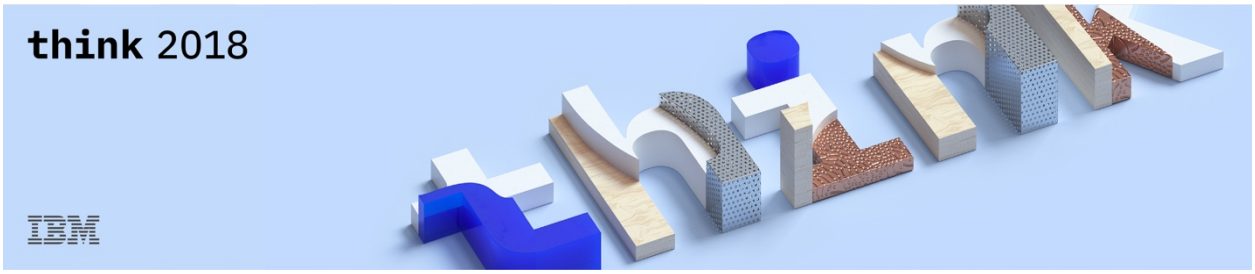


Lab Center – Hands-on Lab

Session 9603

Session Title Secure your Mobile Transactions End to End with IBM Mobile Foundation and Blockchain

Srihari Kulkarni, IBM, skulkarni@in.ibm.com

Sukesh Prabhakar, IBM, sukesh.prabhakar@in.ibm.com

Table of Contents

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.

Secure your Mobile Transactions End to End with IBM Mobile Foundation and Blockchain

Introduction

A block chain is defined as an open, distributed digital ledger of transactions. A blockchain is managed by a network of computers to validate and vet every transaction in the blockchain. Hyperledger is an open source effort spear-headed by the Linux Foundation for the development of blockchain technologies.

In this lab, you will see how you can setup an example blockchain network for the purpose of implementing a digital wallet and transfer virtual money among its peers. All transactions of the virtual wallet will be performed through a mobile app that is secured by IBM Mobile Foundation. Transactions from the mobile app will be submitted to the blockchain network through the use of MobileFirst adapters.

You will also see how you can automatically generate a full fledged MobileFirst adapter that can integrate with Hyperledger.

Getting started

The VM image of the lab has an instance of Hyperledger and the IBM Mobile Foundation Developer Kit pre-installed.

IBM Mobile Foundation is also available as a service on IBM Cloud where the IBM Mobile Foundation server is hosted on the cloud which mobile apps can connect to.

1. Clone the lab repository

Before getting started, clone the respository having the code for this lab.

Open a Terminal window and enter the following commands

```
cd /work
mkdir lab9603
cd lab9603
git clone https://github.com/Think18/Lab9603
```

Get your Hyperledger ready

2. Review the Hyperledger business network

   The payment-network folder contains the definition of the business network for managing peer-to-peer payments.

   The models/com.ibm.payments.cto file contains the model of the business. It contains definitions of the following

   a. Assets
      a. An asset called 'Account' identified by an account ID, owned by an account holder and a property called balance which represents the balance in the account.
   b. Participants
      a. A participant called 'AccountHolder' identified by an email who is the owner of the asset type called 'Account'.
   c. Transactions
      a. A transaction called 'TransferMoney' which takes properties such as the source account and destination account and the amount to be transferred.

   The lib/logic.js file contains the logic for defining the transactions.
   Review this code.

3. Set up your Hyperledger instance

The tools required for setting up a Hyperledger instance has already been installed on the VM. You will now set up the Hyperledger instance for making peer to peer payments.

First, start the Hyperledger Fabric instance

```
cd /work/fabric-tools
./startFabric.sh

cd ../lab9603/Lab9603/payment-network
```

Create an archive file for the business network in the current directory.

```
composer archive create –t dir –n .
```

The next step is to deploy the business network on to the hyperledger fabric.

a. Install the composer runtime

```
composer runtime install --card PeerAdmin@hlfv1 --
businessNetworkName payment-network
```

b. Deploy & start the business network

```
composer network start --card PeerAdmin@hlfv1 --networkAdmin
admin --networkAdminEnrollSecret adminpw --archiveFile payment-
network@0.0.1.bna --file networkadmin.card
```

c. Import the network's admin as a business network card

```
composer card import --file networkadmin.card
```

d. Verify if the business network has been deployed successfully

```
composer network ping --card admin@payment-network
```

e. Start the REST server for the hyperledger instance

```
composer-rest-server -c admin@payment-network -n never -w
true
```

You have now setup your hyperledger instance successfully.

f. Download the Swagger JSON file of the Hyperledger REST APIs.
Open http://localhost:3000/explorer - you will see the REST APIs for the network you just deployed in Swagger UI
Visit http://localhost:3000/explorer/swagger.json to get the JSON format of the Swagger definition.
Copy paste the entire content into a text file named PaymentNetwork.json

Compare the contents of the file you just saved and the one found in /work/lab9603/Lab9603/PaymentNetwork.json
You will find the hostname added and a couple of type modifications to make it compatible with Open API specifications.
Merge the two files. Alternatively, overwrite the one you generated with the one from the github repo.

We will use this file in a later step.

Connect your Mobile app to the Blockchain through IBM Mobile Foundation

4. Setup your MobileFirst server

The MobileFirst server acts as a gateway between your mobile app and the blockchain network. Among other things, the MobileFirst server ensures

a. A secure connection between your mobile app and the blockchain
b. Lifecycle management of your app
c. Protecting your app & blockchain from unauthorized access by ensuring authenticity of the application, the device and the user. In other words, MobileFirst server prevents fake or malicious apps from accessing your blockchain, it can authenticate end users using methods that are unique to a mobile device (e.g. fingerprint)
d. It offers convenient offline storage such that transactions can be made when the device is offline and then submitted to the blockchain when the device gets online.

To set-up your MobileFirst server, first check if the server is already running.

a. Visit http://localhost:9080/mfpconsole from a browser

If you see a web page for the IBM MobileFirst Operations Console, you can skip the next step.

b. Start the MobileFirst server

```
cd /work/MobileFirst-8.0.0.0
export JAVA_HOME=/usr/lib/jvm/java8-openjdk-amd64

./run.sh
```

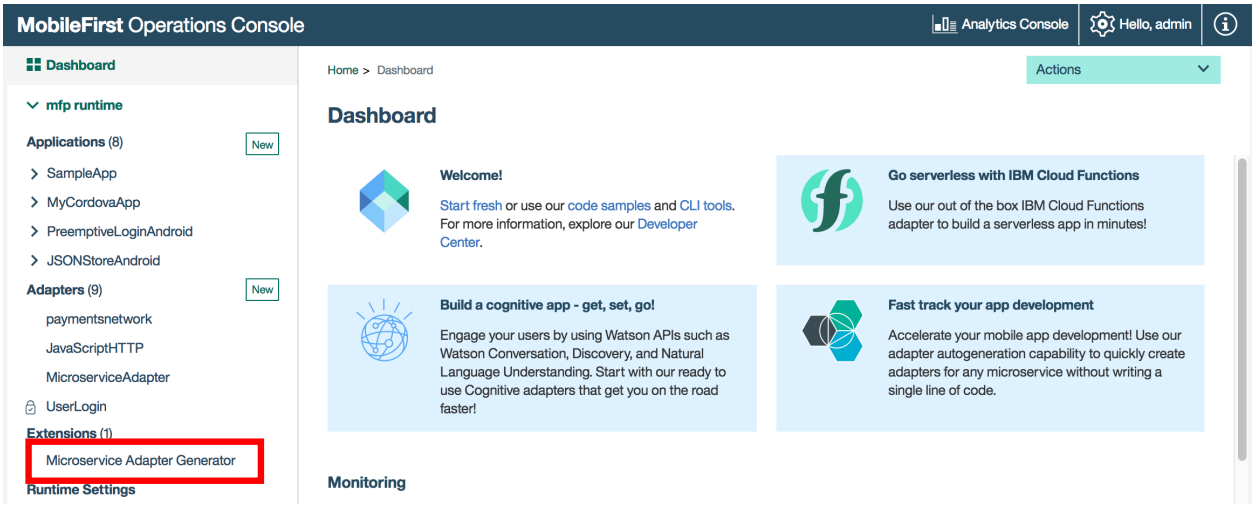
c. Verify your server is running by visiting the MobileFirst Operations Console at http://localhost:9080/mfpconsole

d. Login with the default credentials of admin / admin

The MobileFirst server has an extension called Microservice Adapter Generator which will automatically generate a MobileFirst adapter for any Open API compatible REST service.

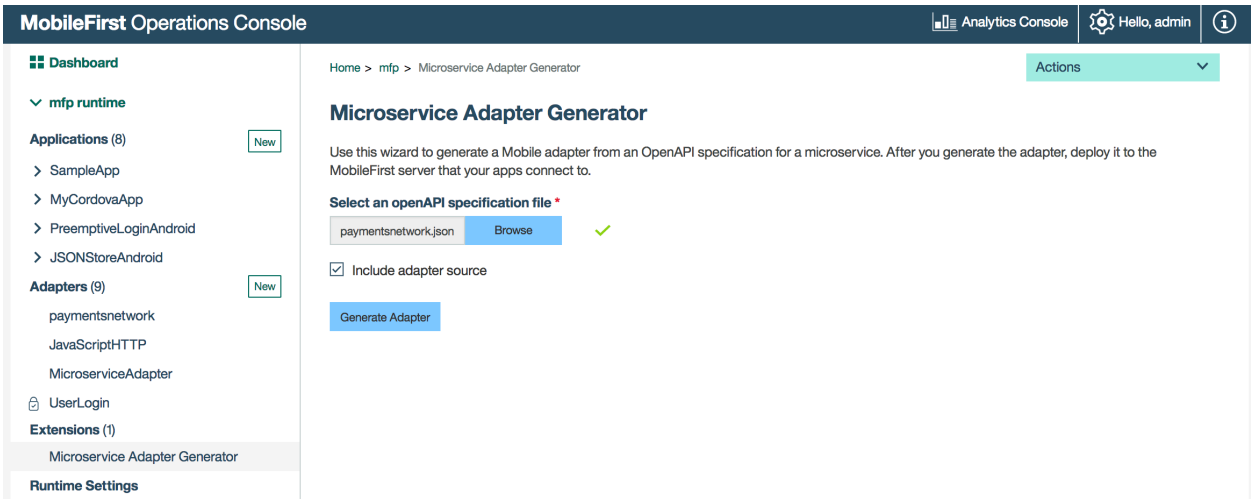
We will provide the Swagger file we saved in Step 3f to the Adapter Generator which will produce a MobileFirst adapter for the app to connect to.

e. Click on Extensions > Microservice Adapter Generator in the left pane

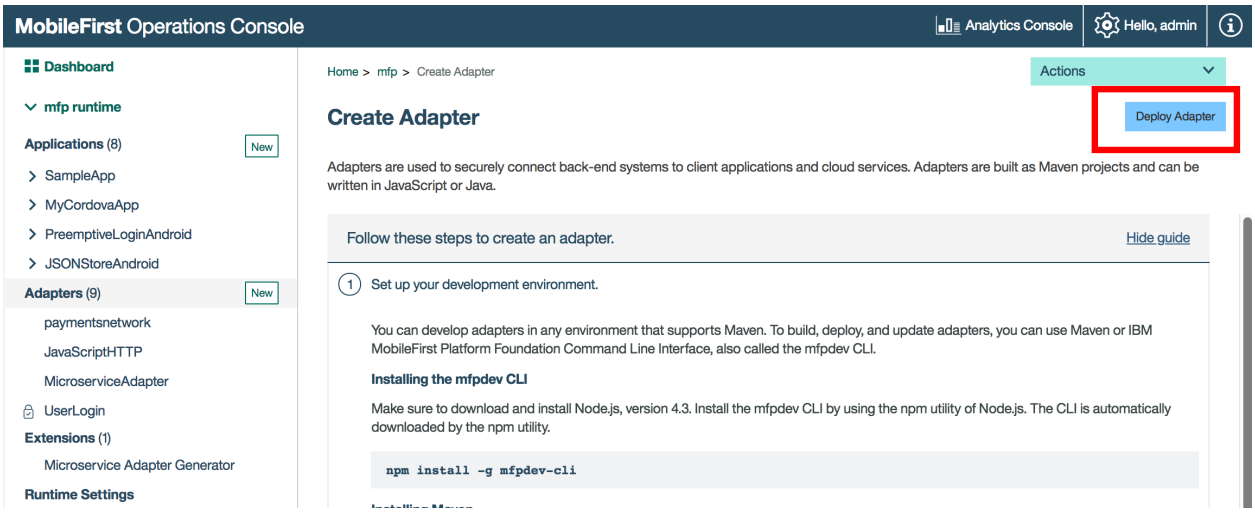


f. Select the PaymentNetwork.json file from /work/lab9603/Lab9603. Select the "Include adapter source" check box. Click "Generate Adapter"

This will take some time to generate the adapter and the adapter will be downloaded.



g. Now, we have an auto-generated adapter for the Hyperledger network we created. Time to deploy it
Click on the New button next to Adapters on the left pane
Click on Deploy Adapter button



h. Navigate to the PaymentNetwork/generatedAdapter/adapter/target folder. Choose the PaymentNetwork.adapter file to deploy it.

i. Click on New Application. Register an application with the following information
Application Name – PaymentsApp
Platform – Android
Package – com.ibm.paymentssample
Version – 1.0

j. Click on New Adapter. Upload the adapter from /work/lab9603/Lab9603/UserLogin.adapter.
This is a sample adapter to validate user credentials.

Your MobileFirst server configuration is ready !

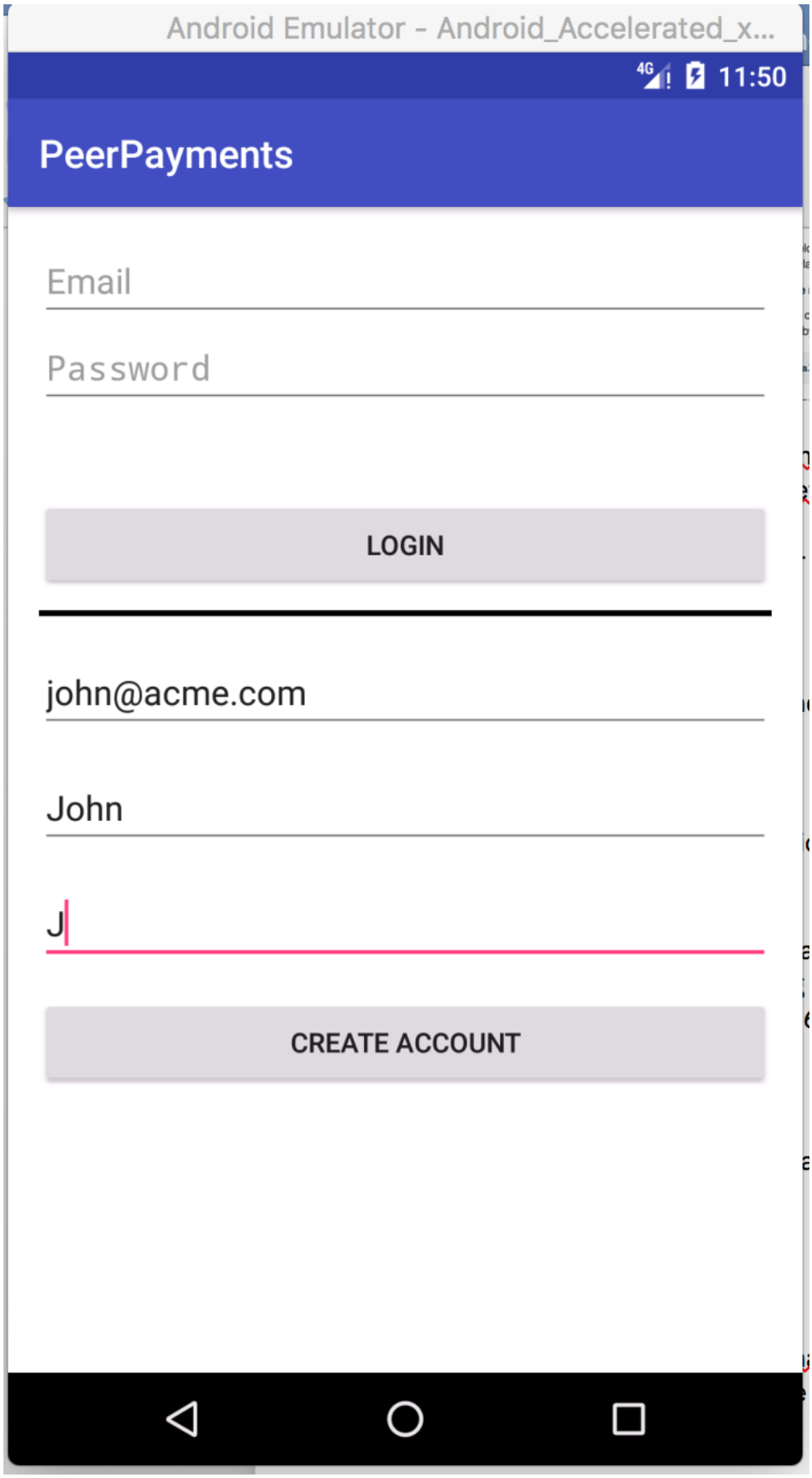
5. Run the app

The next step is to build and run a mobile app that can participate in the Blockchain network

a. Open Android Studio

```
cd /work/android-studio/bin
./studio.sh
```

b. Close open projects, if any
c. Click “Import Project (Eclipse ADT, Gradle etc.)”
d. Navigate to /work/lab9603/Think-Lab9603/mobile-app and open the project PaymentsSample
e. Run the project. You will see the screen as seen below


Android Emulator - Android_Accelerated_x...
11:50
PeerPayments
Email
Password
LOGIN
john@acme.com
John
J
CREATE ACCOUNT

f. Register a new user. You will see the wallet is pre-loaded with $100 credit. Since there are no other users on the network, you will not be able to transfer money.
g. Close the app. Run it again from Android Studio.
   Register as another user.
   This time you will see the option to transfer money. Provide an amount and click on "Transfer Money"
   You will see the balance being updated. You can verify the transfer by closing the app and again login as the user to whom money was transferred.

   The transfer of money is initiated as a transaction to the blockchain from a Mobile device.

Next Steps

a. Explore the various security & application management features of IBM Mobile Foundation such as
   a. Remote disabling of an app
   b. Blocking of specific devices
   c. Application authenticity (to prevent fake apps / malware from accessing the Hyperledger backend)
   d. Protecting each operation by security checks

   And many more...

   See https://mobilefirstplatform.ibmcloud.com/features/

We Value Your Feedback!

- Don’t forget to submit your Think 2018 session and speaker feedback! Your feedback is very important to us – we use it to continually improve the conference.
- Access the Think 2018 agenda tool to quickly submit your surveys from your smartphone, laptop or conference kiosk.