

# Blockchain application and IoT device

Hew, Guo Wei

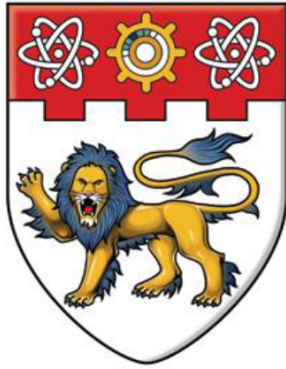
2019

<http://hdl.handle.net/10356/78968>

---

Nanyang Technological University

*Downloaded on 03 Sep 2023 15:36:10 SGT*



**NANYANG**  
**TECHNOLOGICAL**  
**UNIVERSITY**

---

## Final Year Project

### **Blockchain Application and IoT device**

Author: HEW GUO WEI, U1622752K

Supervisor: Prof Dusit Niyato

Examiner: A/P Anupam Chattopadhyay

Project ID: SCSE18-0692

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING  
NANYANG TECHNOLOGICAL UNIVERSITY

## Abstract

Both blockchain and Internet of Things (IoT) have been the buzz words in the recent years and are the driving force in the new Industrial Revolution 4.0 [1]. Between IoT and Blockchain there lies a huge potential and a very positive outlook [2]. They have been explored and studied on, leading to the emergence of platforms like Chainlink, that aims to combine the real world event data with blockchain technology.

This paper describes the problem of today's centralized system and explores the option of utilizing a decentralized one like Interplanetary File System (IPFS) and blockchain. As a demonstration of adoption of blockchain on IoT, a Decentralized Application (Dapp) is developed to retrieve health-related data from a wearable device, Fitbit and to store the data on IPFS with its cryptographic hash stored to Ethereum blockchain.

## Acknowledgements

I would like to express my gratitude towards my supervisor, Prof Dusit Niyato for whenever I had doubts, he would not hesitate to arrange a meet-up with me to clear them and for the amount of freedom given to me to develop something I was passionate about. Besides, I would also like to extend my appreciation to all those Blockchain enthusiasts who contributed to the open source Ethereum projects and documentations as well as countless online tutorials that assisted me in my understandings towards the fundamentals of the blockchain technology and the development of decentralized applications (Dapps).

HEW GUO WEI

OCT 2019

# Table of Contents

<i>Abstract.....</i>	<i>2</i>
<i>Acknowledgements .....</i>	<i>3</i>
<i>Table of Contents .....</i>	<i>4</i>
<i>List of figures .....</i>	<i>5</i>
<i>Chapter 1 – Introduction .....</i>	<i>6</i>
1.1 Motivation.....	6
1.2 Objective and Scope.....	7
<i>Chapter 2 – Background.....</i>	<i>8</i>
2.1 Internet of Things .....	8
2.2 Centralized System .....	9
2.3 Decentralized System .....	10
2.4 Interplanetary File System (IPFS).....	10
2.4.1 Limitation of IPFS .....	11
2.5 Blockchain.....	12
2.5.1 Limitation and Potential threats .....	13
2.6 Blockchain with IPFS .....	14
<i>Chapter 3 – Implementation .....</i>	<i>15</i>
3.1 Decentralized application (Dapp) .....	15
3.2 Use Case Diagram.....	17
3.3 Development tools.....	17
3.4 Configuration: .....	18
3.5 Smart Contract Deployment.....	19
3.6 Demonstration of application workflow .....	20
3.7 Data Privacy .....	24
<i>Chapter 4 -- Conclusion.....</i>	<i>26</i>
4.1 Evaluation.....	26
4.2 Future work .....	26
4.3 Final words .....	27
<i>Bibliography.....</i>	<i>28</i>

## List of figures

Figure 1 Blockchain

Figure 2 Use case diagram

Figure 3 Smart contract

Figure 4 Home page

Figure 5 Public key

Figure 6 Log in

Figure 7 Input date

Figure 8 Retrieved Page

Figure 9 Uploading data

Figure 10 Display stored data

Figure 11 View health status

Figure 12 Share button

Figure 13 Blockchain input data

Figure 14 Readable Text

Figure 15 Unreadable Text

# Chapter 1 – Introduction

## 1.1 Motivation

Data has been a very key element of the Big Data era and it is one of the key features behind the Industrial Revolution 4.0. While the amount of data is increasing at an astonishing rate, the topic on how to manage our data has become a very tough one that we should spend time studying.[4] Managing data in the centralized way we are used to, has put us down several times in the history given the notorious data privacy scandals that happened in the past few years. Even the tech giant Google who generally has a better company image, was caught covering a potential data breach that could affect 500000 users on the Google Plus network [3]. Hence, it is worth studying a decentralized system that could serve as an alternative.

The blockchain technology has become relevant when it comes to decentralization of the internet. It has been under the spotlight in the recent years with cryptocurrency being the most frequently targeted use case of blockchain as well as criticism and regulations from various governments. Despite being a more secure technology, the adoption of blockchain is still considerably low to current's date while the users' scope on the blockchain technology is still very limited to only the cryptocurrency. Hence, there is a demand to study how we can implement a secure connection between blockchain and the real-world events. Internet of Things (IoT) being the device that humans interact with for a big portion of their time, has a significant role to play when we want to integrate blockchain into our everyday life.

## 1.2 Objective and Scope

This paper first studies the difference between a decentralized system and a centralized system. It then explains about blockchain technology as well as the IPFS network and explores how it can be used to serve as a better alternative to today's centralized internet.

In this project, a decentralized application (Dapp) is developed using the Ethereum build-tools like Geth console, Solidity, Web3 library, Remix IDE etc. The Dapp runs on a local private chain. A Fitbit device is used too, to demonstrate how we can extract health-related information from a IoT device and use it on blockchain. In addition, the Dapp is also extended to include more functionality to explore the possibilities of the technology. Cryptography algorithm (asymmetric encryption) is mentioned in this paper as well, to increase the data security on blockchain.

The objective of the demonstration is to show how a Dapp can be easily incorporated into everyday life just like a conventional app. The adoption of Dapp does not serve as a replacement of the current technology, as it may still have its flaws, especially in the area of efficiency and cost, but as a way to improve some of the problems that we are facing in the current centralized and controlled internet.



## Chapter 2 – Background

### 2.1 Internet of Things

The Internet of Things, IoT refers to the billions of devices connected to the internet, to share and receive information.[5] It goes without saying that data is an important element that helps in research, innovation and optimizing solutions. Wearable devices, like Fitbit are part of the IoT network. In the case of Fitbit, cloud service is used to store the health-related data of a user and it can be used to retrieve the data elsewhere.

The adoption of wearable devices has its implications in the health industry. Wearable devices that have sensors monitoring the hearts' pump rates are useful for doctors to detect any early symptoms of heart failures, thereby granting patients the chance of an early treatment like a change in medication, a change in diet or a clinic visit, before anything worse happens. [6]

However, the security of IoT devices are often not paid much attention to and several security issues have happened in the past. A malware Mirai [7] was able to hijack into home devices like toasters, web-cameras to issue distributed denial of service (DDoS) attacks or even mine bitcoin transactions. Hence, due to the insecure nature of IoT device, care should be taken when integrating IoT device with blockchain.

## 2.2 Centralized System

A centralized system is one with a single server that operates as the main processing node that handles all the requests. The central processing nature allows it to be very efficient, consistent and affordable.[8] Most of the networks today most or less operate as, or close to a centralized system due to its lower cost and higher efficiency.

Cloud storage providers like Amazon Web Service, Microsoft Azure, Google cloud all provide not just normal users, but also professional developers, with a better working platform that allows them to work with each other smoothly and smartly.

However, there is always a grey area where users would not know or sometimes rather not bothered to find out if their data is securely maintained. Even when encrypted, there often exists key-management issues while a zero-knowledge model is often not adopted, leading to serious security breach.[11]

Centralized storage system also implies that the storage provider owns the customers' data. It is a known fact that consumers are consuming the so-called free services offered by these tech giants at the expense of their data. In the notorious Facebook-Cambridge Analytica Data Scandal [9] where users' data were harvested to affect political election, it has proven to us that tech service providers have the capability to exploit users with the data the users entrust to them.

## 2.3 Decentralized System

An alternative to a centralized storage system is a decentralized one. Decentralized system is one where there is no central processing node while every node in the network takes the responsibility of processing the communications and data is distributed among the nodes. There exists no single point of failure because in the event of one node being compromised or attacked, there are other nodes out there covering each other, maintaining the stability of the network. The 51% attack theory suggests that the hackers need to take control of at least 51% of the network/nodes to compromise the entire network. Hence, a decentralized system is resilient to attacks. [10] Decentralized storage system also transfers the ownership of data back to the owners themselves, preventing the web service providers to exploit the data and manipulate web service consumers.

## 2.4 Interplanetary File System (IPFS)

IPFS is a decentralized peer-to-peer storage network. It delegates the data storing job from one central server to the distributed network of participating nodes. It works similarly as BitTorrent where the file accessing (uploading and downloading) takes place between peer to peer instead of from a central server. In addition to hosting files, IPFS nodes are able to host websites, allowing developers to operate their websites in a decentralized way instead of relying on web service providers like AWS to offer web hosting service. This is one big leap towards liberalizing the internet from the control of tech giants.

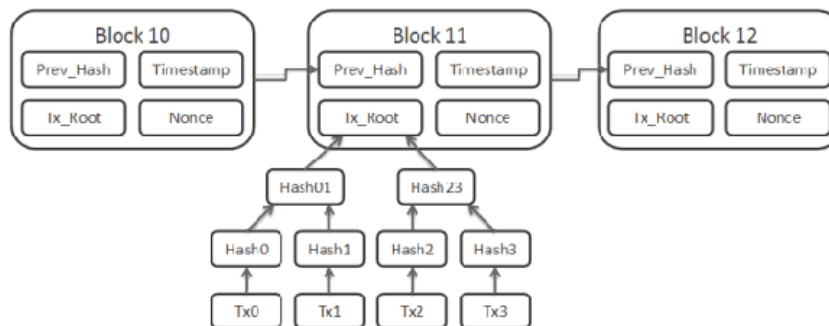
IPFS uses content addressing as opposed to location addressing used by Uniform Resource Locator (URL). This means that accessing a file on IPFS will activate the searching for the cryptographic hash that is generated based on the file content, which gives a file its unique identity. In contrast, location addressing of file content is a pain today. A recent Harvard-led study found that 49% of all hyperlinks cited in US Supreme Court opinions are no longer working today.[18] This means that the references to all these file contents have been lost with no way of retrieving them, although the content itself might still exist somewhere on the internet. Content addressing works the opposite way where as long as the file still exists, it is retrievable given its cryptographic hash.

To search for a file, a Distributed hash table (DHT) is used in IPFS. DHT is a distributed database of key to values (hash to content). In addition, IPFS adopts the Merkle-DAG (Directed Acyclic Graph) model where upon uploading a file to the network, its content is first split into blocks, meaning different blocks of a file will go to different nodes on the network, allowing faster accessing of content than when there is only one source of the file. This also prevents the nodes hosting the file to read the content since one part of the entire file will not make sense if read as only one part. This implies that only the user with the full unique cryptographic hash of the file is able to retrieve the entire content. The cryptographic hash of the content verifies that the file content is the same whenever the owner retrieves it, preserving the content integrity. [12]

### 2.4.1 Limitation of IPFS

IPFS is still at the development stage and its adoption rate is low. Currently, uploading and retrieving content from the IPFS network are mostly carried out through the IPFS public gateway [13]. Accessing a file will engage the public gateway to find the content from the network and the gateway will process it before the content is finally ready for view by the owner. This means there is a central point of possible failure. Furthermore, files on the public gateway are cleared by the garbage collector on a regular basis to free up memory, on top of the fact that there are currently not many nodes hosting the files. Although a file will never vanish on the IPFS network as long as it is pinned, the speed of accessing a file is just very slow due to these factors. Good news is that Filecoin was introduced to serve as a utility token to incentivize file hosting activities.

## 2.5 Blockchain



**Figure 1 Blockchain**

Blockchain is a decentralized, distributed ledger that stores transactions across different computers. Every block has a unique cryptographic hash that gives it an identity, and a pointer to its previous block. Hashes help verify if the blockchain adopted has been tampered, preserving the integrity of the chain. Blockchain database is autonomously managed using peer-to-peer network, giving rise to its decentralized nature. Blockchains like Bitcoin use proof-of-work as its mining mechanism to validate transactions, utilizing the token as the incentive.

Blockchain has many use cases across several different fields, such as financial service, supply chains, video games, and cryptocurrencies being the one receiving most attentions. The immutability and decentralized nature of blockchain makes it perfect to be utilized as a digital currency as it cannot be tampered and transactions can be easily verifiable.

Ethereum is an open source blockchain-based computing platform featuring smart contract functionality.[14] The beauty of executing a smart contract lies in its ability to automate the process without human intervention and a central authority to verify transactions, while still completing the tasks elegantly. Smart contract is designed to include the payable feature that makes it perfect as a platform that could facilitate any mode of financial transactions. This has led to the development of Decentralized Finance (DeFi) applications built on the smart contract, with the idea of performing tasks that a bank does, but at a much lower cost, for example, borrowing and lending at a lower interest in a Dapp named Compound.

### 2.5.1 Limitation and Potential threats

The current adoption of blockchain is very limited to only cryptocurrency for a reason. The security model of how smart contract state is secured precludes the connectivity to weaker, less secure external systems which often house a lot of event data, that is often essential in making an application a good one that goes beyond token movement.[16] There is a wide gap between blockchain technology and the data source (eg. API), that prevents the technology from being adopted for more use cases and for everyday life. Fortunately, Chainlink is built to address the demand for a secure oracle and it is on a good progress.

The Blockchain model itself is resilient to attacks but the implementation of it may not be. The infamous DAO attack is a major event that loses investors' confidence.[15] The Decentralized Autonomous Organization (DAO) is an organisation that does crowd funding through the means of the crypto tokens. The application written in smart contract had one logic error that allowed a hacker to drain tokens from the smart contract infinitely. This eventually led to a hard forking on the Ethereum blockchain, reversing the actions done (the hack). Nonetheless, this is more an error in the implementation of the technology than the flaw in the blockchain model itself, which serves as a reminder that coding on the blockchain should be handled with more care as damage done could be irreversible.

Cryptocurrencies have become a hot target for the hackers in the recent years. According to the Wall Street Journal, more than \$1.7billions have been stolen from various crypto exchanges over the years. Binance has reportedly lost \$40 millions stolen from its hot wallet, through means of virus and phishing. Yet, it is worth noting that the security breach could be attributed to poor key management while the nature of cryptocurrency is still secure. Application security is a topic that developers should be concerned with instead of the cryptography technology.

The proof of work consensus algorithm works perfectly well as a validating mechanism, but it poses several energy issues to the environment. As the difficulty of mining and receiving incentives increases over time, so does the cost of mining which translates to increase draining of energy that is bad to our environment. The several emerging consensus

algorithms such as Proof of Stake, Proof of Authority may be more efficient, but often at the expense of the degree of decentralization.

The development in quantum computing may pose threats to the public-private key pair algorithm, which is the backbone of blockchain. A quantum computer could potentially have the capacity to run a Shor's algorithm which could reverse the one-way hash function that blockchain cryptography relies heavily on, eventually breaking the blockchain model. However, quantum computing is still at the early development stage and there is still a lot of uncertainties. Should a quantum computer be developed, the primary focus would be to help strengthen the cryptography algorithm instead of breaking one, that is solving a problem instead of creating one. [17]

## 2.6 Blockchain with IPFS

The immutability nature of blockchain complements IPFS by storing the content hashes on the blockchain for easy track-keeping of the hash strings. The sole ownership of the data means that only the user with the private key can access that data. Since both are on peer-to-peer network and decentralized, they make a good combination.

Questions may arise as why not simply use blockchain as the storage system while it is a bad idea imagining every node in the blockchain network has to store duplicates of data, consuming the limited resources, like memory. For example, the size of each Fitbit API report used in application prototype developed is about 12KB, while the cost of storing 1KB of data is about 0.035ETH. This results in a cost of SGD97 for storing 12KB of data on Ethereum blockchain at the time of writing this report. [19] Hence, it is very cost ineffective to store data on blockchain. Instead, we store the IPFS hashes which help us access the actual content of a file on blockchain.

## Chapter 3 – Implementation

### 3.1 Decentralized application (Dapp)

A prototype application has been developed in conjunction with a smart contract deployed to Ethereum private local chain. Although permissioned private chain may be preferred for a storage chain that does storing of data as its main functionality, it is generally not desired as a permissioned chain requires a central authority to approve new nodes joining the network which contradicts the main purpose of blockchain where there should not be a single point of control and it should be public enough for other nodes to verify and maintain the network. Hence, private local chain was used in the demonstration solely for development purpose with the ultimate goal of deploying onto Ethereum public chain.

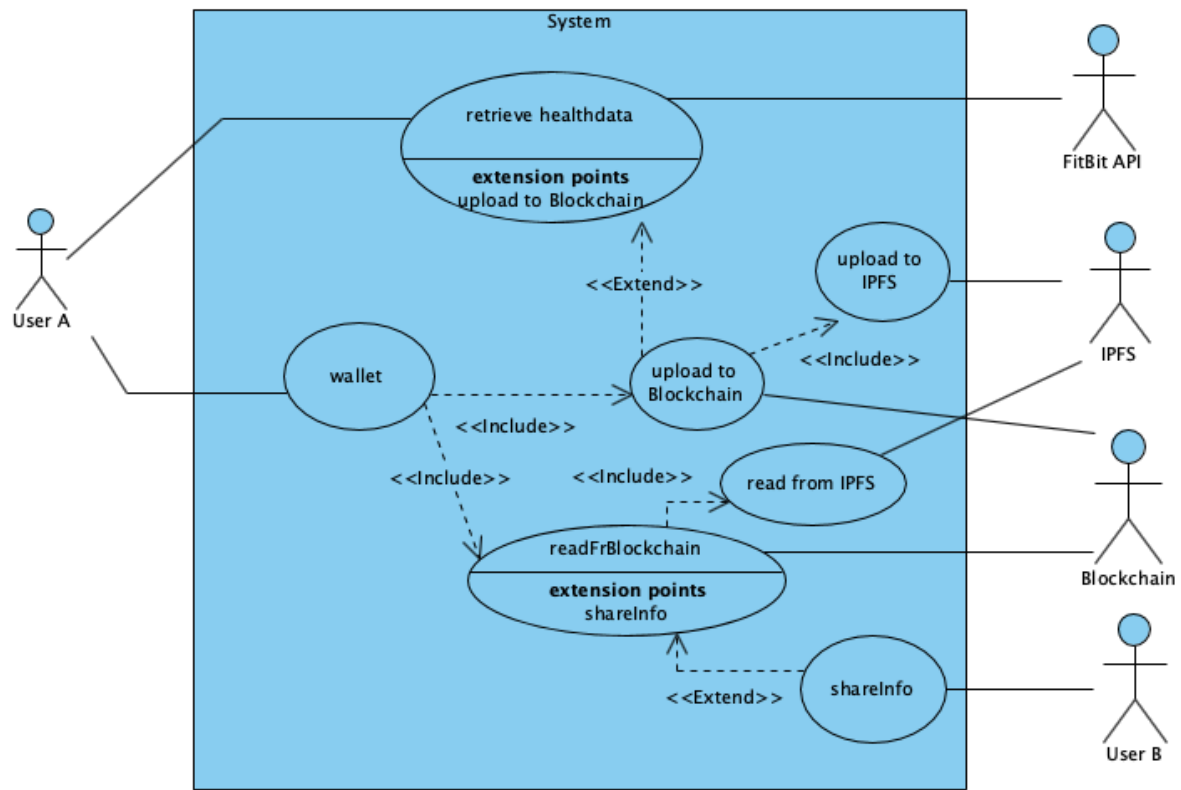
The main functionality would be allowing a user to put his/her Fitbit data on the IPFS and blockchain network. Second functionality allows the user to share his/her Fitbit data with another user, such as a family member or a doctor who needs/wants to keep track of his/her health status. The implication of this is on preventing the deterioration of any illnesses.



Below is the workflow of the application that demonstrates how we can incorporate blockchain with a IoT device:

1. Sync the Fitbit device with the Fitbit mobile app to allow updating of a user's status to the Fitbit server.
2. Using Fitbit API, fetch the data according the date input by the user.
3. Upload the json format file to IPFS network where a cryptographic hash is generated upon successful upload.
4. The hash is then encrypted with the user's public key
5. The encrypted hash is then appended to the smart contract associated with the Dapp (uploading to the blockchain) and the transaction has to be signed by the user.
6. Reading of the data requires an authenticated user (wallet signed in with the private key) with public key as the reference to which the data belongs to, in addition, a decryption using the user's private key converts the encrypted data into readable format.
7. Decrypted hash is used to access the file content on the IPFS network
8. Sharing of the data with user B like family/doctors requires user A to input the public key of user B, as the Dapp will encrypt the data with user B's public key and it can only be decrypted and read by the intended user, user B.

### 3.2 Use Case Diagram



**Figure 2 Use Case Diagram**

### 3.3 Development tools

1. Ethereum private chain + Geth interactive console
2. Web3 library for interaction between app and blockchain
3. secp256k1 library for recovering private key from keystore
4. eth-crypto library for encrypting and decrypting data
5. React JS framework for web application development
6. IPFS API for decentralized storage
7. OAuth 2.0 + Fitbit API
8. Metamask wallet

### 3.4 Configuration:

1. Set up a genesis block :

```
"nonce": "0x0000000000000042",
"mixhash": "0x0000000000000000000000000000000000000000000000000",
"difficulty": "0x20000",
"alloc": {},
"coinbase": "0x0000000000000000000000000000000000000000",
"timestamp": "0x0",
"parentHash": "0x000000000000000000000000000000000000000000000000",
"extraData": "0x",
"gasLimit": "0xffffffff",
"config": {
  "chainId": 10,
  "homesteadBlock": 0,
  "eip155Block": 0,
  "eip158Block": 0
}
```

2. Use the genesis block to generate a blockchain by typing:

```
geth --datadir "./db" init genesis.json
```

3. Run the blockchain network:

```
geth --datadir "./db" --networkid 10 --rpc --rpcport "8545" --rpccorsdomain "*"
--port 30303 --nodiscover
--rpcapi="admin,db,eth,debug,miner,net,shh,txpool,personal,web3"
```

4. To interact with the blockchain, we use geth console:

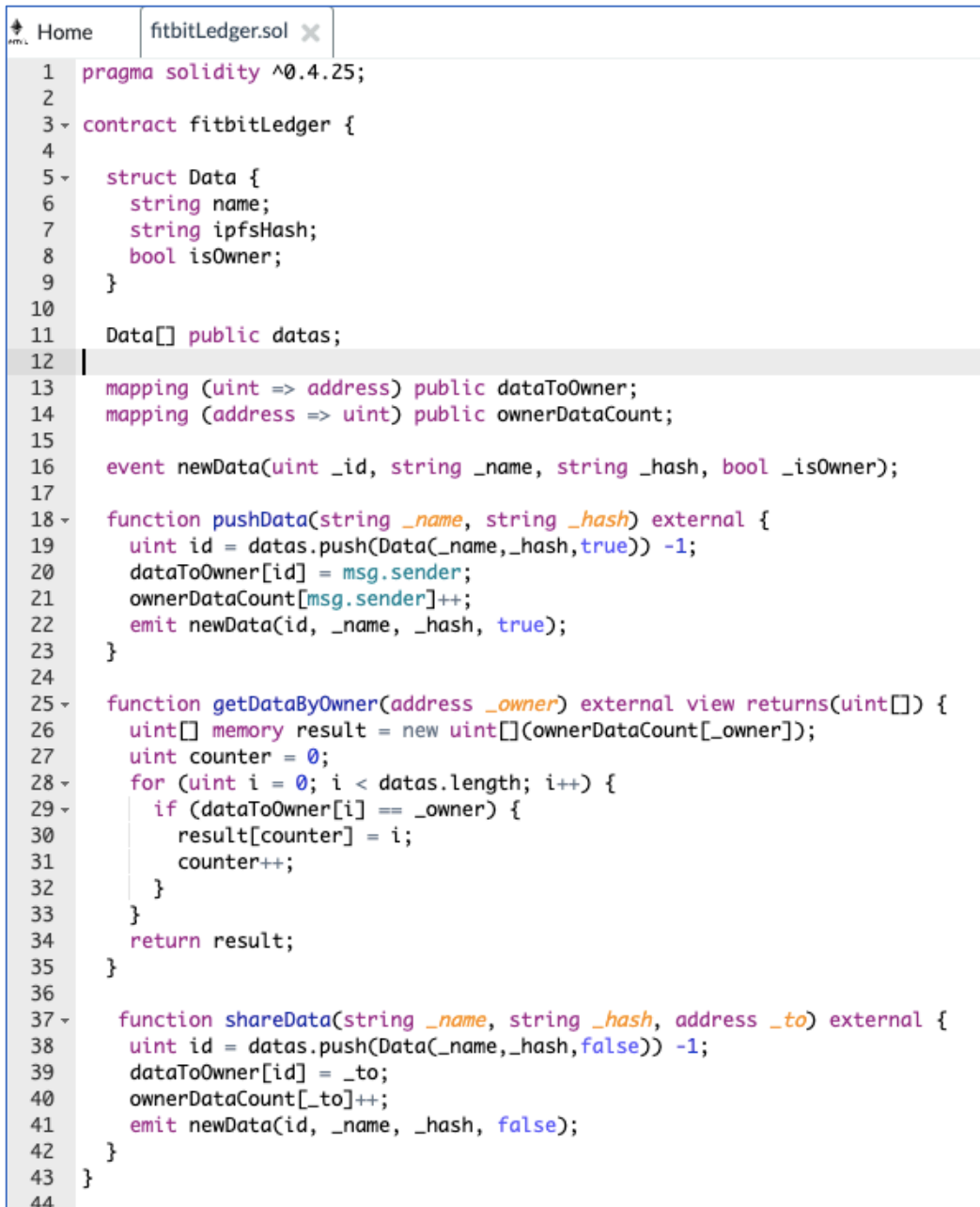
```
geth attach http://127.0.0.1:8545
```

5. The console has several library API that allows us to perform basic operations like creating accounts and signing transactions.
6. Configure metamask account to connect to the localhost:8545, so that our web browser allows interaction between the web application and the local private chain.
7. cd to the directory of our web application, run the following command to start the react-app:

```
npm start
```

8. Generate 2 accounts on the Geth console and import the 2 accounts into Metamask wallet so that we have user accounts that can interact with each in the application.
9. All transactions happening in the application (including deploying smart contract) would need mining command to be manually carried out in the Geth console.

### 3.5 Smart Contract Deployment



```
1 pragma solidity ^0.4.25;
2
3 contract fitbitLedger {
4
5     struct Data {
6         string name;
7         string ipfsHash;
8         bool isOwner;
9     }
10
11     Data[] public datas;
12
13     mapping (uint => address) public dataToOwner;
14     mapping (address => uint) public ownerDataCount;
15
16     event newData(uint _id, string _name, string _hash, bool _isOwner);
17
18     function pushData(string _name, string _hash) external {
19         uint id = datas.push(Data(_name,_hash,true)) -1;
20         dataToOwner[id] = msg.sender;
21         ownerDataCount[msg.sender]++;
22         emit newData(id, _name, _hash, true);
23     }
24
25     function getDataByOwner(address _owner) external view returns(uint[]) {
26         uint[] memory result = new uint[](ownerDataCount[_owner]);
27         uint counter = 0;
28         for (uint i = 0; i < datas.length; i++) {
29             if (dataToOwner[i] == _owner) {
30                 result[counter] = i;
31                 counter++;
32             }
33         }
34         return result;
35     }
36
37     function shareData(string _name, string _hash, address _to) external {
38         uint id = datas.push(Data(_name,_hash,false)) -1;
39         dataToOwner[id] = _to;
40         ownerDataCount[_to]++;
41         emit newData(id, _name, _hash, false);
42     }
43 }
44
```

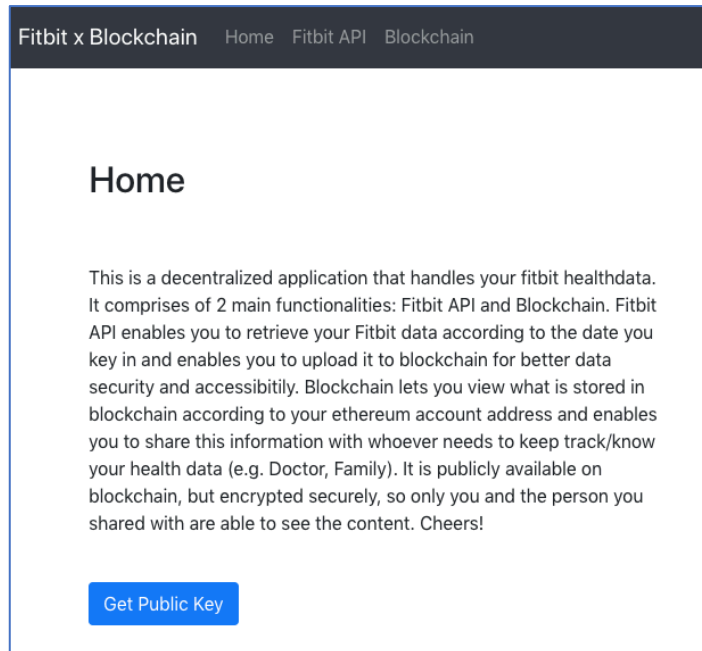
**Figure 3 Smart Contract**

A very short and simple smart contract in Solidity is written for a data storage application.

Remix is an online compiler that compiles smart contract and also offers the functionality to deploy the smart contract to whichever Ethereum chain we want, in this case, the local private chain.

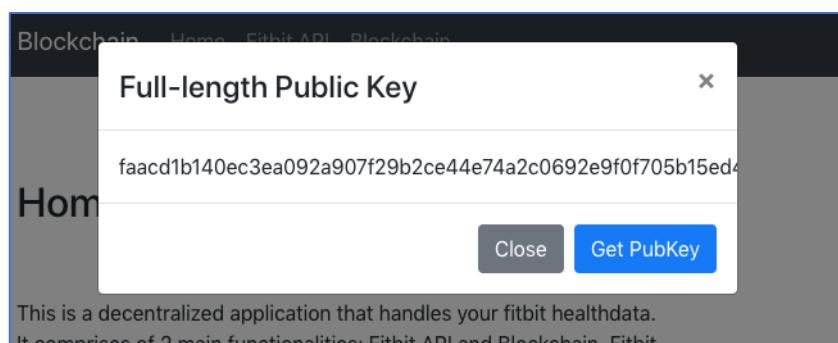
### 3.6 Demonstration of application workflow

1. The home page is an information page and has a generate public key button :



**Figure 4 Home Page**

The application allows user to retrieve the public key of the account and share it with another user for data sharing purpose:



**Figure 5 Public key**

2. The Fitbit API page requires the user to login to his/her Fitbit account using OAuth2.0 authentication:

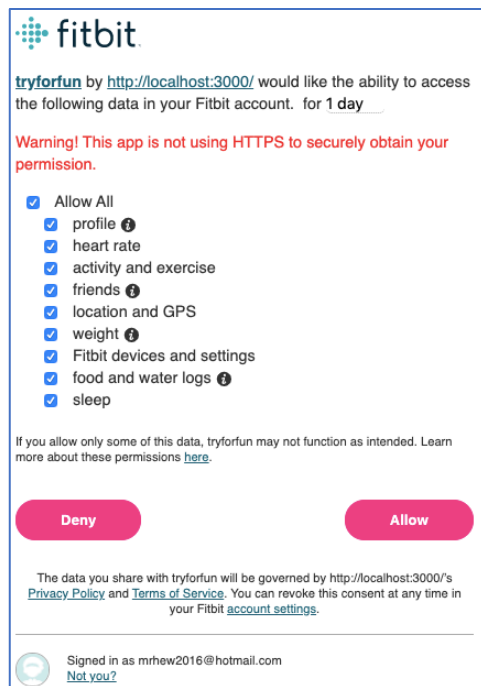


Figure 6 Log in

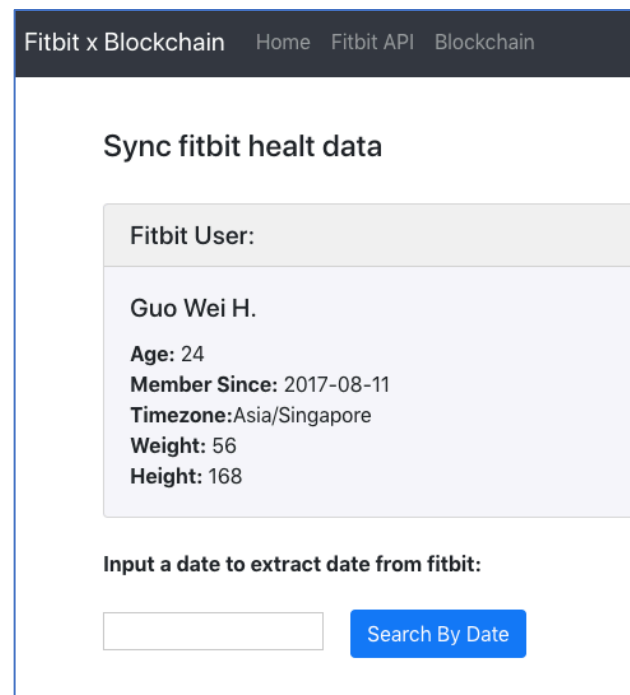


Figure 7 Input Date

A Json format data is fetched using Fitbit API according to the date input and presented:

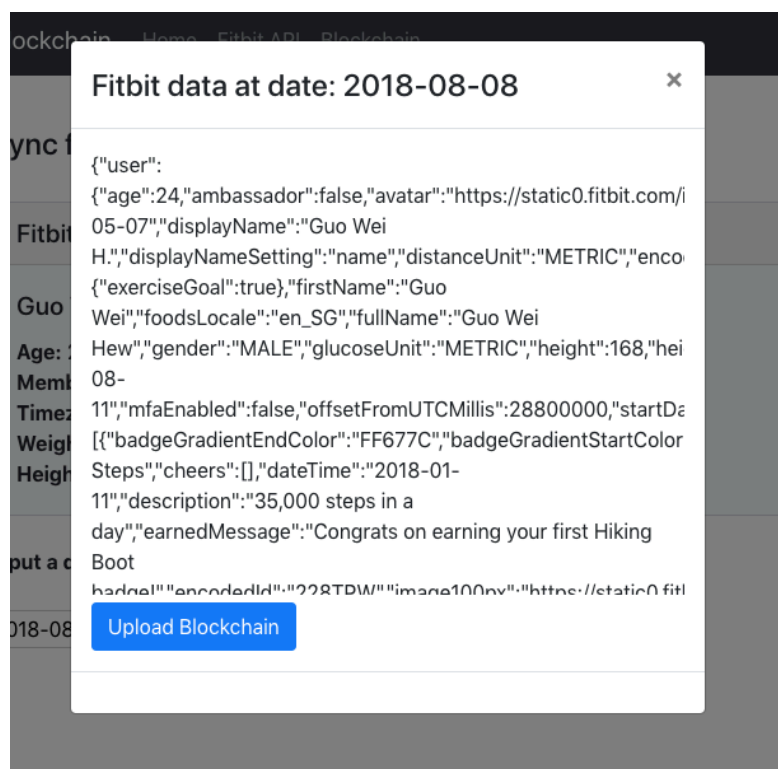
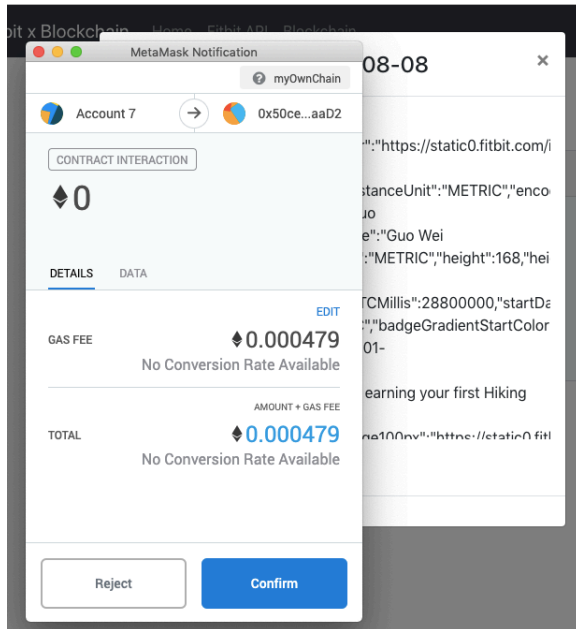


Figure 8 Retrieved Page

The upload button first uploads the file to the IPFS network, then a callback function returns a hash. The hash is encrypted using user's public key and a transaction is triggered to append the encrypted hash to smart contract on blockchain:



**Figure 9 Uploading Data**

3. The Blockchain Page displays the number of items uploaded by or shared to wallet address. All items displayed are retrieved from the blockchain, according to the user's address, and then decrypted using the user's private key to be in readable format:

Fitbit x Blockchain Home Fitbit API Blockchain		
Total num of items stored to the user's account: 5		
List of stored items owned by this account		
data name	ipfs link	
2018-12-11	QmYWhikVVPpUSaTbx7dzRAGf8sQj3xeLjr4pQ9ymtHqgvZ	<a href="#">view</a> <a href="#">share</a>
2018-05-02	QmWcP2kMkM9g3eZ19eYwDEzMdwm6CmypoNnBJXA4FCEg4	<a href="#">view</a> <a href="#">share</a>
2019-10-02	QmYoJriStX3Y7xXp83y6SMfDwGz9non2KiLnJe42u2UPwm	<a href="#">view</a> <a href="#">share</a>
2018-10-10	QmZJ9dqfQwh8SAqiiXf9uWt62GxT9VzzhH8hDzMkoyvKk	<a href="#">view</a> <a href="#">share</a>
List of stored items shared to this account		
data name	ipfs link	
2019-08-16	QmYoMEgA5gxiRWHxoGJK3zjzmtvDxRRK8YNS3aR7D16NWD	<a href="#">view</a>

**Figure 10 Display Stored Data**

The view buttons retrieves the content from IPFS using the decrypted hash key and converts the json format file into readable format content. Currently, the view function only supports certain information like the activity of the day and the amount of sleep. Future version could include more useful information:

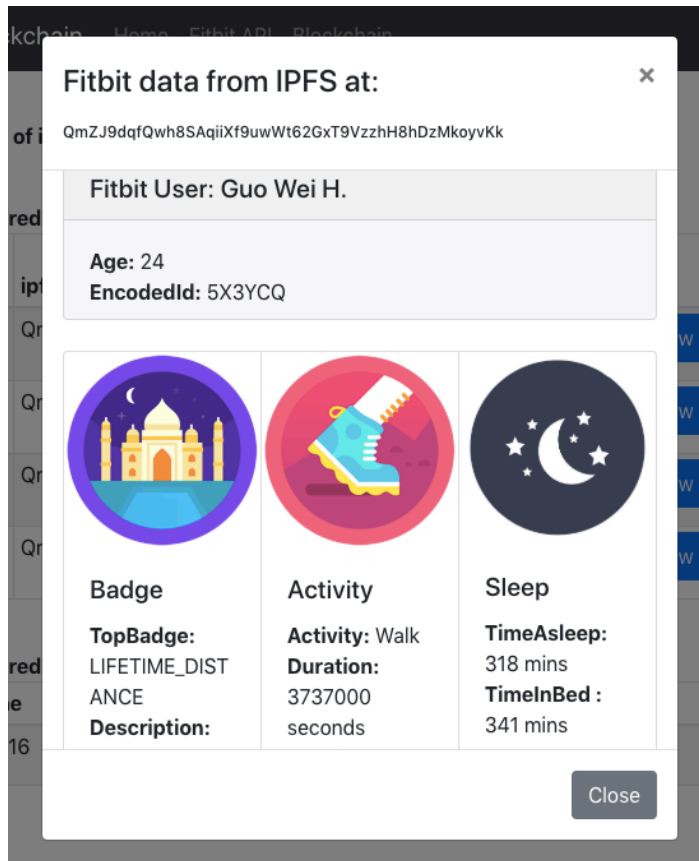


Figure 11 View Health Status

The share button allows user to share the content. Sharing would encrypt the user A's data using user B's public key such that only user B with B's private key can decrypt and read it:

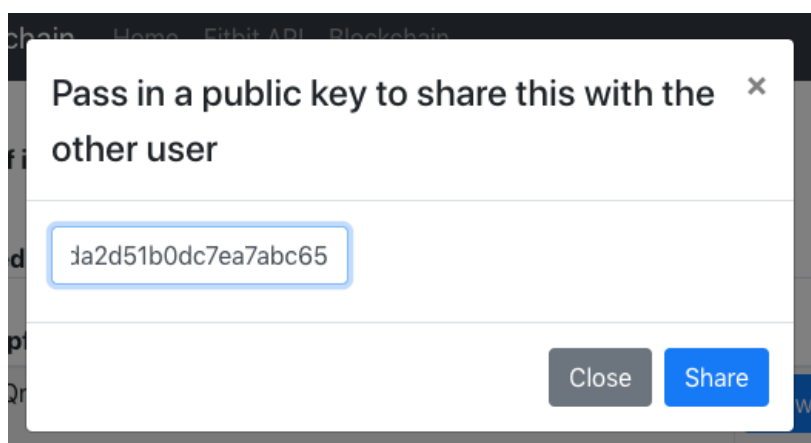


Figure 12 Share button





To address this problem, an encryption library, 'eth-crypto' is used to encrypt the content before uploading the data to blockchain. Below is the result of the same piece of data after encryption:

The screenshot shows a web-based encryption tool. At the top, there is a large text area containing a long string of hexadecimal characters, which is the encrypted data. Below this, there is a section for 'Character encoding:' with a dropdown menu set to 'ASCII'. Underneath the encoding section, there are three buttons: 'Convert' (highlighted with a blue border), 'Reset', and 'Swap'. Below these buttons is another large text area containing a shorter string of hexadecimal characters, which appears to be the result of the encryption process. At the bottom left, there is a 'Select' button.

```
373964303931656463363136393035636335623232653933333730
64303934313266393630346262663938366563336435343834346
63735636439373135623534333331313166353362623339373133
643838663064653434633031313537613637313263363237303433
313865333730363163656637376533623334373435356536376333
613264313439663134613664383932653637303633383965353039
323734306665373835653063663731336666373734000000000000
00000000000000000000000000000000000000000000000000000
```

Character encoding:  
ASCII

Convert Reset Swap

```
y¹P@€ trial b476f5353835357a48ed91d793e6f3fa02b441c0767bc7d
23ec77b167ea0859742b2fa7d99079d091edc616905cc5b22e93370d0
9412f9604bbf986ec3d54844f75cd9715b5433111f53bbb39713d88f0d
e44c01157a6712c62704318e37061cef77e3b347455e67c3a2d149f14a
6d892e6706389e5092740fe785e0cf713ff774
```

Select

**Figure 15 Unreadable Text**

## Chapter 4 -- Conclusion

### 4.1 Evaluation

The usefulness of the demonstrated Dapp is largely limited by the number of nodes running the service. The lower the number of nodes, the higher the power and the control the existing nodes hold to compromise the network, be it intentionally or not. For a Dapp to achieve its intended use, it either has to attract enough nodes in the network or be deployed to Ethereum public main net.

The file accessing speed at the IPFS public gateway is still slow during the first time of retrieving the content. As mentioned earlier, this is due to the lack of IPFS hosting nodes and the low adoption rate of IPFS currently.

Due to the nature of Proof of Work consensus algorithm, it may be too costly to perform the above storage operation on Ethereum and may be too expensive for everyday life usage.

While PoW is precluding Smart Contract from becoming scalable at this stage, the future of Ethereum 2.0 utilizing Proof of Stake may be promising for small applications with not much financial incentive.

### 4.2 Future work

- (a) In future, the application could include a machine learning model running on the Fitbit health data to generate a report on overall health status of the user. This could provide an indication on how close a user is to getting certain chronic diseases, helping detect early symptoms of severe chronic diseases like heart attack etc. It can provide feedback to the users as to whether there is a need for attention and a clinic visit.
- (b) A mobile version of the application could be developed as it is more intuitive and handy when it comes to allowing the user to upload the data more frequently, anytime anywhere.

- (c) Right now only encryption is done on the retrieving key, the IPFS hash. To ensure full privacy, encryption could be done on the file content itself before uploading it to the IPFS network.
- (d) A more exclusive wallet could be developed for this Dapp, to handle the private keys more securely. The prototype is developed solely for demonstration purpose. It has several severe security issues that have to be addressed. Encrypting and decrypting the data is one of them, where if not handled properly, it could leak the information about the keypairs to the network. Currently, there exists no crypto wallets in the market that offer the functionality of encryption/decryption using public-private key as most only offer signing transaction functionality. Hence, there is a need to develop a wallet that could encrypt/decrypt content without exposing the keys.

### 4.3 Final words

The above Dapp implementation merely serves as a demonstration on how we can utilize decentralized network in place of a centralized one as well as how it can be incorporated into our everyday life just like a traditional application. Dapp undeniably has its flaws, yet with its ability of executing tasks autonomously and elegantly, it has huge potential.

There is so much possibility in the blockchain world and we are only at the stage of exploration. Inevitably, there are legal and regulation issues circulating around blockchain that we have to solve. Yet, it should not be an obstacle that deters the humans from embracing a new internet that is more decentralized and free of control by authorities. Contributing to a blockchain project is one of the ways we could show our support and appreciation to the blockchain world. I look forwards to a day where we have the freedom in the world of internet. Cheers!

## Bibliography

- [1] The forth revolution, what it means and how to respond. (14 Jan 2016)  
Retrieved 18 Oct 2019, from <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>
- [2] Blockchain, the driving force behind 4th industrial revolution. (26 July 2016)  
Retrieved 18 Oct 2019, from <https://www.linkedin.com/pulse/blockchain-driving-force-behind-fourth-industrial-revolution-vega/>
- [3] How our data got hacked, scandalized and used in 2018. (13 Dec 2018)  
Retrieved 18 Oct 2019 from <https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018>
- [4] Decentralizing Privacy: Using Blockchain to Protect Personal Data. (20 July 2015)  
Retrieved 18 Oct 2019 from <https://ieeexplore.ieee.org/abstract/document/7163223>
- [5] What is the IoT? Everything you need to know. (21 Aug 2018)  
Retrieved 18 Oct 2019 from <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/>
- [6] New Ways to Monitor Advanced Heart Failure. (27 Nov 2018)  
Retrieved 5 Sep 2019 from <https://www.webmd.com/heart-disease/heart-failure/heart-care-16/new-ways-monitor-advanced-heart-failure>
- [7] Mirai, The Infamous Internet of Things Army, Can Now Mine Bitcoin. (10 Apr 2017)  
Retrieved 19 Oct 2019 from <https://www.coindesk.com/mirai-infamous-internet-things-army-can-now-mine-bitcoin>
- [8] Centralized Networks vs Decentralized Networks. (30 Nov 2018)  
Retrieved 19 Oct 2019 from <https://www.solarwindsmsp.com/blog/centralized-vs-decentralized-network>
- [9] Facebook–Cambridge Analytica data scandal. (14 Oct 2019)  
Retrieved 18 Oct 2019 from [https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge\\_Analytica\\_data\\_scandal](https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal)
- [10] 51% Attack. (6 May 2019)  
Retrieved 19 Oct 2019 from <https://www.investopedia.com/terms/1/51-attack.asp>
- [11] Why is decentralized and distributed file storage critical for a better web? (20 Jun 2017)  
Retrieved 18 Oct 2019 from <https://coincenter.org/entry/why-is-decentralized-and-distributed-file-storage-critical-for-a-better-web>

- [12] IPFS documentation.  
Retrieved 19 Oct 2019 from <https://docs.ipfs.io/introduction/how-ipfs-works/>
- [13] The IPFS Gateway Problem. (7 Feb 2019)  
Retrieved 19 Oct 2019 from <https://medium.com/pinata/the-ipfs-gateway-problem-64bbe7eb8170>
- [14] Ethereum. (29 Sep 2019)  
Retrieved 18 Oct 2019 from <https://en.wikipedia.org/wiki/Ethereum>
- [15] Understanding The DAO Attack. (25 Jun 2016)  
Retrieved 19 Oct 2019 from <https://www.coindesk.com/understanding-dao-hack-journalists>
- [16] Chainlink CEO Talks About His Product Roadmap. (21 Sep 2019)  
Retrieved 19 Oct 2019 from [https://www.youtube.com/watch?v=ulyI\\_K-TFDI](https://www.youtube.com/watch?v=ulyI_K-TFDI)
- [17] Quantum Computing Vs. Blockchain: Impact on Cryptography. (30 Jun 2019)  
Retrieved 19 Oct 2019 from <https://cointelegraph.com/news/quantum-computing-vs-blockchain-impact-on-cryptography>
- [18] Scoping and addressing the problem of link rot. (22 Sep 2013)  
Retrieved 20 Oct 2019 from  
<http://blogs.harvard.edu/futureoftheinternet/2013/09/22/perma/>
- [19] Cost of storing 1KB data on Ethereum. (14 Dec 2017)  
Retrieved 20 Oct 2019 from <https://ethereum.stackexchange.com/questions/872/what-is-the-cost-to-store-1kb-10kb-100kb-worth-of-data-into-the-ethereum-block>