FUTUREquipped

ICT Sector

Ethical considerations for programmers of SMART Home devices

UNIT 3

Funded by:

Scottish Funding Council
Promoting further and higher education

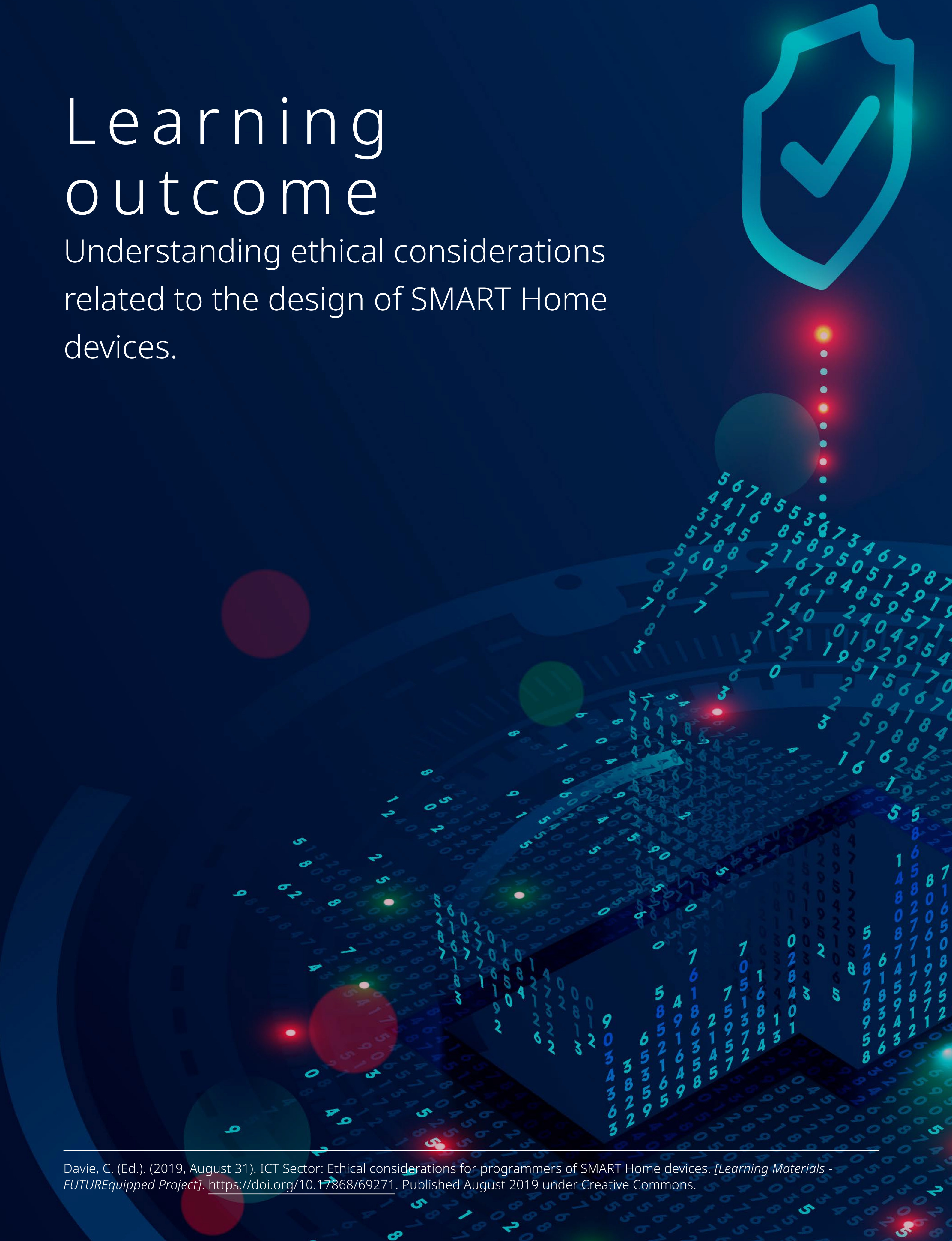
Designed and delivered in collaboration by:

CONSTRUCTION SCOTLAND INNOVATION CENTRE

DIGITAL HEALTH & CARE INSTITUTE

Learning outcome

Understanding ethical considerations related to the design of SMART Home devices.



Davie, C. (Ed.). (2019, August 31). ICT Sector: Ethical considerations for programmers of SMART Home devices. *[Learning Materials - FUTUREquipped Project]*. https://doi.org/10.17868/69271. Published August 2019 under Creative Commons.

Ethical considerations for programmers of SMART Home devices

Introduction

When considering the creation of software to interface with SMART Home sensors and human occupants there has been much thought given to the technical aspect of software development. But these technologies are bringing us into a reality which has only previously been in the realm of science fiction.   With this new ground brings new considerations such as what data is captured, for what purpose and is accessible to whom.

In this piece of learning you will begin to explore the implications of the technology being created and work with others to discuss the impact your software could potentially have on the individual and society. This learning unit will introduce you to topics which will help you create software solutions that are both technically, legally and morally sound.

Key drivers for the emergence of ethical considerations for programmers, now and in the future

Software to monitor safety and health systems within a SMART Home setting is not a new idea, but the rapid expansion of SMART Home technology means that there will be more segments of society exposed to these technologies and a wider range of software developers will be creating solutions using these technologies so therefore need to address important ethical issues.

Ethics is a large topic and this micro-learning piece is intended as in introduction to the types of issues facing software developers of SMART Home technologies in order to encourage debate and further investigation by the learner.

Ethical Considerations

1 - Code bugs

Software is now so large and complex that is unreasonable to expect that released software is 100% free from error. Software bugs are not viruses but small errors in code that produce undesired or unpredictable results. Bugs are often found during testing and either corrected or flagged for correction at a later date. Some small, harmless bugs may be acceptable in certain situations as long as they do not interfere with the correct performance of the software. However, what about bugs that are not harmless? Insufficiently or incorrectly tested software can result in deadly consequences when applied in health care situations. For example, incorrect calculations can lead to incorrect medicine being dispensed or warning systems not being triggered appropriately. These sorts of mistakes can be made by very small errors in the code. Software development companies need to ensure that software used in these settings must be robust, reliable and safe for the user.

2 - Privacy - Data and Physical

A current trend in technology, is a move towards free services or low cost components and the company makes money off the database instead. Companies such as Facebook have already shown there is money to be made out of monetising data gathered from ‘free’ services. As more people, devices, sensors and wearables are connected, the greater the amount of data collected and the greater the risk of data being misused.

2 - cont

In the context of SMART Homes for enhancing health care, there must also be a balance between protection and privacy of the individual in relation to the physical kit used inside the house. Developers must ensure that systems are designed in such a way that individuals are in control of what is being shared at all times. For example, a CCTV system that has a physical shutter on the lens that cannot be overridden by software.

3 - Data / Cyber Security

The amount of data available in a SMART Home setting is very attractive to criminals looking to steal information or hold it to ransom. Security must be at the core of all stages of software development rather than something that is checked later. In current application of smart devices in the home it is not uncommon for devices such as cameras or televisions to have default admin accounts that are the same for every single unit. Few users bother to change these, and this can leave a huge vulnerability in an interconnected system. It is essential that devices intended for health application do not have these vulnerabilities. Data should be validated at key points in the transmission chain. All data being passed between systems should also be encrypted so that the data cannot be used in the event of a data breach.

Key players in ethical considerations for programmers

- Government – adaption and creation of appropriate legislation to ensure safety and privacy of citizens, growing pressures of aging population.
- Health boards – gaining access to information to allow personalised health care whilst minimising the costs of visits, tests, appointments etc.
- Care receiver – desire to maintain independence and take control of own health destiny
- Care givers – technology giving them the ability to provide better care and priorities areas where technology cannot help as much.
- Families of care receivers – desire to be better informed of relative's care.
- Technology companies – emergence of new market allows for benefits of being early adopters in the market and therefore brings associated business benefits.

Which Scottish Innovation centre is most closely linked to this theme?

The Centre for Sensor and Imaging System (CENSIS) would be linked to this theme as their remit covers the actual hardware and software involved in the sensor data collection.

The Data Lab would also be linked to this since they look at the analysis and use of data collected. They would be relevant to the theme of data ownership and usage.

The Digital Health & Care Institute (DHI) would be linked because they are currently embedding consent-driven, methods into the way digital health and care services are designed, helping users own and control their own data.

Key challenges and opportunities for the development / adoption / progress

- Opportunity – emerging technologies such as AI have a real and exciting application in this field.
- Challenge – existing bad press regarding data theft and misuse of personal data shared with organisations.
- Challenge – multiple platforms and manufacturers means that there can be compatibility issues.
- Challenge – lack of public trust in data collection may be a barrier to participation.
- The NHS governance and regulatory methods create a high trust bar for clinicians to be able to use data from devices. This is particularly hard when the NHS does not deploy and control the device. The overall system may have a hard time trusting SMART Home data for clinical decision making purposes.

Case study

highlighting best practice and emergent trends

Blockchain as a solution to data security

Blockchain has seen its popularity rise due to its application in cryptocurrencies such as Bitcoin. But this technology such can have a positive impact on the storage and distribution of sensitive healthcare information. In simple terms a blockchain is a distributed database that is spread over a number of computers and can only be changed or accessed by someone who has special cryptographic key. There can be different keys for different types of access. Data is stored in a specific chronological manner which means it is reliable and complete, as well as secure. Blockchains may be public or private depending on the level of trust between accessing parties.

Blockchain is already gaining popularity outside of cryptocurrency and its use is growing within the Internet of Everything (IoE). The Brooklyn Microgrid is a current project that allows businesses and individuals with excess energy from solar panels to trade green electricity without the need for third parties. The transactions are managed by blockchain technology which allows the system to be run in a cost effective and secure/fraud resistant manner. This has the potential to revolutionise the way that a community can take charge of its own power needs and interaction/dependency on utility firms. This also highlights the benefits and success of blockchain technology allowing individuals to take charge of their own data and its use.

Points to Discuss:

1. What are the advantages and disadvantages of data subjects taking responsibility for their own health care information?
2. What are the implications for the size of data and processing speed of a blockchain?
3. Who is responsible for managing a blockchain?

What is Blockchain Technology? Easy To Understand Video (Blockgeeks, 2018)

STUDY ROOM
LIVING ROOM
DINING ROOM
DEPOSIT
LAUNDRY ROOM
KITCHEN
HOUSEKEEPING ROOM
FA

Assessment 1

Multiple Choice Assessment

1. ***What should programmers consider when creating software to ensure it is ethical?***

a. The user's ability to operate the software program.
b. What data is captured, for what purpose and is accessible to whom.
c. The cost of design and writing the software program.
d. The hardware on which the program will run.

2. ***In relation to coding bugs what should software development companies ensure?***

a. That software is 100% free from error.
b. They ignore bugs are often found during testing.
c. They limit focus on testing.
d. That software used in these settings is robust, reliable and safe for the user.

3. ***Companies such as Facebook can monetise data by:***

a. selling wearable and sensors.
b. selling data gathered from 'free' services.
c. limiting data sharing.
d. minimising the amount of data gathered.

4. ***Software developers can aid privacy for the physical kit used by:***

a. writing code to ensure individuals are in control of what is being shared at all times.
b. limiting the users control over access.
c. ensuring the physical kit can be overridden.
d. ensuring the user has no control over access.

5. ***It is not uncommon for devices such as cameras or TV's to have default admin. Software developers should: (Select two options)***

a. ensure default admin cannot be changed.
b. ensure validation is added at key points in the transmission chain.
c. only the manufacture of the device can change default admin.
d. all data being passed between systems is encrypted so that the data cannot be used in the event of a data breach.

6. ***Which of the following is NOT a key player in Ethical considerations for programmers?***

a. Technology companies
b. Government
c. Retail industry
d. Health boards

7. ***Blockchain is a distributed spreadsheet that is spread over a number of computers.***

a. True
b. False

8. ***Data transferred using blockchain***

a. can be changed or accessed by anyone.
b. is not a popular method of data transfer.
c. is not a secure method of data transfer.
d. can only be changed or accessed by someone who has special cryptographic key.

9. There can be different levels of blockchain access

a. True
b. False

10. Who owns a blockchain?

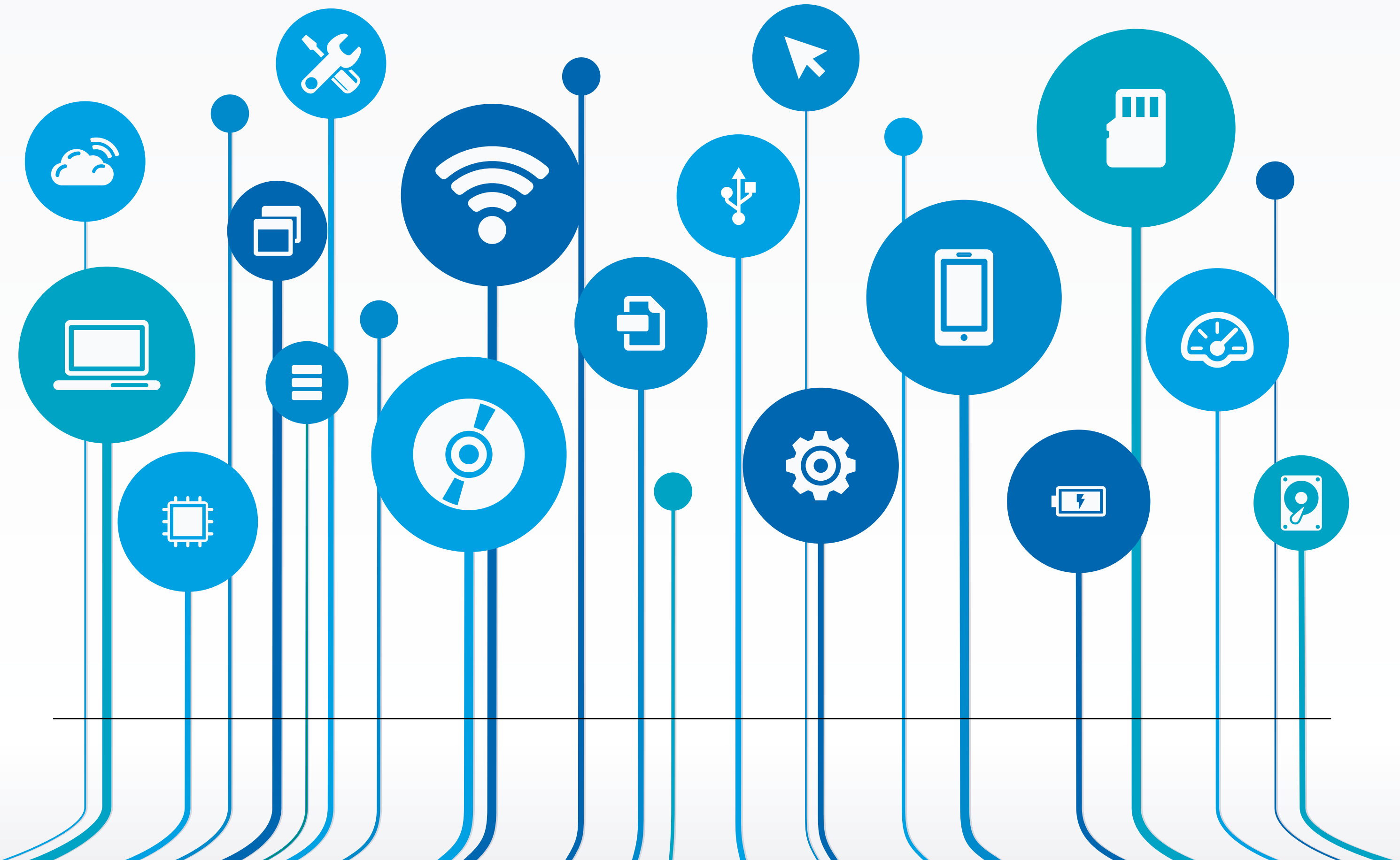
a. Shared ownership.
b. The company who administers the blockchain technology.
c. The recipient of the blockchain.
d. The individual who sends the blockchain.

Assessment 2

Project Based Assessment

Falling is an expensive health care issue for the NHS costing over £2bn and 4 million bed days per year. SMART Homes can be equipped with sensors that can detect a fall and also use data analytics to predict future falls.

1. Discuss what sensitive information could be shared using blockchain technology to provide the relevant care givers the information needed to provide care in the in the event of a fall.
2. What should software testers consider when creating test plans for such a system?
3. How could the analytics of the fall detection system be used?



Assessment 1 Answers

1 b. What data is captured, for what purpose and is accessible to whom.

2 d. That software used in these settings is robust, reliable and safe for the user.

3 b. selling data gathered from 'free' services.

4 a. writing code to ensure individuals are in control of what is being shared at all times.

5 b. ensure validation is added at key points in the transmission chain.

d. all data being passed between systems is encrypted so that the data cannot be used in the event of a data breach.

6 c. Retail industry

7 b. False

8 d. can only be changed or accessed by someone who has special cryptographic key.

9 a. True

10 a. Shared ownership

These materials were produced by college lecturers as part of the FUTUREquipped project in 2018. The project was funded by the Scottish Funding Council and designed and delivered in collaboration by the Digital Health and Care Institute and the Construction Scotland Innovation Centre.

Digital Assets

What is Blockchain Technology? Easy To Understand Video https://www.youtube.com/watch?v=27nS3p2i_3g

What is BLOCKCHAIN? The best explanation of blockchain technology

https://www.youtube.com/watch?v=3xGLc-zz9cA

References:

Linforth, P. (2019). Data Security. [image] Available at: https://pixabay.com/illustrations/data-security-cyber-digital-3970343/ [Accessed 12 Apr. 2019].

Linforth, P. (2018). Blockchain. [image] Available at: https://pixabay.com/illustrations/blockchain-technology-exchange-3438501/ [Accessed 12 Apr. 2019].

Blockgeeks (2018). What is Blockchain Technology? Easy To Understand Video. [video] Available at: https://www.youtube.com/watch?v=27nS3p2i_3g [Accessed 12 Apr. 2019].

Mostazo, L. (2018). What is BLOCKCHAIN? The best explanation of blockchain technology. [video] Available at: https://www.youtube.com/watch?v=3xGLc-zz9cA [Accessed 31 Mar. 2019].