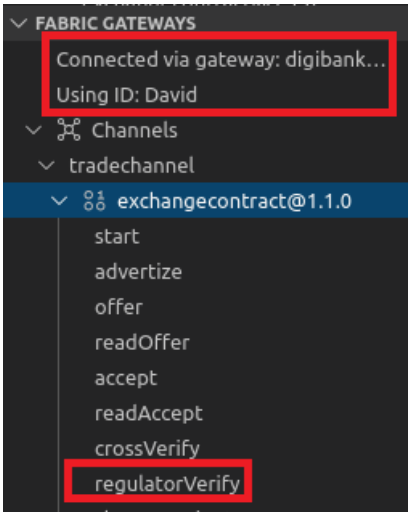
It should provide a match of the source data hash (for which we calculated a hash for from the terminal) against the private data hash store record for Contract "001" – a '**MATCHES'** banner should appear, and a confirmation of the hash values that were compared:



Note that equally, DigiBank, can take on the role of verifier (in the scenario where it needs to be verified by the other party): DigiBank can verify that the EcoBank hash store ('CollectionE') proves that the accept price stored by EcoBank privately, matches what was agreed by DigiBank, when the transaction was committed to the blockchain.

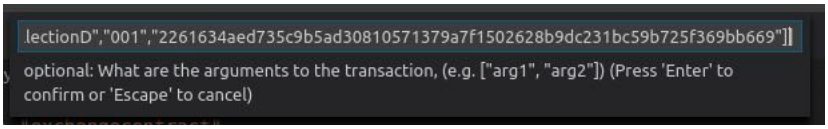
The next step is to cross-verify data as a Regulator auditing the data. The transaction **regulatorVerify** was added as part of the code you pasted into the smart contract earlier. This transaction can only be called by someone from the regulator organisation.

__ **129.** Still connected as the identity 'David' from DigiBank, highlight the **regulatorVerify** transaction, **right-click** on **regulatorVerify** and click **Evaluate Transaction**



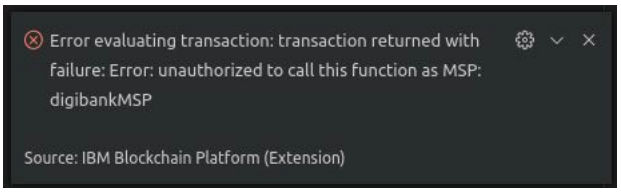
__ **130.** Provide the following one-liner parameter list as arguments when prompted, replacing the existing '[]' text:

```
["CollectionD","001","2261634aed735c9b5ad30810571379a7f1502628b9dc231bc59b725f369bb669"]
```



__ **131.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

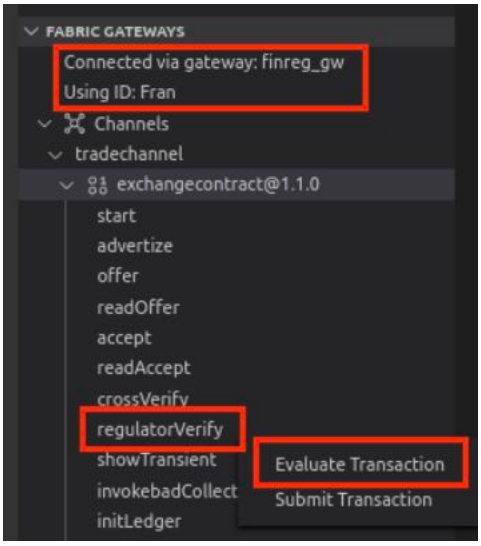
__ **132.** You should get an error, with a message explaining that you are not authorized to call this transaction because you're not an identity issued by the regulator organisation. (The **regulatorVerify** transaction checks the MSP id of the invoking identity.)



We will now switch to FinReg and invoke the transaction with an authorized identity.

__ **133.** On the **Fabric Gateways** panel disconnect from DigiBank's gateway and click **finreg_gw** and connect with identity **Fran.**

__ **134.** Once again, **right-click** the **regulatorVerify** transaction from the transaction list and click **Evaluate Transaction**

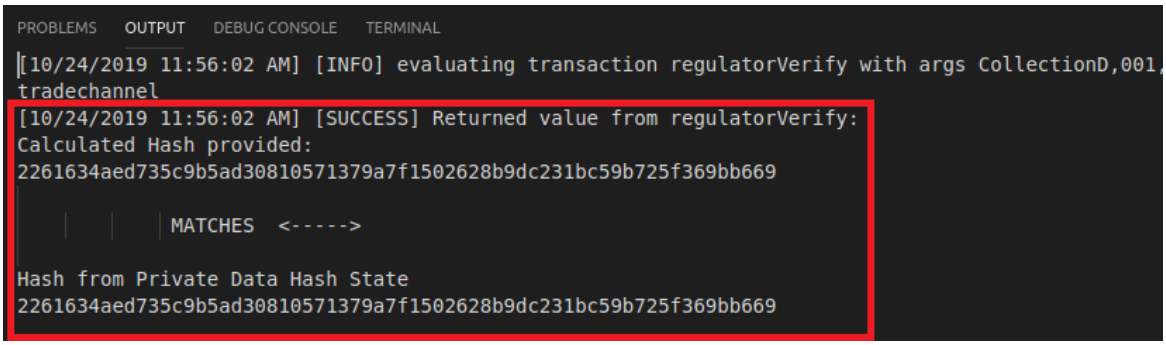


__ **135.** Provide the same parameter list as before when prompted:

```
["CollectionD","001","2261634aed735c9b5ad30810571379a7f1502628b9dc231bc59b725f369bb669"]
```

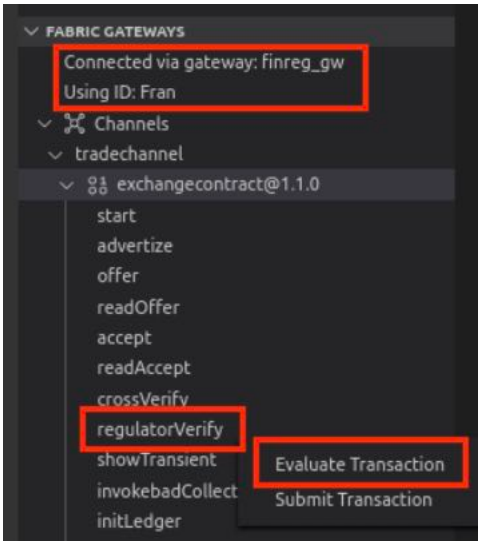
__ **136.** Again, there is no transient data for this transaction so just press **enter** leaving the empty curly braces **{}**

Now you should see that the evaluation is successful this time and the hashes match. You used evaluate for this transaction because there is no status update to the ledger by the transaction and the regulator only uses read transactions.



Up to now, all the cross-verify and regulator verify transactions have shown a MATCH so now we will deliberately mis-MATCH a regulator verify

__ **137.** Once again, **right-click** the **regulatorVerify** transaction from the transaction list and click **Evaluate Transaction**

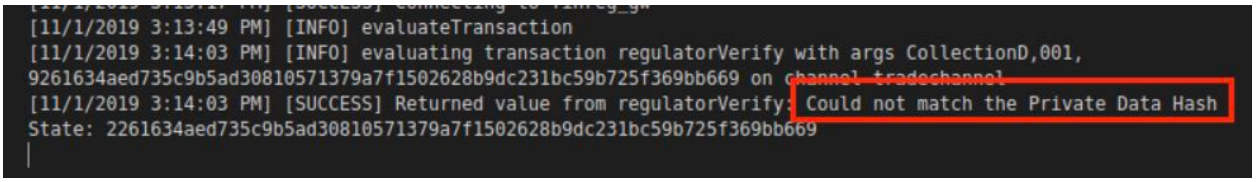


__ **138.** Provide the same parameter list as before except we change the first digit of the hash to be a **9** instead of a 2:

```
["CollectionD","001","9261634aed735c9b5ad30810571379a7f1502628b9dc231bc5
9b725f369bb669"]
```

__ **139.** Again, there is no transient data for this transaction so just press **enter** leaving the empty curly braces **{}**

Now you should see that there is no match.



This illustrates that the transaction works as expected, reporting when there is no match. This situation might arise if the regulator has been provided with the wrong pricing information to hash up, and the regulator would have to initiate a detailed investigation with the trading organisations.

Review

In this part of the lab

- You have modified the smart contract to add new transactions, installed on peers for all 3 organisations and upgraded the running version to v1.1.0
- You have worked with a **crossVerify** transactionthat both **EcoBank** (as the seller/acceptor) and **DigiBank** (as the buyer) can execute against collection hash stores to verify data shared for verification purposes.
- You have worked with a **regulatorVerify** transaction, which enables Fran (an identity associated with the regulator **FinReg**) to cross-verify or 'audit' that the private data evidence matches against the hashed records in the private data hash stores.
- You have tested the **regulatorVerify** with a hash that does not match.

5 Add Demo Data and Private Query Transaction

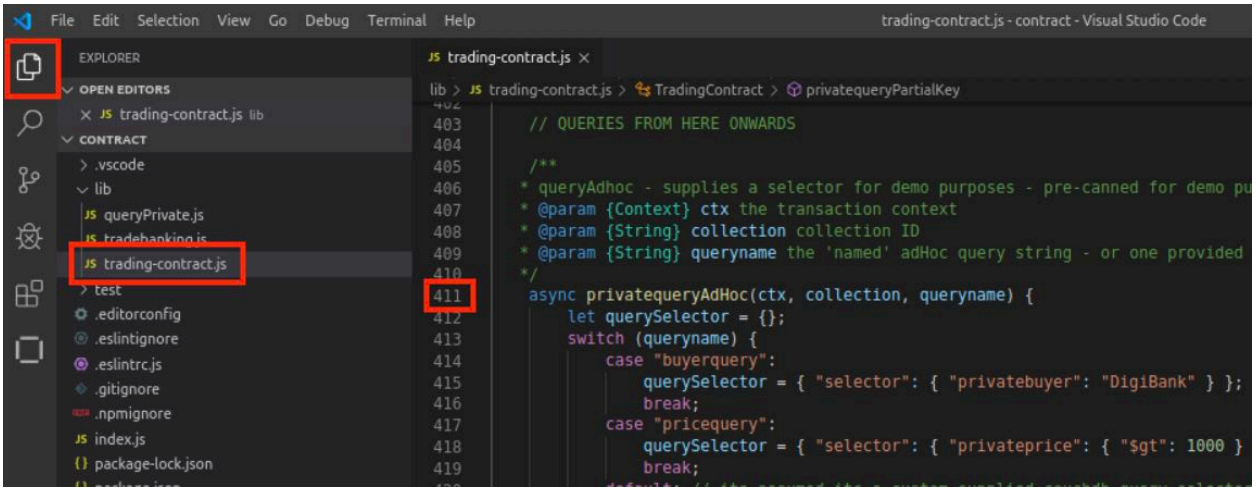
In this section of the lab we are going to focus on working with transactions to:

- Add sample data to two separate Private Data collections for query purposes – and
- Execute Private Data query transactions that allow you to perform 'rich queries' against the private collection data.

The demo data transaction **initLedger()** was added as part of the upgrade, as were the query transactions **privatequeryAdhoc()** and **privatequeryPartialKey**.

Let's look at the transactions:

__ **140.** Click the **Explorer** icon open **trading-contract.js** if it is not already displayed. Scroll to line 411 in the code.



The **initLedger** transaction creates four DEMO contracts that are advertised and – against those contract IDs, creates some offer and offer/accept sample data in both DigiBank's and EcoBank's private data collections. Next, let's briefly review the query transactions.

The first is **privatequeryAdhoc**() – this can take either a 'named query' (example;"pricequery" - queries Collection D for Contracts > 1000 USD) or it takes an 'ad-hoc' query string – where you create a 'custom query' selector string (CouchDB/Mango format) – and supply that to the **privatequeryAdhoc()** transaction itself.

```
403     // QUERIES FROM HERE ONWARDS
404
405     /**
406     * queryAdhoc - supplies a selector for demo purposes - pre-canned for demo purposes or provide ad-hoc string
407     * @param {Context} ctx the transaction context
408     * @param {String} collection collection ID
409     * @param {String} queryname the 'named' adHoc query string - or one provided as a parameter
410     */
411     async privatequeryAdHoc(ctx, collection, queryname) {
412         let querySelector = {};
413         switch (queryname) {
414             case "buyerquery":
415                 querySelector = { "selector": { "privatebuyer": "DigiBank" } };
416                 break;
417             case "pricequery":
418                 querySelector = { "selector": { "privateprice": { "$gt": 1000 } } }; // price is in integer format
419                 break;
420             default: // its assumed its a custom-supplied couchdb query selector  (collection, selector)
421                 // eg - as supplied as a param to VS Code:     ["CollectionD","{\"selector\":{\"privateprice\":{\"$lt\":1000}}}"]
422                 querySelector = JSON.parse(queryname);
423         }
424         console.log('main: querySelector stringified is:' + JSON.stringify(querySelector)); // logged for audit in the Docker container
425         let queryObj = new Query(Namespace);
426         let results = await queryObj.queryAdhoc(ctx, collection, querySelector);
427
428         return results;
429     }
```

Line 411 accepts the named query or ad-hoc as the queryname parameter, along with the collection name. Depending on the query, the selector is a pre-built query string, or the invoker of the query supplies a querystring themselves – you will see an example of using both later. Line 425-426 sets up the query object by calling a helper transaction from the **queryPrivate.js** source (where its class is defined) and then iterates through the query results, before (**line 428)** returning the query results to the VS Code output pane in this case.

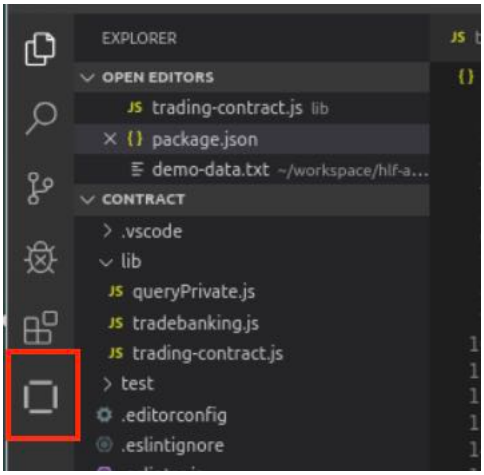
There is also a **privatequeryPartialKey** transaction that does a query of a private data collection by partial key (e.g. Asset namespace, to find all records for that namespace, in the collection supplied).

5.1 Create some Demo Data for querying data

We will now create demo data using the initLedger transaction, and we will be using both DigiBank and EcoBank identities to create the data. The result will be some additional records to run queries against.

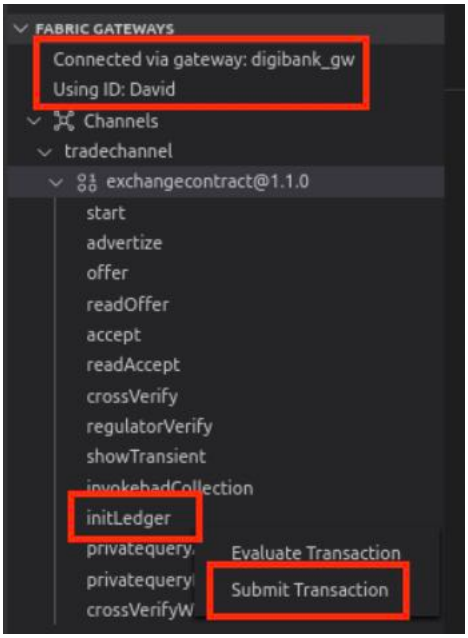
We need to return to the IBM Blockchain Platform extension.

__ 141. Click on the IBM Blockchain Platform extension icon.



__ **142.** On the **Fabric Gateways** panel disconnect from FinReg's gateway and click **digibank_gw** and connect with identity **David.**

__ **143.** Expand the **exchangecontract** and right-click **initLedger.** Click **Submit Transaction**



__ **144.** There are no parameters, just press **enter** leaving the empty square brackets **[]**

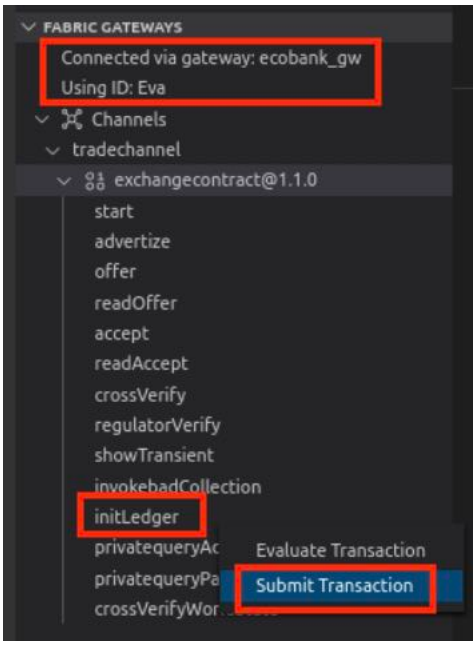
__ **145.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

The transaction should return a 'success' message in the output pane, indicating the demo data was created:

```
Created some new demo contracts (main ledger) and private Data for DigiBank
```

__ **146.** On the **Fabric Gateways** panel disconnect from DigiBank's gateway and click **ecobank_gw** and connect with identity **Eva.**

__ **147.** Scroll down to the transaction **initLedger**, right click then click **Submit Transaction**



__ **148.** Once again, there are no parameters, just press **enter** leaving the empty square brackets **[]**

__ **149.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

__ **150.** Review the messages in the output pane – it should indicate that the private demo data was created this time for EcoBank

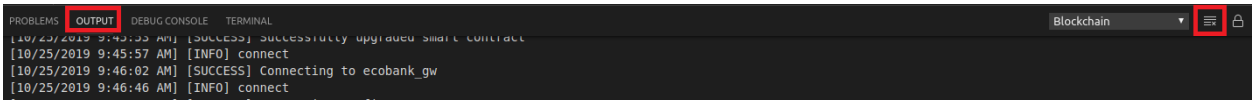
```
Returned value from initLedger: Create some private Data for EcoBank
```

We can now proceed with the next part – to try out the private data queries. In doing so, we will perform some simple queries that will query each of the private data collections for **DigiBank** and **EcoBank** – which contain both demo data and data you created during this lab exercise.

5.2 Executing Rich Queries against the Private Data Collections

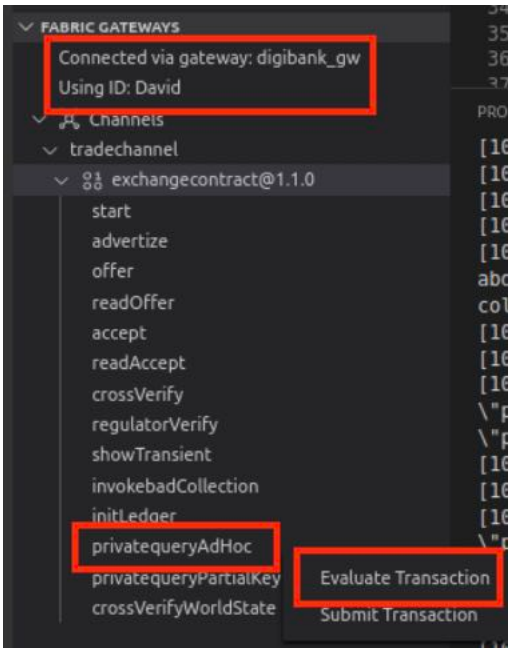
So that we can more easily see what is happening, we're going to reset the Output pane and make it larger.

__ **151.** At the top right of the Output pane click on the Clear Output icon, then resize the pane up, to create a larger space for output messages.



__ **152.** On the **Fabric Gateways** panel disconnect from EcoBank's gateway and click **digibank_gw** and connect with identity **David.**

__ **153.** Expand the **exchangecontract** and right-click **privatequeryAdhoc.** Click **Evaluate Transaction**



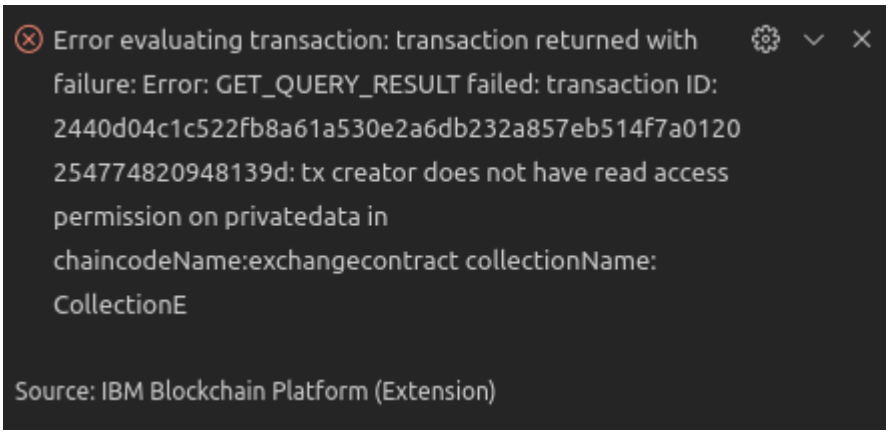
__ **154.** When prompted, **copy and paste** the following parameters, replacing the '[]' text offered with the following parameter list:

```
["CollectionE","buyerquery"]
```

The first parameter is the private collection name (recall that we have 2 collections CollectionD and CollectionE). The second parameter is the name of the query that we wish to run.

__ **155.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

Notice that we provided **Collection 'E'** in the parameter list – to which DigiBank does not have access – so we will get a popup error indicating the query could not be performed (access denied)



__ **156.** Close the error popup message, and clear the Output pane using the **Clear Output** icon, as shown previously.

__ **157.** Once again, right-click **privatequeryAdhoc** and click **Evaluate Transaction.**

__ **158.** When prompted, paste in the following parameters, replacing the '[]' text offered with the following 'named' query called 'buyerquery' :

```
["CollectionD","buyerquery"]
```

Review the output pane showing your query results.

Let's try another query, a price query for a 'privateprice' value that's greater than 1000 USD

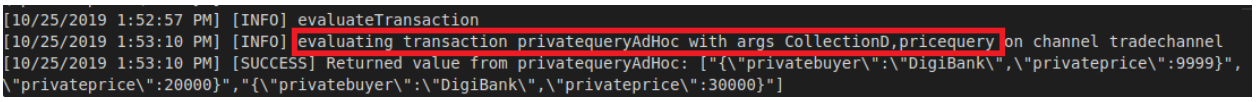
__ **159.** Once again, right-click **privatequeryAdhoc** and click **Evaluate Transaction**.

__ **160.** When prompted, paste in the following parameters, replacing the '[]' text offered with the following 'named' query, 'pricequery' :

```
["CollectionD","pricequery"]
```

__ **161.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

__ **162.** Review the output pane for messages – you should see your query results – a screenshot of sample output is shown below – you will see different results. Missing from these results are are two records from the earlier listed results that are under 1000 USD. This is because out example pricequery is hard coded to show only values over 1000.



Next you will try some queries as EcoBank.

__ **163.** On the **Fabric Gateways** panel disconnect from DigiBank's gateway and click **ecobank_gw** and connect with identity **Eva.**

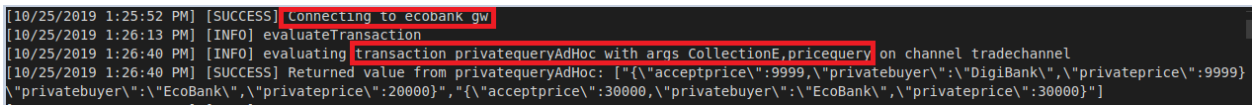
__ **164.** Expand the **exchangecontract** and right-click **privatequeryAdhoc**. Click **Evaluate Transaction**

__ **165.** When prompted, paste in the following parameters, replacing the '[]' text offered with the following – and press **enter**

```
["CollectionE","pricequery"]
```

__ **166.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

__ **167.** Review the messages in the output pane – you should see the results show the additional 'accept' data that's only recorded in EcoBank's private data collection.



Finally, lets supply an 'ad-hoc' query selector query string to the **privatequeryAdhoc** transaction – this enables a user to supply a custom query – in this case, to see the accept/offer records, whose values are less than 1000 USD.

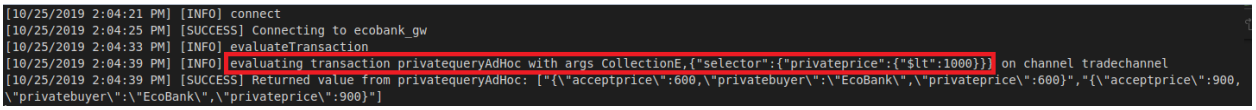
__ **168.** Once again, right-click **privatequeryAdhoc** and click **Evaluate Transaction**.

__ **169.** When prompted, paste in the following parameters, replacing the '[]' text offered, with the following string, pasted in exactly as shown – and press **enter**:

```
["CollectionE","{\"selector\":{\"privateprice\":{\"$lt\":1000}}}"]
```

__ **170.** There is no transient data for this transaction, just press **enter** leaving the empty curly braces **{}**

__ **171.** Review the messages in the output pane – you should see a different set of results, which are the two records that match the criteria we provided ("less than 1000").



This concludes the lab steps for working with Private Data queries.

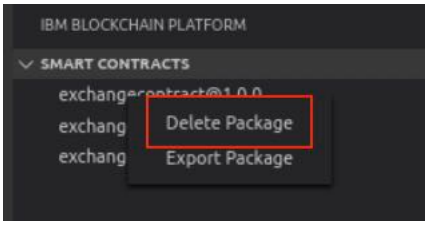
Review

You've now successfully:

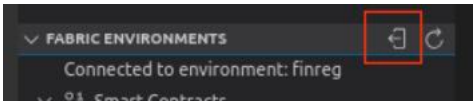
- created some additional demo or sample data
- performed queries against private data collections
- understood more about using rich queries to filter result sets, by using different criteria.

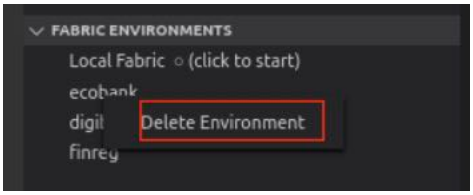
Finally you need to cleanup the virtual machine in preparation for the next lab.

__ **172.** In the **Smart Contracts** panel **right-click** each package in turn and click **Delete Package**.

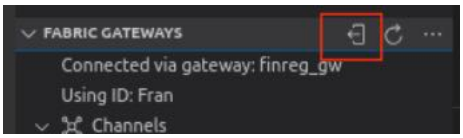


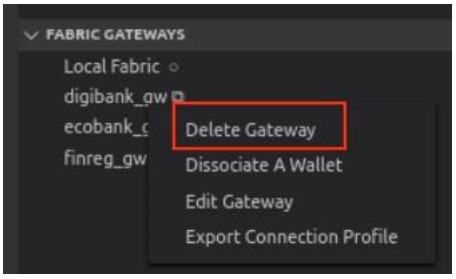
__ **173.** In the **Fabric Environments** panel **Disconnect** the current environment, and then **right-click** each environment and click **Delete Environment**.



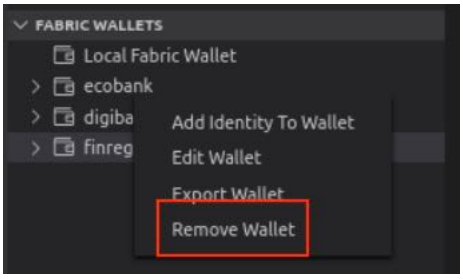


__ **174.** In the **Fabric Gateways** panel **Disconnect** the current gateway, and then **right-click** each gateway in turn and click **Delete Gateway**.





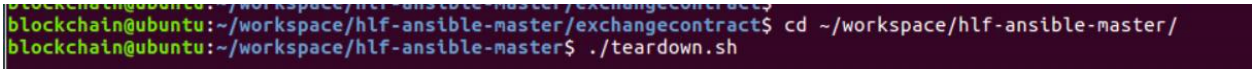
__ **175.** In the **Fabric Wallets** panel **right-click** each wallet in turn and click **Remove Wallet**.



__ **176.** In the terminal window, use the following two commands to navigate to the **hlf-ansible-master** folder and teardown the custom network using a bash script:

```
cd ~/workspace/hlf-ansible-master
```

```
./teardown.sh
```



Congratulations!

We Value Your Feedback!

- Please ask your instructor for an evaluation form. Your feedback is very important to us as we use it to continually improve the lab material.
- If no forms are available, or you want to give us extra information after the lab has finished, please send your comments and feedback to "**blockchain@uk.ibm.com**"

Appendix 1 - transaction List Info for 'exchangecontract'

A table containing the smart contract transaction names, parameters and main objective of each – is shown below.

Fields in BOLD / RED are the private data elements, the remainder are stored in the ledger world state. The contract ID represents the trade commodity contract, being bought/sold/traded on the exchange marketplace FYI. Note that you may have seen that both private and public data are passed in the transient data set in the lab exercises.

transaction	Action	Parameters / {Transient Data}	Summary Objectives
advertize	submit	contractID, seller, symbol, quantity, reserveprice, marketdate	'Broadcast' the commodity for sale on the marketplace. The composite key is made up of an Assetspace (domain) + Contract ID
offer	submit	contractID, { buyer, offerprice, offerdate }	The buyer's bank (ie on behalf of his broker), makes an offer on the advertised commodity – its key is retrieved exactly as described above.
readOffer	evaluate	contractID	Helper transaction: The beholder of the actual private data, can use this simple transaction, to see what's written to 'its' Org's collection
accept	submit	contractID, {buyer, offerprice, acceptprice, acceptdate }	The seller's bank, notified by the buyer's bank, accepts the offer on behalf of his client – a status of UNVERIFIED will be written, pending a cross-verification to see the offer is genuine
readAccept	evaluate	contractID	Helper transaction: The beholder of the actual private data, can use this simple transaction, to see what's written to 'its' Org's collection

crossVerify	submit	Collection ID, contractID, calculated_hash	The seller's bank, must verify the integrity of the offer hash, written on the blockchain. It uses the offer data it received 'out-of-band', to calculate a hash and cross-verify the offer hash on the ledger. (Note: The regulator will also use this to verify both the offer/accept private data, later on)
invokebadCollection	evaluate	<none>	A transaction to show what the user would see (in VS Code) if an invalid collection is invoked in the smart contract.
privatequeryAdhoc	evaluate	collection, <<queryname or query selector>>	Query the private data by 'name' (by buyer, by offer price etc) or supply query selector (Mango) as a parameter
privatequeryPartialKey	evaluate	Assetspace prefix	Find all contracts in a private data collection, with given prefix

Appendix 2 Access control considerations for Private data

If the private data is relatively simple and predictable (e.g. transaction dollar amount), channel members who are not authorized to the private data collection could try to guess the content of the private data via brute force hashing of the domain space, in hopes of finding a match with the private data hash on the chain. Private data that is predictable should therefore include a random “salt” that is concatenated with the private data key and included in the private data value, so that a matching hash cannot realistically be found via brute force. The random “salt” can be generated at the client side (e.g. by sampling a secure pseudo-random source) and then passed along with the private data in the transient field as transient data, at the time of chaincode invocation. For more information, see the Fabric documentation:

https://hyperledger-fabric.readthedocs.io/en/latest/private-data-arch.html#access-control-for-private-data

Appendix 3 - Alternate Trade Network Fabric

In case of problems setting up the Fabric in Part 1 of this lab document, an alternate Fabric can be started using these steps. This Alternate Fabric should only be used at the explicit instruction of the Instructor.

1. In VS Code disconnect any connected Fabric Environment.

2. Right click on any Fabric Environment for Ecobank, digibank, finreg and **Delete Environment** (Remember to click **yes** in the bottom corner of the screen)

3. Disconnect any connected Fabric Gateway.

4. Right click on any Fabric Gateway for Ecobank, digibank, finreg and **Delete Gateway**

5. In a terminal window, run the following commands to clearup the "regular" Fabric:
   cd ~/workspace/hlf-ansible-master
   ./teardown.sh

6. Run these commands in the terminal window to work with the BackupFabric:
   cd ~/workspace/hlf-ansible-master
   tar -xzf backupFabric.tar.gz
   cd backupFabric
   ./start.sh

   wait for the output to end with "Successfully submitted channel update"

7. In VS Code, hover over **Fabric Wallets**, and click the "**+**" sign to **add wallet**.
   At the top of the screen click the option to **Specify an existing file system wallet**
   Click **Browse** then navigate to the folder:
   home/blockchain/workspace/hlf-ansible-master/backupFabric/adminWallets
   and click **ecobank** and then **select**

8. In the same way add the new wallets for digibank and finreg.

9. Hover over the **Fabric Environments** and click the "**+**" sign to **add environment**
   At the top of the screen specify **ecobank** as the name
   Click **Browse** then navigate to the folder:
   home/blockchain/workspace/hlf-ansible-master/backupFabric
   and click **Ecobank-nodes** and then **select**

Click **done adding nodes**

10. Click on the **ecobank** environment and verify that it connects to the Fabric

11. Disconnect from the ecobank environment and using the same technique add the environments for **digibank** and **finreg**

12. Hover over **Fabric Gateways**, and click the "**+**" sign to **add gateway**.
    At the top of the screen click the option to **Create a gateway from a Fabric environment**
    Click **ecobank** as the environment to create from
    Press enter to accept **ecobank_gw** as the name
    Click **caecobank.ecobank.example.com** as the ca for the gateway
    Click on the new **ecobank_gw** and click **Eva** as the id for the connection

13. Disconnect from the ecobank_gw gateway, and using the same technique add the gateways for **digibank_gw** and **finreg_gw**. When testing the gateways use the IDs **David** and **Fran** respectively.

14. Return to the main lab instructions at **Part 2 – Deploy a Base Version of the Smart Contract** …