# CST4125
# Blockchain Development
# Week 1

Dr Ian Mitchell

## 1 Linux

20-25

If using another operating system create a virtual machine with Ubuntu. If you are already using Linux then you should not need to do anything. Much of what we do will be based on Ubuntu 18.04 LTS (64 bit).

This week we are going to look at the virtual environment for linux. Install Oracle's Virtual Box (see `https://www.youtube.com/watch?v=EOibXehwYWE` for MS Windows installation). Then download the virtual machine from Smerf.net - this will take 15-30mins depending on your connection strength and bandwidth - and click on the zip link. Decompress this file and make sure you have 20Gb of hard drive space.

All development will take place in this environment. Get the CST4125VM working as a guest in Virtual Box. The password is '**4125**'.

# 2 Presentation

40-50

In each subsection below are some questions. Each of these questions will require a slide and someone to present them at the end of the workshop. Much of the information is in Yaga's *et al* [3] review of blockchain technology.

Your presentation should be conducted as a group, include slides and be 5-8 minutes long.

## 2.1 Blockchain

What is blockchain? Create a slide that explains what blockchain does?

## 2.2 Blockchain Anatomy

Identify the components of blockchain. Create a slide that briefly explains the components of blockchain.

## 2.3 Blockchain Types

Identify the types of blockchain and how they differ. Create a slide that explains the types of blockchain.

## 2.4 Immutability

Explain how immutability is achieved in blockchain. Create a slide that explains the concept?

## 2.5 Inappropriate Blockchains

Explain when and why applications are inappropriate for blockchain. Create a slide and think of some important aspects or characteristics of a system that is not conducive to blockchain technology.

# 3 Blockchain Applicability

The understanding of blockchain technology is important. Once a key grasp of the essentials is understood, the next question is do I need a blockchain? This is not to be confused with Feasibility, this is Applicability.

## 3.1 Case Study 1 - Chain of franchised Pizza Restaurants

20-25

There is a company that franchises its restaurants and takeaway outlets across the country. In a single day the company can receive between 4-–5000 orders nationwide. The company pride themselves with delivering pizzas in a guaranteed time and issue financial bonuses to franchises that meet delivery times. The company want to monitor the franchises to see when they receive an order, prepare an order, transport an order, deliver an order and receive feedback on an order. The issue is trust, the company currently have a database to complete the auditing but distrust the franchise partners with the entering of data. Case Study 1 explains more details about the franchises, read this and discuss if blockchain technology is applicable as a business solution. To help your argumentation it is recommended to use Scriber's Blockchain Applicability Framework [2] and [3] flowchart.

### Case Study 1: Pizza Restaurant Chain

Ordering a pizza is a linear process and follows the 5 processes below:

**Order** : placing an order, note that no franchise can create an order, only read, update and cancel the order.

**Preparation** : Once the order has been created there is a simple process of preparing the order to meet the customer's request.

**Dispatch** : Once the preparation is completed, the order is then dispatched, or the customer is notified of the completion of their order and is now ready for collection.

**Delivered** : Once the order is

**Feedback** : Once the delivery and consumption is complete the customer is asked to respond to some simple questions for futuer quality improvement

There is a guarantee that each order is delivered in a timeframe. The rules for this timeframe are as follows:

- Delivery process should be completed in 25 mins for all delivery addresses in a 5Km radius.
- Delivery process should be completed in 40 mins for all delivery addresses in peak times, this is identified by the amount of orders received. When the number of pending orders at a single franchise outlet exceeds 20.
- Delivery process should be completed in 45 mins for all delivery addresses in a 10Km radius.
- No deliveries beyond 10 Km.
- The preparation for all orders should be prepared in 15mins for all orders.
- During peak times all orders should be prepared in 30mins.

## 3.2 Case Study 2 - School Register

15-20

A school has 450-500 pupils between ages 5-10 years old. It has been having issues with attendance. Currently, this is completed every morning and after lunch and entered on a database. The school are worried about their data and need security and looking at alternative technologies.

Case Study 2 explains more details about the franchises, read this and discuss if blockchain technology is applicable as a business solution. To help your argumentation it is recommended to use Scriber's Blockchain Applicability Framework [2] and [3] flowchart.

**Case Study 2: School Register**

For many years a primary school (age 5-10) has been using a database to record the attendance of children. May 2017 saw the introduction of GDPR [1], whilst this was many years ago, staff are concerned about the security of data on such registers.
This is how the registers are implemented:

- In the morning before the first lesson a register is taken for the class.
- The teacher calls out the names of the pupils and if present the teacher enters a 'yes'. If the student is absent a 'no' is entered.
- This process is repeated after lunch.
- The database is stored locally and accessed via online networked laptop.
- The database is MySQL.

# 4 Reflections

5-10

1. Explain the difference between permissioned and permissionless blockchain technologies.
2. Why are consensus algorithms required in blockchain technologies?
3. Explain the difference between non-incentivised and incentivised consensus algorithms.
4. What is the difference between crash fault-tolerant and byzantine fault-tolerant blockchain techonologies.
5. Give an example of permissioned blockchain?
6. Give an example of permissionless blockchain?

# 5 Further Reading

There are many areas for reading for blockchain technologies and it depends on what area you are interested. The best start is NIST Blockchain review [3]. Despite its age, this gives an overview of the technology and supporting components.

# References

[1] European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council*. of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88, May 4, 2016. URL: https://data.europa.eu/eli/reg/2016/679/oj (visited on 04/13/2023).

[2] Brian A Scriber. "A framework for determining blockchain applicability". In: *IEEE Software* 35.4 (2018), pp. 70–77.

[3] Dylan Yaga et al. *Blockchain technology overview*. Tech. rep. National Institute of Standards and Technology, 2018.

# Acronyms

**LTS** Long Term Support. 1

**NIST** National Institute of Standards and Technology. 5