Decentralisation Through Blockchains

Sanzhar Kozhay, tutor: Jaime Delgado

Contents

1 Context and Objectives

Blockchain is an emerging technology that has especially been popular the last couple of years. In 2008 [1] when the global financial crisis served as catalyst for the desire of a strong financial currency outside of failed governments' influence, Bitcoin was born. Since then the blockchain technologies have been gaining popularity [Figure 1].

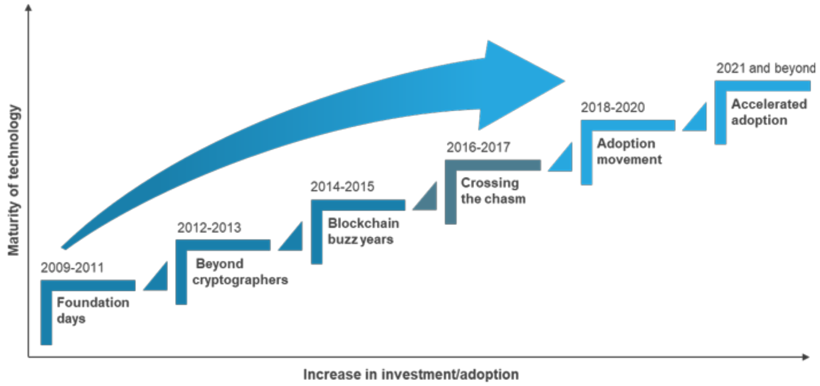


Figure 1: brief blockchain history [2]

1.1 The Challenges To Conventional Systems

Currently all of the conventional systems are centralised meaning there comes the issue of trust. The same trust issue that gave birth to bitcoin in 2008. Not only trust in technology but trust in people, seeing how most cyber attacks are targeted at the human factor [3]. Trust is also divided into several layers. Some users might not trust the institutions while others might trust the central authority to not be malicious but not believe that the central authority is capable enough to not be fooled by other malicious actors. By removing the human factor with decentralised solutions we have one less problem to worry about.

There is a number of other benefits to using blockchain that will be described in 3.2.

1.2 Objectives

Just like any other technology-based project it will be necessary to have at least some understanding of technology and having heard of crypto currencies on some level. Some programming knowledge is recommended.

This project is mainly focused on the website that we will see in the section 3 and some theory. Figure 2 shows the list of objectives and subobjectives of this project.

- **T1 Project Management**. Organising and planning the time and resources for the project.

- **T2 Smart Contract**. This involves learning the language necessary to write smart contracts on ethereum mainnet/testnet. I bought and started a virtual bootcamp for developing on Ethereum that lasted several months and later on i had to spend some time on my own researching Solidity (the smart contract language), web3 (API for interacting with smart contracts) and ReactJS (a javascript framework, currently has the best compatibility with Ethereum smart contracts) to properly make a website from scratch. It also included researching testing envinronments, namely Ganache and Kovan. Oracles were necessary as an important component to achieve interaction between blockchain and the real world. Finally, it was necessary to research how to use smart contracts to work together with Stripe API that accepts fiat payments.

- **T3 ReactJS frontend**. This involves learning enough html to make the external look of the website as well as learn how to connect the front end to the backend. Also learn to embed external APIs, namely Stripe for fiat payments.

- **T4 Cloud**. Linode will be used as a cloud service provider to host the website online. Docker containers are a great tool for being able to host the website without compatibility issues. Kubernetes used as load balancing.

- **T5 Usability**. Navigation tools to let the user understand how to use the crypto currency payments.

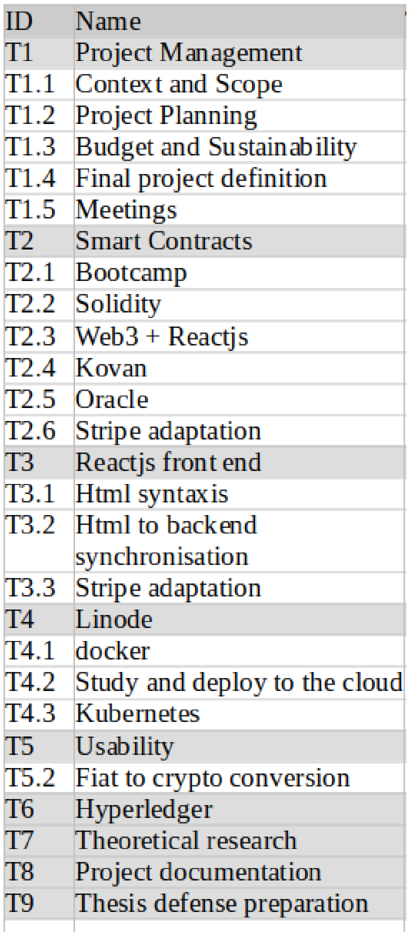
- **T6 Alternative platforms**. Investigating how it can be used on other platforms. Cardano seems to be the most promising candidate. Ethereum is currently the leading platforms for smart contract development but it has many emerging competitors.

- **T7 Theoritcal research**. To provide context to what blockchain is and its potential.

- **T8 Project Documentation**. Putting everything into a neat document, unfortunately, takes a big portion of time out of development.

- **T9 Thesis defense preparation**. Likewise.

We will first see the blockchain introduction and the website created for crowdfunding with the listed objectives in mind, followed by a discussion on the blockchains' security, legal battles and widespread adoption.



ID	Name
T1	Project Management
T1.1	Context and Scope
T1.2	Project Planning
T1.3	Budget and Sustainability
T1.4	Final project definition
T1.5	Meetings
T2	Smart Contracts
T2.1	Bootcamp
T2.2	Solidity
T2.3	Web3 + Reactjs
T2.4	Kovan
T2.5	Oracle
T2.6	Stripe adaptation
T3	Reactjs front end
T3.1	Html syntaxis
T3.2	Html to backend synchronisation
T3.3	Stripe adaptation
T4	Linode
T4.1	docker
T4.2	Study and deploy to the cloud
T4.3	Kubernetes
T5	Usability
T5.2	Fiat to crypto conversion
T6	Hyperledger
T7	Theoretical research
T8	Project documentation
T9	Thesis defense preparation

Figure 2: Objectives

2 Blockchain Introduction

For many people blockchain technology is synonymous with bitcoin and for a good reason as it all started from Bitcoin and then evolved to further uses. Bitcoin is currently known to most people as a volatile currency compared to normal fiat money and has made many people rich and others poor due to its price swings. However, lets first have a look at blockchain at a more basic level before diving into any particular cases. Blockchain is, like the name suggests, a chain of blocks and it implements a peer-to-peer protocol. Every block contains a series of information, one of which is a hash pointing to the previous block, hence creating a chain of said blocks. Although there are many key characteristics associated to blockchains such as timestamping, immutability, transparency and such, there are exceptions that forgo conventions in favor of their own objectives and visions. First of all lets have a look at the most important part of every blockchain: consensus mechanism.

2.1 Consensus Mechanism

Blockchain is usually thought of as a decentralised database that stores information on many different nodes rather than a centralised storage. While in many cases it's true because the information stored on the blockchain tends to be small, it's not accurate as the blockchain is for the most part a timestamped record of transactions. A good example is Filecoin that stores files on its underlying platform while the blockchain itself merely serves as an index.

It's also important to note that blockchains have no transaction cost except for the negligible electric energy spent on it. The infrastructure has a great cost with the most prominent example being mining farms but the transactions themselves have non. The peer-to-peer network constantly sends new transactions to each other and here comes the problem of consensus. We don't know in which order the transactions occurred which is no small issue. If a wallet has 1 bitcoin and it sends 1 bitcoin to Bob and 1 bitcoin to Alice then one of those transactions is legitimate while the other is not.

The validating nodes are tasked with organising the new transactions into an ordered list and, depending on the consensus mechanism in use, to catch fraudulent transactions such as spending wallet funds several times. Once this work is done this new list of transactions is put in a block and the blockchain is now 1 block longer.

2.1.1 Proof-of-Work

There is a popular notion that proof-of-work is an old consensus mechanism and proof-of-stake is just better. This is by no means a one-sided issue, there are many proponents for both sides and the debate rages on albeit proof-of-stake amassing bigger support. There are certainly many arguments being presented, which we will see in the security section 4.

PoW(Proof-of-work) is, as the name implies, a proof via a hash result that work, i.e. resources invested that in this case happen to be electric energy, has been invested into performing this operation. But lets start from the beginning. In 1993 PoW has been developed as tool to prevent DoS(denial of service) attacks and other such as spamming. The service user's device is required to perform work meaning processing time and resources hence making any attacks costly. In 2009 bitcoin introduced a way to use proof-of-work as consensus.

Miners on a network are validating nodes that are tasked with participating in the consensus. When a new transaction is created the miners will compete to solve a complex digital puzzle which is difficult to solve but easy to verify the correct answer. The first miner to solve the problem sends his answer and when verified by other miners as the correct answer he receives the reward for it in tokens, for example bitcoin.

2.1.2 Proof-of-Stake

In 2011 PoS(proof-of-stake) was born. the idea of competition between miners is wasteful, so PoS uses an algorithm to choose which node, called validator as opposed to miner in PoW, gets to mint the new block and then a number of other nodes are tasked with confirming its validity. The chances of being selected depends on how much is staked. If a node tries to add a fraudulent block, depending on the network, it will lose a part of or all of its stake. There can be other conditions for nodes to follow such as losing part of its stake if minimal uptime is not met.

PoS is a very flexible mechanism that allows many blockchain projects to invent just about anything. Some notable examples are DPoS(delegated proof-of-stake) that includes a groups voting on who gets to mint a block, Cardano's Ouroboros that includes staking pools that later distribute the rewards between contributors, Ethereum's Casper that combines PoS with PoW and even innovative solutions like Solana's proof-of-history that makes use of a clock mechanism for delayed validation which drastically increases processing speed.

PoA(Proof-of-Authority) is a particularly important variation of PoS because it is the basis for many businesses that do not wish to expose internal information. The most popular solution is to use Hyperledger Fabric by IBM which allows to handpick the participating nodes and can also choose which information is public and which is private. This allows for confidentiality and control over the blockchain at the cost of poor decentralisation. A good example of a PoA project is VeChain which will be discussed further in 5.2

Also important to note: platforms such as Cardano and Ethereum v1.0 while using PoS and PoW respectively, can host PoA projects on them. VeChain is, in fact, built on Ethereum and Cardano's head developer has already announced plans to give the same opportunity and even improve on it.

2.1.3 Other

It is important to note that both of those mechanisms are very young and there may soon be a third mechanism that will overtake as the default choice for new projects. One example is Ripple team that has their own consensus mechanism based on setting up servers with a list of other trusted servers. The consensus for the transactions is reached via a list of requested transactions and the proposals from trusted servers. An incremental voting mechanism is set between servers till all servers agree on some transactions while discarding the dubious ones. Also just to mention another example there is Proof-of-Replication and Proof-of-Spacetime both used by Filecoin as it is an unconventional type of blockchain for file storage.

2.2 Oracles

The oracles serve to take real world data (offchain data) and connect it to the blockchain (onchain data). An example would be to indicate which team won a football match and then the contract sends the money on the bet to whoever guessed right. Oracles can feed just about any kind of data but currently the most common use is simply crypto currency prices and confirmations of certain events like whether a package has been delivered or whether an insurance money has to be paid out or not.

There are centralised as well as decentralised oracles. The most widely known decentralised oracle is Chainlink that currently works closely with Ethereum but intends to widen their range of operations for example its recent partnership with Tezos. Chainlink oracles are set up by paying to a number of nodes to tell the offchain information and come to the final conclusion based on what kind of information is request and the types of answers received.

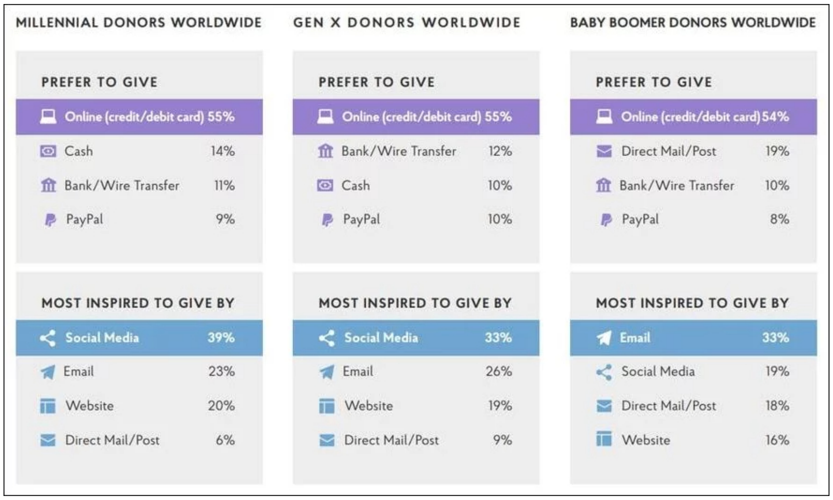
3 Crowdfunding website

3.1 Introduction

Crowdfunding originated back in 1700 [4] when the concept of microcredit was invented in an irish loan fund. It later branched into 4 main categories. This project is from the donation-based category where nothing is given in return, just like most with charities. by 1800s there were more than 300 crowdfunding programs.

Jumping to 1976 the idea of modern microfinancing was coined. This was a research project with the aim of providing banking opportunities to underprivileged individuals to encourage self-employment. The growth was especially high with the emergence of the social media. The online contributions are currently the most popular type [Figure 3] within the ever growing market [Figure 4]

In 2008 and 2009, IndieGoGo and Kickstarter—which have since grown into 2 of the most popular crowdfunding platforms—sprung onto the scene with the goal of supporting creative entrepreneurs and projects. These platforms helped popularize the rewards-based method of crowdfunding, combining the original principle with an ever-growing social sharing mindset and technical infrastructure.



MILLENNIAL DONORS WORLDWIDE

PREFER TO GIVE	
Online (credit/debit card)	55%
Cash	14%
Bank/Wire Transfer	11%
PayPal	9%

MOST INSPIRED TO GIVE BY	
Social Media	39%
Email	23%
Website	20%
Direct Mail/Post	6%

GEN X DONORS WORLDWIDE

PREFER TO GIVE	
Online (credit/debit card)	55%
Bank/Wire Transfer	12%
Cash	10%
PayPal	10%

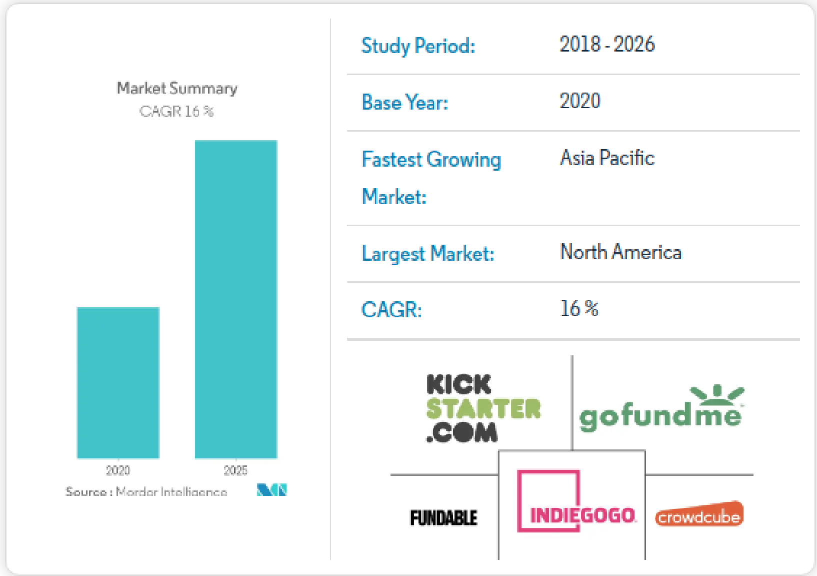
MOST INSPIRED TO GIVE BY	
Social Media	33%
Email	26%
Website	19%
Direct Mail/Post	9%

BABY BOOMER DONORS WORLDWIDE

PREFER TO GIVE	
Online (credit/debit card)	54%
Direct Mail/Post	19%
Bank/Wire Transfer	10%
PayPal	8%

MOST INSPIRED TO GIVE BY	
Email	33%
Social Media	19%
Direct Mail/Post	18%
Website	16%

Figure 3: Source: 2018 Global Trends in Giving Report [6]



Study Period:	2018 - 2026
Base Year:	2020
Fastest Growing Market:	Asia Pacific
Largest Market:	North America
CAGR:	16 %

Figure 4: crowdfunding market value [7]. CAGR = compound annual growth rate

3.2 Why Use Smart Contracts

The blockchain adoption has been steadily growing, especially last year due to enormous inflation [47] due to the global pandemic. More and more people start using crypto currencies and the evergrowing adoption is predicted to only go ever higher [Figure 5].

Small scale donors are getting more and more crypto wallets [5] and many vendors adapt by setting up donations wallets. Especially in poor countries like South America and Africa with a high degree of uncertainty in their local fiat currencies and banking [37] so local people don't trust their currency. Crypto donations provide transparency as all of the donations will be visible. [Figure 6] shows an example where all the operations done by the smart contract are visible and the same applies to crypto wallets. Crypto wallets, however, are only simple donations. Smart contracts allow adding an extra step of adding functionalities to better allocate the fund hence not needing to trust the charity campaign. This way the donors can have an extra assurance that their money will not be misused. For example the contract can allocate accumulated resources to vendors and transportation services without the campaign being able to change the contract since smart contracts are immutable.

To many people, charities have become synonymous with corruption and money laundering and for a good reason, there have been countless examples [8]. Providing a fully transparent system hopefully will put those fears to rest.

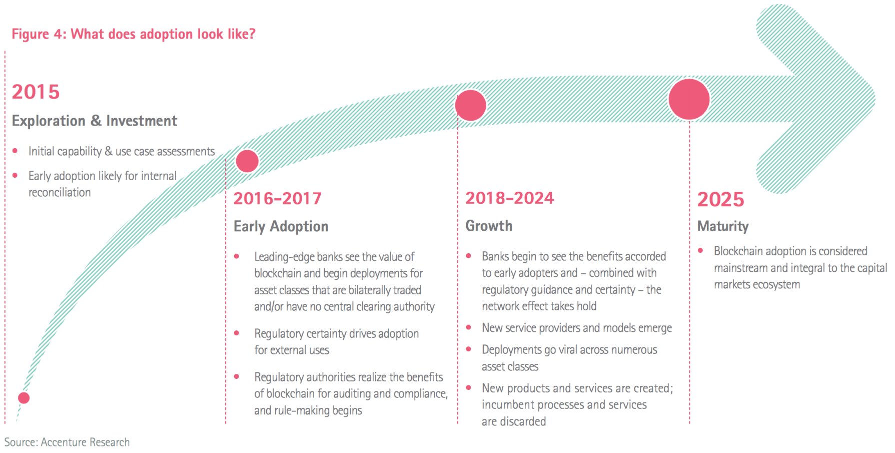


Figure 4: What does adoption look like?

2015

Exploration & Investment

- Initial capability & use case assessments
- Early adoption likely for internal reconciliation

2016–2017

Early Adoption

- Leading-edge banks see the value of blockchain and begin deployments for asset classes that are bilaterally traded and/or have no central clearing authority
- Regulatory certainty drives adoption for external uses
- Regulatory authorities realize the benefits of blockchain for auditing and compliance, and rule-making begins

2018–2024

Growth

- Banks begin to see the benefits accorded to early adopters and – combined with regulatory guidance and certainty – the network effect takes hold
- New service providers and models emerge
- Deployments go viral across numerous asset classes
- New products and services are created; incumbent processes and services are discarded

2025

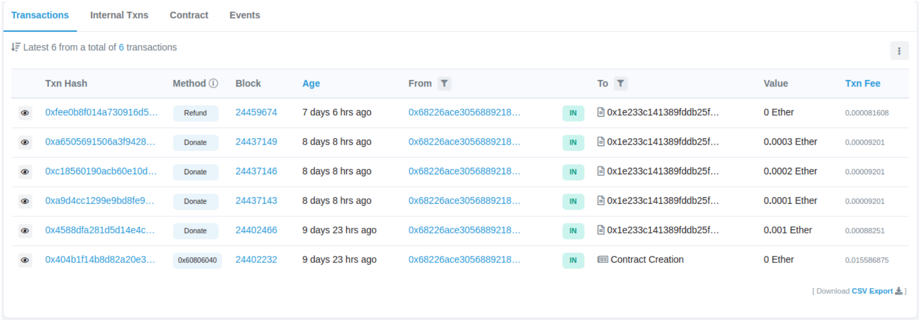
Maturity

- Blockchain adoption is considered mainstream and integral to the capital markets ecosystem

Source: Accenture Research

Figure 5: blockchain adoption prediction

The larger scale institutional donors that contribute a significant amount [Figure 7] are more likely to be interested in technicalities and transparency provided by smart contracts. The invoices and lack of transparency can cause problems so automating the process in an immutable and transparent way can have many benefits. There are also cost saving benefits to automating and decentralising business procedures. A good example is supply-chain blockchains



Transactions Internal Txns Contract Events

Latest 6 from a total of 6 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0xfee0b8f014a730916d5...	Refund	24459674	7 days 6 hrs ago	0x68226ace3056889218...	IN	0x1e233c141389fddb25f...	0 Ether	0.000081608
0xa6505691506a3f9428...	Donate	24437149	8 days 8 hrs ago	0x68226ace3056889218...	IN	0x1e233c141389fddb25f...	0.0003 Ether	0.00009201
0xc18560190acb60e10d...	Donate	24437146	8 days 8 hrs ago	0x68226ace3056889218...	IN	0x1e233c141389fddb25f...	0.0002 Ether	0.00009201
0xa9d4cc1299e9bd8fe9...	Donate	24437143	8 days 8 hrs ago	0x68226ace3056889218...	IN	0x1e233c141389fddb25f...	0.0001 Ether	0.00009201
0x4588dfa281d5d14e4c...	Donate	24402466	9 days 23 hrs ago	0x68226ace3056889218...	IN	0x1e233c141389fddb25f...	0.001 Ether	0.00088251
0x404b1f14b8d82a20e3...	0x60806040	24402232	9 days 23 hrs ago	0x68226ace3056889218...	IN	Contract Creation	0 Ether	0.015586875

[Download CSV Export]

Figure 6: etherscan example

in section 5.2 where resources are wasted [44] because the distribution systems are not transparent making communication ineffective.

The 10 most generous corporations
donate over
$
$2 BILLION
annually to nonprofits, much of it through
employee matching gift programs.
doublethedonation.com
Double the Donation
matching gifts made easy

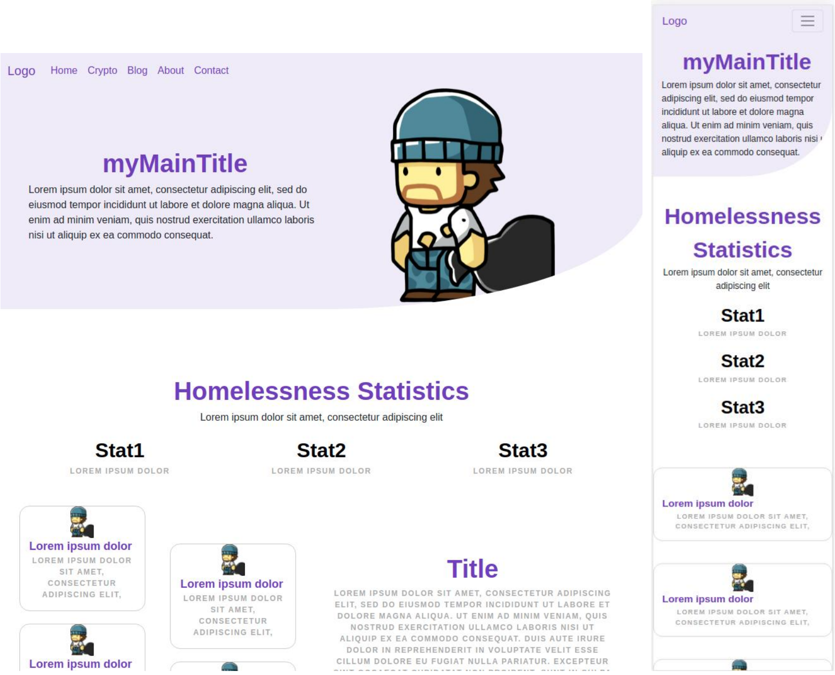
Figure 7: donations from big corporations [6]

There are some websites (more on it in 5.3) that accept crypto payments but they usually do so by direct donations to the website's crypto wallet withot using smart contracts. Also cryptounlocked.wetrust.io features the same structure of an ethereum smart contract but it is a lot less customizable and has to be hosted on their website hence a custom built website serves better as a charity campaign tool.

3.3 Website Overview

The idea of the project is to set up a generic donation website for charity. An example that is being used for this campaign is funding a soup kitchen by sending the donations to a food distributor who will then deliver the goods to the soup kitchen. The website itself is meant to be a normal charity template that has all the basic functionalities of a smart contract.

Figure 8 shows the generic look of the website. I took some inspiration from a different template but all of it was written from scratch. It has several tabs: the landing page tab with fiat donations, crypto tab for crypto donations, blog tab, about tag and the contact tab. The website is adapted for mobile too.



myMainTitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Homelessness Statistics

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Stat1 LOREM IPSUM DOLOR

Stat2 LOREM IPSUM DOLOR

Stat3 LOREM IPSUM DOLOR

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Title

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT, SED DO EIUSMOD TEMPOR INCIDIDUNT UT LABORE ET DOLORE MAGNA ALIQUA. UT ENIM AD MINIM VENIAM, QUIS NOSTRUD EXERCITATION ULLAMCO LABORIS NISI UT ALIQUIP EX EA COMMODO CONSEQUAT. DUIS AUTE IRURE DOLOR IN REPREHENDERIT IN VOLUPTATE VELIT ESSE CILLUM DOLORE EU FUGIAT NULLA PARIATUR. EXCEPTEUR

Lorem ipsum dolor

myMainTitle

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Homelessness Statistics

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Stat1 LOREM IPSUM DOLOR

Stat2 LOREM IPSUM DOLOR

Stat3 LOREM IPSUM DOLOR

Lorem ipsum dolor

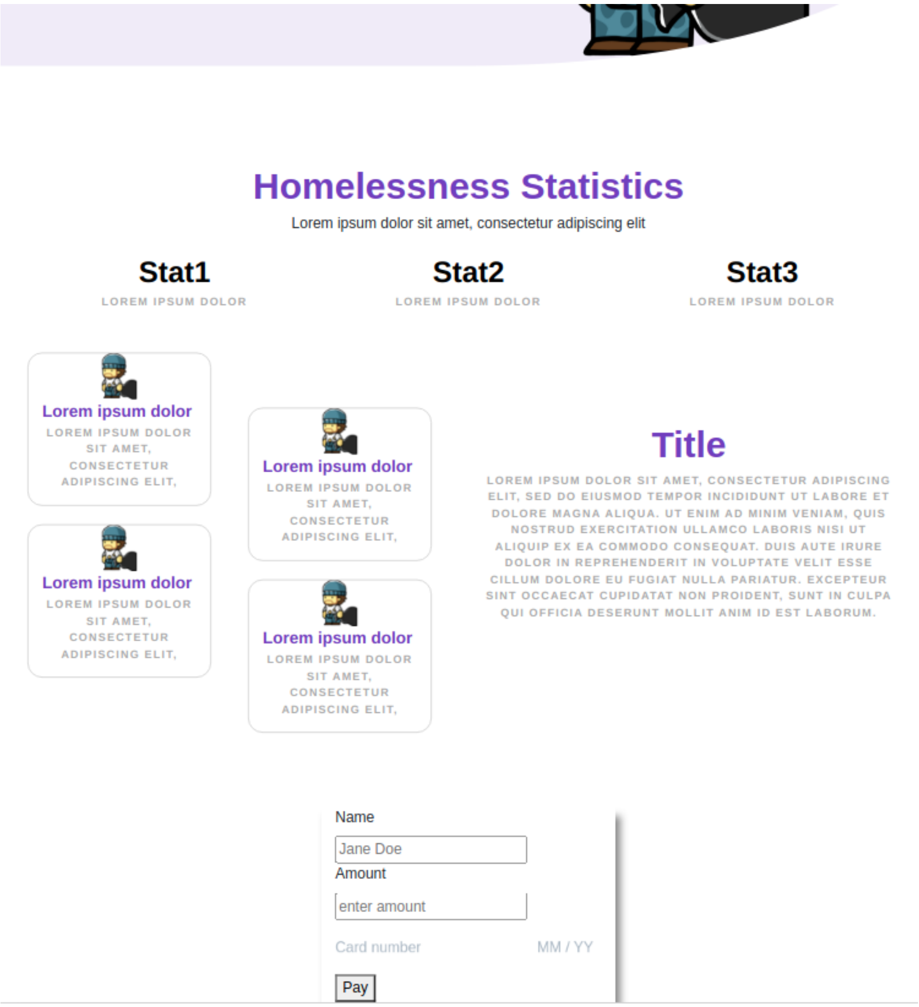
LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Figure 8: landing page

First of all we have the normal situation where we have a landing page with fiat currencies. The Landing page presents a template that can be filled with whatever marketing and promotion ideas the campaign might have. At the end it sets up a field for fiat currencies [Figure 9. It is implemented using Stripe API which, importantly, does not reveal to the website any information about the card so it cant be stolen [Figure 14].



Homelessness Statistics

Lorem ipsum dolor sit amet, consectetur adipiscing elit

Stat1

LOREM IPSUM DOLOR

Stat2

LOREM IPSUM DOLOR

Stat3

LOREM IPSUM DOLOR

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Lorem ipsum dolor

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT,

Title

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT, SED DO EIUSMOD TEMPOR INCIDIDUNT UT LABORE ET DOLORE MAGNA ALIQUA. UT ENIM AD MINIM VENIAM, QUIS NOSTRUD EXERCITATION ULLAMCO LABORIS NISI UT ALIQUIP EX EA COMMODO CONSEQUAT. DUIS AUTE IRURE DOLOR IN REPREHENDERIT IN VOLUPTATE VELIT ESSE CILLUM DOLORE EU FUGIAT NULLA PARIATUR. EXCEPTEUR SINT OCCAECAT CUPIDATAT NON PROIDENT, SUNT IN CULPA QUI OFFICIA DESERUNT MOLLIT ANIM ID EST LABORUM.

Name

Jane Doe

Amount

enter amount

Card number MM / YY

Figure 9: payment field for fiat

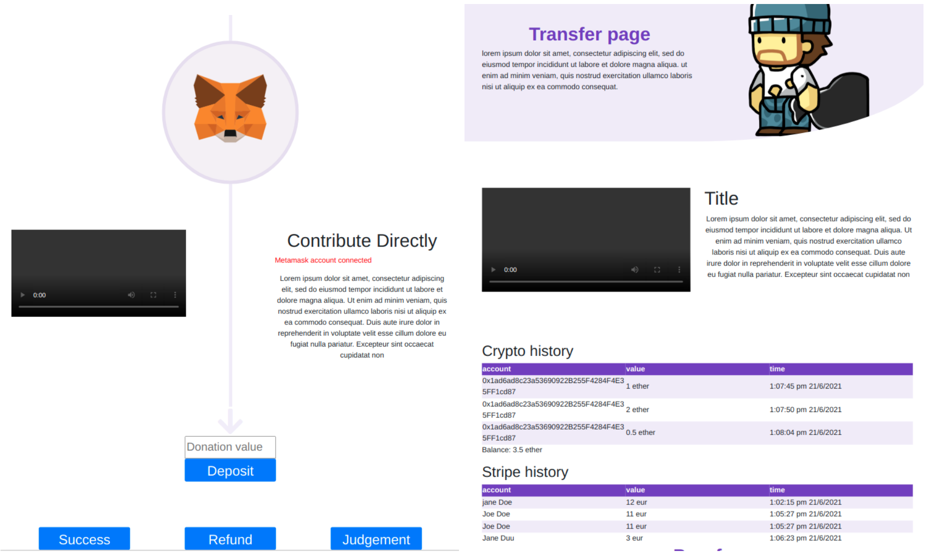
The next tab is for crypto donations. For crypto donations the user has to use Metamask. This is a chrome browser extension that acts as a virtual crypto wallet. If unavailable the user will see ”please connect with metamask” instead of the buttons provided in [Figure 10]. In absence of metamask donations can come as a direct donations to the smart contract’s address. With a metamask the user will have to confirm the transaction and it will be sent to Ethereum and confirmed after a few minutes.

The 3 buttons on the bottom are debugging buttons. The ”Success” button to send the funds, the second to make a full refund and the third to ask the oracle which action should be taken. In this project the use of oracle only serves as a proof of concept as it is questionable if it is a good idea to use it with crowdfunding. The supply-chain blockchains use smart contract a lot with their own oracles. More about it in 5.2. An example would be sending the funds only once the oracle confirmed that the goods were received. Crowdfunding campaigns can customise the oracle question make contingency donations. For example a big corporation wants to make a donation but only if their end of the year growth numbers are high enough. The oracle confirms the numbers and then the contract code executes.

At the beginning of the page there is a record of all donations, crypto donations in one table and fiat in the other. The fiat donations come through Stripe using a bank account but the blockchain keeps the history of every donations.

Once the campaign is completed it will indicate it by showing ”completed” [Figure 11]

The last 3 tabs are just basic pages that most websites have [Figure 12].



Contribute Directly

Metamask account connected

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non

Transfer page

lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Title

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non

Crypto history

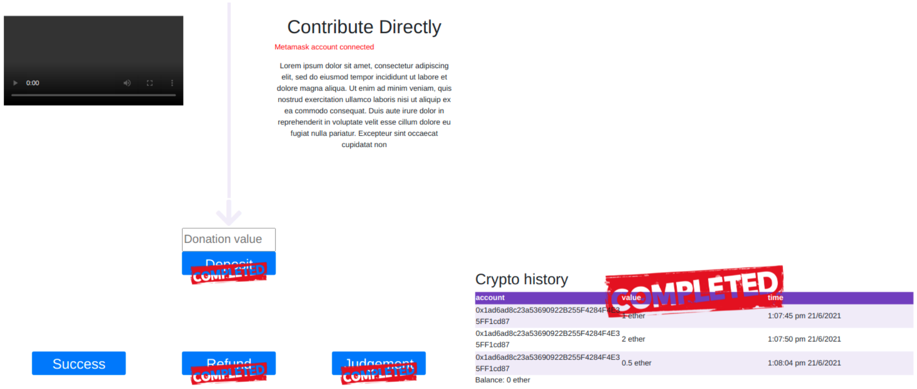
account	value	time
0x1ad6ad8c23a53690922B255F4284F4E35FF1cd87	1 ether	1:07:45 pm 21/6/2021
0x1ad6ad8c23a53690922B255F4284F4E35FF1cd87	2 ether	1:07:50 pm 21/6/2021
0x1ad6ad8c23a53690922B255F4284F4E35FF1cd87	0.5 ether	1:08:04 pm 21/6/2021

Balance: 3.5 ether

Stripe history

account	value	time
jane Doe	12 eur	1:02:15 pm 21/6/2021
Joe Doe	11 eur	1:05:27 pm 21/6/2021
Joe Doe	11 eur	1:05:27 pm 21/6/2021
Jane Duu	3 eur	1:06:23 pm 21/6/2021

Figure 10: crypto page



Contribute Directly

Metamask account connected

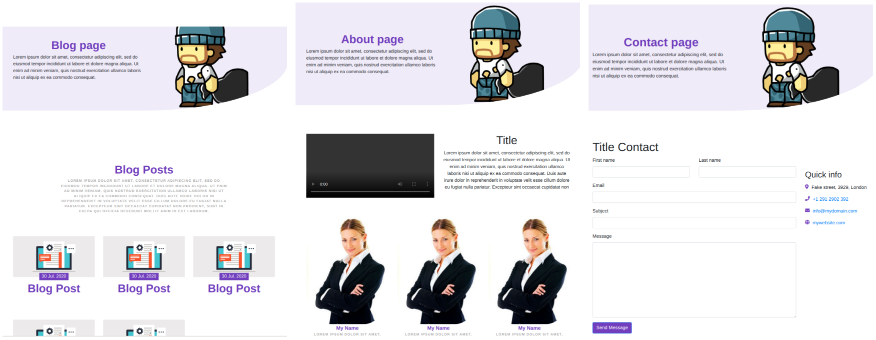
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non

Crypto history

account	value	time
0x1ad6ad8c23a53690922B255F4284F4E3 5FF1cd87	1 ether	1:07:45 pm 21/6/2021
0x1ad6ad8c23a53690922B255F4284F4E3 5FF1cd87	2 ether	1:07:50 pm 21/6/2021
0x1ad6ad8c23a53690922B255F4284F4E3 5FF1cd87	0.5 ether	1:08:04 pm 21/6/2021

Balance: 0 ether

Figure 11: when completed



Blog page

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Blog Posts

LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT, SED DO EIUSMOD TEMPOR INCIDIDUNT UT LABORE ET DOLORE MAGNA ALIQUA. UT ENIM AD MINIM VENIAM, QUIS NOSTRUD EXERCITATION ULLAMCO LABORIS NISI UT ALIQUIP EX EA COMMODO CONSEQUAT. DUIS AUTE IRURE DOLOR IN REPREHENDERIT IN VOLUPTATE VELIT ESSE CILLUM DOLORE EU FUGIAT NULLA PARIATUR. EXCEPTEUR SINT OCCAECAT CUPIDATAT NON PROIDENT, SUNT IN CULPA QUI OFFICIA DESERUNT MOLLIT ANIM ID EST LABORUM.

About page

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Title

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non

0:00
My Name
LOREM IPSUM DOLOR SIT AMET,
My Name
LOREM IPSUM DOLOR SIT AMET,
My Name
LOREM IPSUM DOLOR SIT AMET,

Contact page

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Title Contact

First name

Last name

Email

Subject

Message

Quick info

Fake street, 3929, London

+1 291 2902 392

info@mydomain.com

mywebsite.com

Figure 12: basic tabs

3.4 Solidity Contract

```
contract Charitycontract{

  event Donate(address user, uint256 amount, uint256 timestamp);


  //donation registry
  uint256 public addressListSize = 0;
  mapping(uint256 => address payable) public addressList;
  mapping(address => uint256) public refundAddress;

  //epoch format of GMT: Friday, April 2, 2021 11:53:21 AM
  uint256 public finishingDate = 1617364401;
  //the receiving account
  address targetAccount;
  //whether the final transaction has been made
  bool completed = false;

  ....

  function donate() payable public{
    require(!completed);
    if(refundAddress[msg.sender] == 0){
      addressList[addressListSize] = msg.sender;
      addressListSize++;
    }
    refundAddress[msg.sender] += msg.value;

    emit Donate(msg.sender, msg.value, now);
  }

  function transferFunds() public {
    require(now >= refundDate);
    if(completed) return transferToCampaign();
    else{
      bytes32 oracleResponse = getOracleResponse();
      bytes32 one = 0x0...1;
      if( oracleResponse == one)  transferToCampaign();
      else refund();
      completed = true;
    }
  }

...
}
```

Listing 1: curated and shortened version

The main contract that goes on the mainnet has a few key concepts and some others that are self explanatory or unimportant and are removed for brevity.

The first line is the ”event” that are being called from functions and can be thought of as history that can be easily obtained. The following part is a data structure to track donations by index and account, and the next part is a number of variables as described by the comments.

The donate function tracks the sender of the donation and if this is the first donation then makes a slot for it and updates the contributed amount. At the end calls the ”Donate” event to track the history of donations.

3.4.1 unit-testing

```
describe("donate ether", () => {
    let amount
    let result

    beforeEach(async() => {
      const amountEther = 1
      amount = web3.utils.toWei(amountEther.toString(), "ether")
      result = await charitycontract.donate({from: user2, value: amount})
      //console.log(result.logs)
    })

    it("donate ether", async() => {
      const balance = await charitycontract.getBalance()
      balance.toString().should.equal("1000000000000000000")
    })
    it("emits a Donate event", async() => {
      const log = result.logs[0]
      log.event.should.eq("Donate")
      const event = log.args
      //console.log(event)
      event.user.should.equal(user2, "user is correct")
      event.amount.toString().should.equal(amount.toString(), "amount is correct")
      const checkingBalance = await web3.eth.getBalance(user2)
      //console.log("over here ", checkingBalance)

      ....

    )}
}
```

Listing 2: testing the contract

Unit-testings are done to ensure that the contract is working properly before sending the contract to the testnet and mainnet. Contracts are unchangeable once they are deployed so there is no room for error. Every step of the way has to be included in the unit-tests including but not limited to: smart contract initiation, smart contract data, events information, crypto currency amounts and triggering errors when faulty information is submitted.

Below is a small part of the unit-test file written with chaijs. It organises into sections with ”describe(...)” and then subsection with ”it(...)”. This part sends some ether in the ”beforeEach” section and then checks the result of the operation and makes sure the ”Donate” event has been called.

3.5 Oracle

”Reality” oracle operates by setting up a reward for participating in answering a question. A more detailed description can be read here [9]. Every time an answer is given a deposit has to be made and in case the answer is incorrect it will be given to the owner of the right answer, therefore discouraging fraudulent answers. For each subsequent answer the deposit gets bigger and the last answer with the biggest deposit wins. If there are several identical answers a system is set up to split the reward based on timing and deposit amount. In case of conflict between several answers an arbitration can be requested by anyone for a price. The arbitrator and its fee are predetermined when the question is asked. The arbitrator being the final judge has to be taken into account when asking and answering the question, hence the arbitrators are interested in maintaining their reputations.

3.6 Reactjs

The javascript language is being used due to Solidity (smart contract language) being based on javascript and has a good compatibility with it. First of all due to their similarity it is easier to relate one to the other and second of all the web3 library that connects smart contract to external code has a good javascript support. Also javascript is for me personally an easier language to use for development that its python alternative. Furthermore Reactjs framework has a starting template to start using a blockchain application so it’s easier to set up.

Due to ReactJS being a single page framework a lot of scalability considerations had to be taken into account. Reactjs is poorly scalable and it is mainly for simple websites. Hence breaking the html parts of the website into a number of files for smooth interaction. For example in the figure below almost every element is imported as an html piece from another file otherwise the one big file would become impossible to work with.

```
function Home(props) {
  return (
    <>
      <MainBanner title="myMainTitle" text="Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat."  />
      <div class="container">
        <DappStats />
        <Elements stripe={stripePromise}>
          <StripeForm />
        </Elements>
      </div>
    </>
  );
}
```

Listing 3: testing the contract

3.6.1 Web3

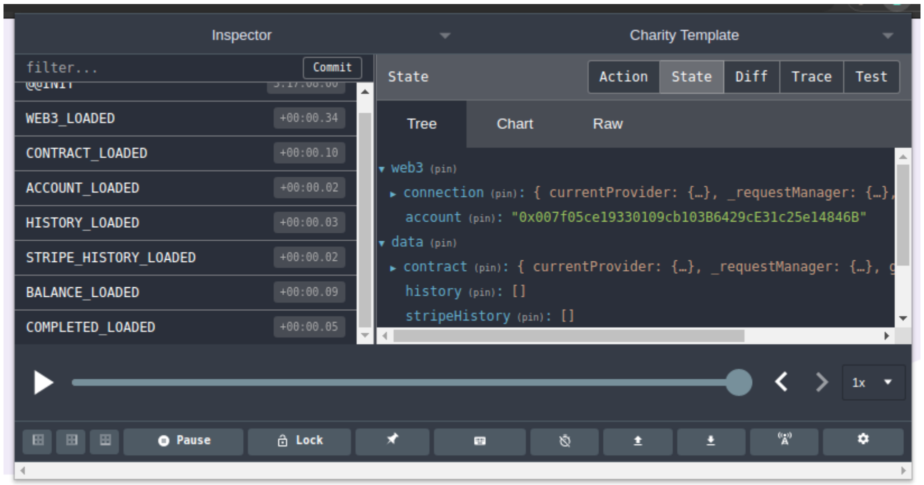
Web3 is an API for interacting with the smart contract. Below is a short example how to call contract methods. It has several other functions like getting events history, getting public variables, obtaining network information etc.

```
import Charitycontract from "../abis/Charitycontract.json"
const charitycontract= new web3.eth.Contract(Charitycontract.abi,
    Charitycontract.networks[networkId].address)
const contractBalance = await charitycontract.methods.getBalance
  ().call()
await charitycontract.methods.donate().send({from: account, value
  : web3.utils.toWei(amount.toString(), "ether")})
```

Listing 4: web3 call example: fetch contract by address; get contract balance; make donation

3.6.2 Redux

Redux helps not only serves as a state container but also allows the user to see everything that is happening [Figure 13]. Redux is a state container that acumulates variables necessary for calling certain functions. In the main App.js file the variables are obtained from the smart contract and the network and are stored in the redux container which can then be easily accessed by any part of the program instead of either 1)getting the function results from smart contract again or 2)constantly passing the variables as arguments between numerous parts of the website that can get quite messy. It is also a very convenient tool for debugging by showing its entire data set and history in the browser debuggin extension which can be seen in the figure below.



```
@@INIT
WEB3_LOADED            +00:00.34
CONTRACT_LOADED        +00:00.10
ACCOUNT_LOADED         +00:00.02
HISTORY_LOADED         +00:00.03
STRIPE_HISTORY_LOADED  +00:00.02
BALANCE_LOADED         +00:00.09
COMPLETED_LOADED       +00:00.05
```

```
▾ web3 (pin)
  ▸ connection (pin): { currentProvider: {…}, _requestManager: {…},
    account (pin): "0x007f05ce19330109cb103B6429cE31c25e14846B"
▾ data (pin)
  ▸ contract (pin): { currentProvider: {…}, _requestManager: {…}, g
    history (pin): []
    stripeHistory (pin): []
```

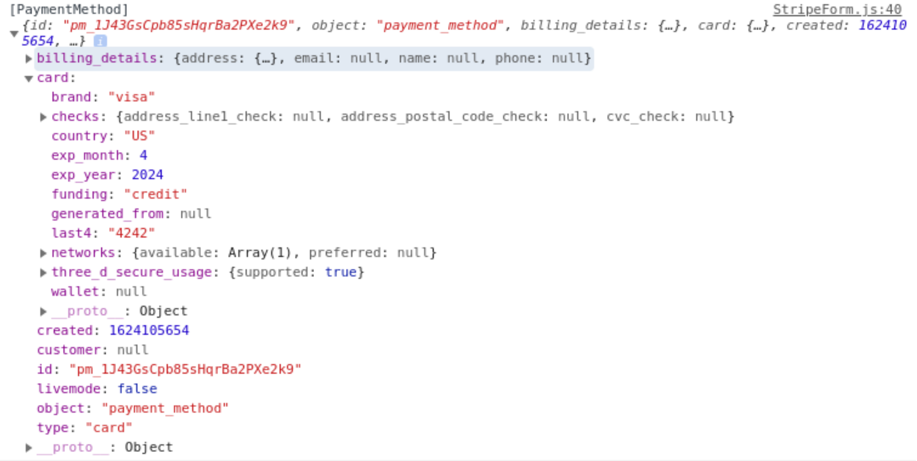
Figure 13: redux development tool

3.6.3 Stripe

Stripe API is used to make fiat donations. Stripe features security measures of never exposing the card number to the website despite the user typing it into the form. More about Stripe API secret key here [10]

Meanwhile for every stripe donation an event in the smart contract is triggered featuring who and what quantity has been sent to keep an immutable history of transactions. Normally the metamask browser extension is required to make any ”write” operation on a smart contract because it has a fee in crypto currency. To go around this a private key is be stored in the program that will sign the operation automatically without requiring the user to do anything other than press ”submit”. The smart contract will only allow changes coming from the account with this particular private key so if someone wants to host the docker image then he will not be able to interact with the smart contract without the private key.

The current gas (in other words crypto currency fee) price per each transaction with the current price for ether is roughly 2euros per transaction making it impractical. However the Ethereum developers are promising to solve this issue in the upcoming version 2.



```
[PaymentMethod]                                                                                   StripeForm.js:40
▼{id: "pm_1J43GsCpb85sHqrBa2PXe2k9", object: "payment_method", billing_details: {…}, card: {…}, created: 162410
 5654, …} ℹ
  ▶billing_details: {address: {…}, email: null, name: null, phone: null}
  ▼card:
     brand: "visa"
    ▶checks: {address_line1_check: null, address_postal_code_check: null, cvc_check: null}
     country: "US"
     exp_month: 4
     exp_year: 2024
     funding: "credit"
     generated_from: null
     last4: "4242"
    ▶networks: {available: Array(1), preferred: null}
    ▶three_d_secure_usage: {supported: true}
     wallet: null
    ▶__proto__: Object
   created: 1624105654
   customer: null
   id: "pm_1J43GsCpb85sHqrBa2PXe2k9"
   livemode: false
   object: "payment_method"
   type: "card"
  ▶__proto__: Object
```

Figure 14: stripe ”secret” log. The bank card information is hidden to the website

3.7 Development Environment

3.7.1 Kovan + Ganache

The smart contracts on the ethereum network that charge fee for any operations so Ganache test environment by truffle is being used in development. It is a personal blockchain with 1 node that allows to write and test smart contract without any fees and it works in much the same way as ethereum mainnet. Afterwards Kovan testnet is used which is much slower than Ganache and much faster than Ethereum mainnet to validate transactions and uses KETH (kovan ether crypto currency) to pay for transactions. Kovan is functionally the same as mainnet and in this project if it works on Kovan then it is considered finished to avoid paying fees for the mainnet usage.

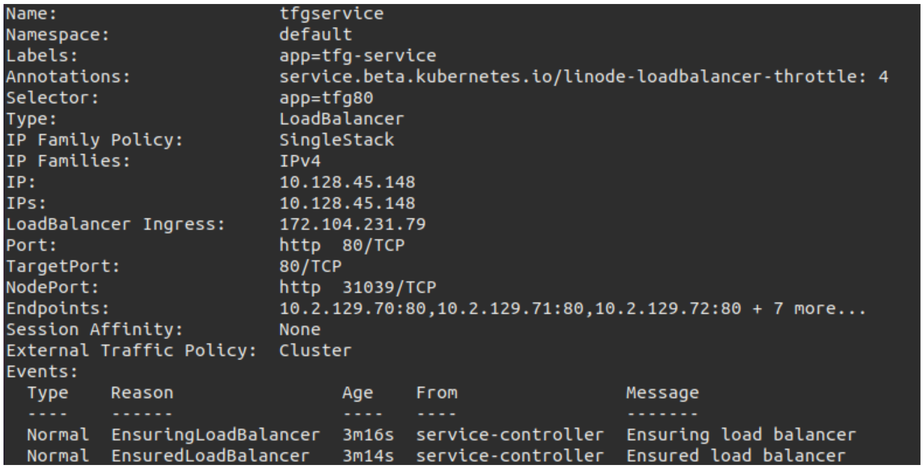
3.7.2 Docker + Linode

For transparency purposes as well as portability and version control docker is used for development. Docker is a software for containerising applications. Multiple images can be maintained in case of mistakes and for version history allowing better development efficiency. It also allows easy download of the images for code review in case anyone decides to check for malicious code and to be able to host without setting up a webserver like nginx. With the current implementation it's only a matter of pulling the image and creating a container to host it on your local machine.

Linode is being used for hosting at a low price of 5$/month and has a good docker template to simply download it and it's just working. For another 15$/month there is the kubernetes service to have a better DDoS attack tolerance. Kubernetes sets up several node instances in an efficient and time-saving manner for load balancing if the website gains a lot of popularity. While not necessarily useful in this project especially because ReactJs is inherently poorly scalable, as a proof of concept it is worthwhile doing. At the very least it makes DDoS attack requirements several times bigger.

Also, due to hosting the website through Linode to the public some legal considerations have to be taken into account. Due to limited time compliance will not be part of this project. The european GDPR (general data protection regulation). It came into force in 2018 and due to the deployed website planning to collect some information like a name and the amount donated in the future work with stripe, it will have to comply with this law. There are several aspects such as completing a DPIA(data privacy impact assessment) that describes how information is collected, processed and which risks there are to the users, then if the information will be transferred outside EU, make a privacy notice similar to cookies' notice, retention and discoverability of data, how opt in forms in the front end html are used and a few others.

There are a few other laws that might need to be taken into account such as WCAG, it explains how to make web content more accessible to people with disabilities.



```
Name:                     tfgservice
Namespace:                default
Labels:                   app=tfg-service
Annotations:              service.beta.kubernetes.io/linode-loadbalancer-throttle: 4
Selector:                 app=tfg80
Type:                     LoadBalancer
IP Family Policy:         SingleStack
IP Families:              IPv4
IP:                       10.128.45.148
IPs:                      10.128.45.148
LoadBalancer Ingress:     172.104.231.79
Port:                     http  80/TCP
TargetPort:               80/TCP
NodePort:                 http  31039/TCP
Endpoints:                10.2.129.70:80,10.2.129.71:80,10.2.129.72:80 + 7 more...
Session Affinity:         None
External Traffic Policy:  Cluster
Events:
  Type    Reason                Age    From                Message
  ----    ------                ----   ----                -------
  Normal  EnsuringLoadBalancer  3m16s  service-controller  Ensuring load balancer
  Normal  EnsuredLoadBalancer   3m14s  service-controller  Ensured load balancer
```

Figure 15: Kubernetes: deploying 10 instances as seen in "endpoints"

4 Security

for private blockchains that use a poor degree of decentralisation the usual security exist as always. Malware, ransomware, social engineering, DoS, DNS attack, sql injection and such. However, we will discuss which risks are associated with decentralised applications as centralised cyber security is a whole other area of study and all of the attacks listed above rely on attack the single point of failure or access to sensitive information non of which would be of any use against a decentralised implementation.

4.1 Centralisation

The biggest threat to many decentralised platforms is, curiously, centralisation. There are obviously businesses that operate with a minimum degree of decentralisation like VeChain that only has a handful a nodes and there is nothing wrong with that, they will operate like a centralised business model with some benefits of a decentralised solution. For many others, however, who are aiming to reap full benefits of decentralisation there is always a risk that by having group of users band together they might start dominating the network. The centralisation-type attack on the network is called "51% attack" or "majority attack" and how it works depends on the consensus. If successful the attacker will be able to double spend his funds and obtain money by selling his funds several times, and prevent other transactions from being confirmed.

4.1.1 PoW attack

With PoW in its current form the 51% attack can happen by amassing more than half of the hashing power. Lets break this down. In PoW the longest blockchain always wins. Lets imagine a situation when 2 miners mine a new block at the same time, not some nodes will accept one block, and others will accept the other, so what happens now? Now we have 2 separate blockchains and eventually one of them will become longer than the other by producing more blocks. When that happens, as i mentioned previously, the longest blockchain always wins, so the users will abandon the shorter blockchain and migrate to the longer blockchain.

In PoW blockchain the complexity of the digital puzzle changes with the quantity of miners. The more miners the more complex the puzzle to maintain on average 10min per block. In other words, the more populated the networks the more energy it takes to solve the puzzle. What if a malicious user wants to add a fraudulent block? He will have to create the block, which is not too difficult, and then solve the puzzle by himself which means he will have to spend the same amount of electricity on this block as would be spend by the entire collective of PoW miners. In case if Bitcoin it consumes about 110 Terrawatt-hours per year [12] or 2.1Gigawatt-hours per 10min which is 1 block. Electric costs are obviously different depending on where you live with Bulgaria having 10 cents/kWh and Germany 30cents/kWh. Keep in mind that most mining farms are located in areas with cheap electric costs and with renewable sources of energy such as wind and hydro. Lets take the European average of 21cents/kWh [13] that makes it 441 000 euros in price per every block for an attempted attack.

However, the costs don't end here. As mentioned before, the longest blockchain always wins. so if you cant outrun everyone else banded together in the production of the block then your block will be rejected. The attackers needs 51% hashing power to outrun other miners. Assuming existing miners don't participate in the attack the cost of hardware would exceed $5.46 billion [14].

The more plausible way of obtaining 51% hashing power would be to take over the mining pools instead of buying or renting the hardware. Mining pools are a group of miners banded together to mine block and then splitting the reward between them. according to this article [15] 65% of the mining goes through chinese mining pools and if CCP(chinese communist party) seizes the pools it could perform this attack. Or that would be the case if not for the issue that miners can switch pools in a matter of seconds. As soon as news break out that a pool is seized the miners will abandon it, not only because of the potential attack but also because seized pools don't share mining rewards. It is unlikely that CCP will attempt anything like this as there is no benefit to trying to destroy bitcoin. In contrast attacking smaller blockchain with fewer miners behind it might very well prove profitable by double spending the funds and then liquidating them into fiat when done on a small scale as liquidation gets increasingly difficult with more funds hence attacks are only practical on smaller blockchains with low attack cost. Furthermore the more observed a blockchain is by its user base the faster they will react by stopping all dealings in this particular crypto currency, dropping the price for it and organising some kind of pushback.

There are many developments on that front with miners planning to leave china due to its regulations [16]. The miners are likely to spread out around the world making the centralisation risk less threatening.

Also, the attacker might not necessarily need the majority of hashing power as it is a game of numbers, simply start mining blocks alongside everyone else and with enough cards stacked in attacker's favour at some point the attacker might produce a block first. According to this article [17] it takes $513.000 per hour to attack with it being unclear how many hours it will take to attack till it works.

So far we have talked about PoW attacks from Bitcoin's perspective and sure enough Bitcoin benefits from a strong community support. In 2014 ”ghash.io” Bitcoin pool was nearing 51% which made everyone freak out and miners promptly left the pool [18]. In addition, when a blockchain is attacked there is an easy way out: the nodes organise together to reset the blockchain to its state before the attack. Unfortunately not all PoW blockchains have the same benefits, Ethereum Classic (not to be confused with Ethereum) has experienced 3 attacks [19] as its miners arent as big as Bitcoin's. This article [20] compares Bitcoin vs Ethereum Classic attack cost. There are many concerns that those attacks are far more prominent than people realise but they are kept quiet to not spoil the reputation. Some of the known attacks are Feathercoin 2013, Bitcoin Gold 2018, Bitcoin Cash 2019 and Vertcoin 2018 [21]

Monero is an interesting case of how to mitigate mining centralisation. It has increased decentralisation first of all via low transaction prices that currently sit at 5cents/transactions [22] unlike bitcoin's $7/transaction [23]. Next, Bitcoin suffers from average people being unable to compete with mining farms that have a specialised equipment and that presents a centralisation risk so Monero developed RandomX PoW algoritwhm. RandomX is optimized for general-purpose CPUs so specialised equipment will have no edge making mining more egalitarian. Now anyone with a PC or even a smartphone can start mining [24]

4.1.2 PoS attack

PoS attacks work in much the same way except with a slightly different validation mechanism. In PoS in order to not waste electric resources the system chooses a node to perform the block minting. Your chances of minting a new block depends on your staking. So does it favour the rich with deep pockets to stake? In a way, yes. PoW does too because the rich enjoy the economies of scale for their mining equipment, choice of location and higher quality equipment. So if a group of rich people band together to buy 51% of the cryptocurrency and start staking it then they have the majority voting power. When a block is minted the other nodes have to confirm that the block is legitimate. If, however, the majority of voting power is taken over by the attackers, then fraudulent block can go through. That, however, implies that they would have to somehow obtain such large funds. For example in Cardano blockchain over 50% is already locked up in staking pools so unless they somehow obtain funds from those people that are not trading their currency that would be impossible. But if that wasn't the case then the attackers can try obtaining the funds through trading and once they start buying all of the crypto currency its price will go through the roof.

One of the arguments for PoS is that unlike PoW the validators don't need expensive equipment so anyone can become one. Monero being an obvious exception to the rule in their creative approach. That implies that the degree of decentralisation is much higher due to more participants hence more difficult to attack the network. At the same time it can be said that PoS is less decentralised because in many cases there is a central authority that directs the networks in the direction it wants and performs 51% attacks on a regular basis. That is one way of putting it, the other way is to say that this authority is the official development team and when updating they fork the network which is essentially a 51% attack by having all people on the previous blockchain migrate over to their updated version. This central authority is what many of the PoW supporters don't like. As a side note: forks are not only for updates but also for team to build their project on top of an existing project, for example Bitcoin Gold is a fork of Bitcoin and Stellar is a fork of Ripple.

Nevertheless, others might say that having some centralised authority is a net positive for the network as in case of an attack it can lead the charge in reversing the attack. Ethereum's founder Vitalik Buterin famously said "A successful attack may cost $50 million, but the process of cleaning up the consequences will not be that much more onerous than the geth/parity consensus failure of 2016.11.25. Two days later, the blockchain and community are back on track, attackers are $50 million poorer, and the rest of the community is likely richer since the attack will have caused the value of the token to go up due to the ensuing supply crunch. That's attack/defense asymmetry for you."

There are no known examples for 51% attack on PoS blockchain, maybe only whales (a slang term for big crypto currency holders) banding together to vote on which direction the development team should take [25].

4.1.3 Oracles

It is worth a quick mention that oracles can be decentralised with some notable examples like chainlink and charli3. Many others, however, are not, but instead are offered as a centralised service to blockchains hence making an easier target to attack. Oracles themselves are a very new concept and so far there are no known big incidents.

4.1.4 Front End

Front end is the other offchain part that tends to be centralised as it tends to be focused on a single or a small group of servers. In case a DoS attack [26] or problems with a corrupt government the front end attack could severely damage accessibility to a blockchain. There are many decentralised services offering to provide a domain name, https://unstoppabledomains.com/ being of the popular choices.

The domain can be decentralised but what about the data? As far as file storage goes there are a few options with filecoin leading the charge. Filecoin is also a blockchain that is based on IPFS(Inter Planetary File System), it's a peer-to-peer decentralised protocol that stores files on several peers' memories and references said files via hashes. Of course if every peer has deleted the file and noone can provide it anymore then its lost. One solution to this problem is using an IPFS API called Pinata that for a price guarantees that the file will not disappear. The other is using Filecoin which is built on IPFS. Just like many other blockchain projects it uses its own cryptocurrency as payment for its services as well as for staking in its consensus mechanism and as reward for mining i.e. storing files according to their contract. Filecoin currently has no smart contract support to be used in businesses but the work is well on its way [27].

4.2 Regulations

The blockchain and crypto currency market is very new and the government around the world have had little time to adapt regulations to them. If anything, it might not be the best idea to pass any regulations at the moment since this emerging market is moving and changing faster than the necessary formalities to pass regulations. It is colloquially said that the blockchains to survive regulations will be the regulated and the unregulatable. There have already been numerous developments by several countries to ban or regulate crypto currencies [28]. Some others embrace it [29] .

The relationship of the crypto currency with the government is both a formality and a risk. Ripple makes news headlines for having a huge legal battle with SEC (american Securities and Exchange Commission). It started in December 2020 and was suspected to be end of this project as well as any other that gets on the SEC's radar. The allegations alone made many exchanges delist xrp [30] and its price made to fall. As of the time of writing the lawsuits is still in process but it seems to be going in Ripple's favour so far [31]. The gist of the lawsuit is that the xrp (the crypto currency tied to Ripple) is a security instead of a currency hence the xrp sale was illegal. Unlike many other projects Ripple is a private for-profit company with unconventional branding and marketing so it was an easier target for the SEC. This will potentially set a strong precedent for all future lawsuits. Ripple is not the first legal case for SEC. Telegram, for example, had to abandon its aspirations as the result of it [32].

Monero is the most likely next big blockchain lawsuit target. DOJ (american department of justice) said that the mere use of the privacy coins is a "high-risk activity that is indicative of possible criminal conduct" [33]. IRS hired a couple of agency to try to crack Monero [34]. Some indicate privacy coins will facilitate money laundering while others say basic human privacy shouldn't be violated on the basis of a few incidents so it is not a one sided issue.

As the result of this scrutiny xmr (tokens by Monero) got delisted from many major exchanges [35] This is yet another example of a centralisation threat, except its a centralisation of trading which is outside the blockchain itself. This is not to say xmr has become untradeable, there are still decentralised exchanges that cannot be targeted by the government such as "waves.exchange" that keeps trading xmr. The other solution that Monero is implementing is atomic swap between bitcoin and monero [36] hence providing yet another path towards being independent of exchanges.

5 Adoption

The use of smart contracts can serve to decentralise all kinds of operations to any type of business. Like my example with the crowdfunding earlier any capital movement can be done through or with the help of a blockchain. It can be money-transfer (crypto and fiat both), contracts with big clients and partners, contingency contracts, sale of tokenised products and more are in development.

If a company chooses to use a crypto currency it makes a number of changes. First of all in the vast majority of situations the business will create a crypto currency that is built on top of another crypto currency. In case of Ethereum it offers ERC20 tokens that are very easy and cheap to create and many decentralised projects do just that. There is a number of other platforms that offer the same opportunity notably Cardano, Polkadot and Solana but they are still growing.

Upon creating a crypto currency the company will usually charge said crypto currency as fee for its services and distribute it to miners or validators. The distribution of the coins will in most cases happen through ICOs (initial stake offerings) where the company sells said crypto currency for its initial low price and by so doing raise capital for development. Of course the investors take a gamble whether this company will succeed or fail or even run away with all of the money they got. There are some variations like STO, IICO, airdrops and others but those are rare.

The company might be for-profit or non-profit. In case of for-profit the company will usually make money from the blockchain indirectly by having partnerships and promotions. Also the founders usually keep a stock of the crypto currency in hopes it will appreciate considerably.

5.1 DeFi

DeFi (decentralised finance) is one of the first and most popular application of blockchain. DeFi removes the middleman in traditional finances. It is not completely decentralised because the smart contract production for a loan is still being done by a centralised authority. Similarly to taking a loan from a bank when taking a loan from DeFi the user has to bring a crypto currency collateral that will be taken away is the loan is not paid off properly. The biggest benefits of DeFi is not having barriers of the traditional finance such as confirming your identity, credit score or get a government approval. Just like banks the DeFi earns money by charging the borrows higher interest rates than the lenders. This is especially useful for poor countries where people remain unbanked [37]. There is currently $59.55B locked up in DeFi [38] and it will keep on growing [39].

Aave is the biggest player in DeFi, its founder has been obsessed with risk management and user protection since day 1. It is a lending and borrowing platform build on Ethereum and requires no identity check for use. The founder's biggest motivation has been to make institutional investors more comfortable with DeFi [40] which is something that has not been done by any other DeFi protocol. It is now in the process of the legal work to start accepting fiat collateral [41]

5.2 Supply-chain

Supply-chain businesses are a particularly interesting example due to its significance in the current times of the global pandemic as well as it being an unconventional and new application of a blockchain. Businesses that choose to decentralise for the most part use PoA(proof-of-authority) and that is usually done with Hyperledger Fabric by IBM but it's all very new so little data is available on it. This is not to say that VeChain is massive, it has only a handful of partnership as it's still very young. VeChain has 101 masternodes handpicked by its foundation and is smart contract compatible for any businesses that would like to join in.

VeChain is the current leader in decentralised supply-chain industry. VeChain is expected to have huge success in the near future as customers will have the opportunity to know exactly where their food came from which is a huge concern for many proponents of healthy way of life. Atala that offers this traceability and is developed by the same team as Cardano jokingly refers to it as Proof-of-Steak [42]. From the business perspective it also holds many advantages with supply-chain businesses having a fragile system where a single failure led to $60 billion in damages [43]. And that is on top of supermarket shortages seen during the initial stages of the covid-19 pandemic which was at least in part due to fragility of the supply lines. [44]

Blockchain's transparency and immutability benefits aren't limited to healthy eating. Pfizer's covid-19 vaccine requires certain conditions one of which is cold temperature to properly deliver it worldwide so the countries have to be assured the right conditions were met across the whole chain [45]. Smart contracts can replace invoicing processes that can take months to settle similarly to how supplychains can be switched much faster given its transparent plug-and-play structure unlike lengthy business negotiations.

Keep in mind that many blockchains with different consensus mechanism can communicate with each other so they are not isolated to themselves. Atala PRISM produced by IOHK team who are also working on Cardano blockchain and they have made a connection with them in their Ethiopia development project [46]. Atala PRISM is a digital identity product that only exposes selected information to the public blockchain hence maintaining privacy.

5.3 Payments

The crypto currency payments have been steadily growing since Bitcoin started growing in popularity and has particularly gained more favourability in the last year due to the global pandemic because of the high inflation [47] that will likely only get higher [48].

Bitcoin is now accepted by a number of businesses including: Travala [49] for traveling paid with dozens of crypto currencies , surfshark vpn [50] accepting btc, eth and xmr , expressvpn accepting bitcoin [51], bitgild [52] and european mint [53] accepting btc for gold purchase, namecheap [54] selling domain names for btc, bitcars [55] and autocoincars [56] selling cars for btc, bithome [57] accepting btc for real estate, newegg [58] selling electronics for btc, as well as many luxury items such as yachts [59]

There are many initiatives to improve upon the already impressive list above. The payments options still have ways to go to gain widespread acceptance and judging from the paypal case [60] where it took them only 6 months to complete implement their service the future potential is looking very promising. Apple [61] and Google [62] are looking in follow in its steps.

5.4 Banking

This is yet another innovative area for blockchain. At the forefront of it we have Ripple that was mentioned earlier when talking about its lawsuit battle with SEC. Then we have Stellar that was born as a fork from Ripple when one of the co-founders of Ripple left to create his own project in his own vision. Ripple stayed on the course of targeting financial institutions and payment providers to gain institutional adoption while Stellar focuses on individuals to facilitate ease of use for anyone willing to learn which will bring especially high benefits to developing countries where financial institutions are still in development. Both want to build fast and secure payment networks and neither of their approach is necessarily wrong and many could say they could easily coexist seeing as how their client base is very different

RippleNet is a closed source network that uses a nonstandard consensus called Ripple Protocol Consensus that is based on proposals and voting between the nodes. An individual cannot setup a node and start mining xrp tokens because the xrp is meant to be used between financial institutions not consumers. RippleNet gives users to global payments, on-demand liquidity and access to more than 40 different currencies with transactions being seamless, certain and fast. This comes in huge contrast to huge fees and long time delays when sending money to another country through banks. Ripple's transfer comes under 1 cent [63] and Stellar's even lower [64]

Stellar is open source. It uses SCP(Stellar Consensus Protocol) that unlike PoS uses a node reputation metric rather than staking and does allow setting up nodes and start mining XLM tokens. The project allows anyone to settle payments and trade. It aims to let individuals to rise above local economies and interact with international markets. Stellar is currency agnostic, it allows to handle and swap both crypto as well as fiat currencies. Its low cost per transaction makes it very accessible for payments.

Another interesting case is Algorand. Recently many governments have been rushing to develop CBDCs (Central Bank Digital Currencies) [65] and this has led some governments to turn to enterprise-oriented crypto projects with Algorand being one of them. Algorand uses PPoS(pure proof-of-stake) smartcontract-compatible platform that aims to solve the scalability problem that plagues Ethereum. Unlike Ethereum that aims to be a generic platform, Algorand is focused on financial market aiming to connect decentralised and traditional finance.

5.5 Cultural

It is often said that technological advances are not enough to promote adoption, the people have to be willing to accept the change, in other words marketing and promotion remain a big factor. The cultural adoption aspect has been especially felt after the recent Dogecoin boom. Dogecoin is a cryptocurrency that was started as a joke. Sometimes called ”memecoin”. It was 2013 when there was barely any awareness of crypto currencies and the founders mockingly made another coin that was supposed to be fighting for widespread adoption. In fact they thought of their coin so little that they didnt allocate any stock of coins for themselves upon creation. So why is dogecoin gaining widespread use? Simply for the fact that people on the internet like the ”shiba inu” meme that is used as Dogecoin’s logo and the coin itself doesnt present itself as something serious. For many people they see Bitcoin’s enourmous price and market cap and get intimidated from buying it but when they see a silly dog meme coin that is only worth under a dollar it makes it that much easier to try it. Simplicity sells. Dogecoin cannot be used as a storage of value due to its high inflation. It is not smart contract compatible. The founders are not working to improve it. And all of this is why Dogecoin is booming, it is all just for fun.

After the famous turning point of Elon Musk starting to promote doge on twitter it created enourmous speculation waves. A simple tweet from a person with a large following kickstarted the move [66]. To show how much community rally there has been behind it, robinhood (a stock trading platform) crashed due to the trading volume [67]. This dogecoin community didnt start with Elon Musk. In 2014 the Dogecoin community raised $25 000 to send a jamaican bobsleigh team to the olympics [68] and $50 000 for drinking water in Kenya [69] so it was a mix of both the silly and the serious. Even a number of merchants started to accept dogecoin [70] rivaling bigger adoption than most currencies after btc.

There is a number of other movements for crypto adoption such as trending social media hashtags, channels for specifically crypto currency discussions even a specific social media platform dedicated to crypto currency [71] and Coinbase (the most popular crypto currency exchange company) having a crypto currency fact check [72] to go with the rise of fact checkers on social media. By far the biggest benefit of dogecoin is that it introduced average people to crypto currencies through normal everyday activities like sports [73] instead of something with high barriers to entry such as long term investment and speculation.

Blockchain has come even to start a livestreaming platform. Livepeer is quite a promising new project that aims to use underutilised resources, provided by miners/validators, to improve price and quality of livestreaming that will be uncensorable during the times of crisis around the world. Note that it is also built on Ethereum. Livepeer has open source code policy and has a paid platform that provides video content distribution and storage. This is not only a competitor to youtube but also might be a competitor to twitch in the future, the popular game streaming platform.

NFT (non fungible tokens) are expected to be the next big boom due to them being collectables that drive a lot of communities to buy them simply because collecting is a hobby for many. Especially for those with deep pockets. Some people like to collect cards, others painting and here it's the tokens. Fungibility refers to exchangeability. If 2 individuals swap a 1 euro coin then nothing has happened, each individual retains the same value making euros fungible. If we are talking about dogs they are non-fungible. Even if 2 dogs are of the same species, height, gender they are still not the same dogs so they cant be easily exchanged one for another making them non-fungible.

The most common type of NFTs is about art and game items. It all started with a game on Ethereum called crypto kitties. A crypto kitty is an image of a cat whose ownership is tokenised. The token holder is the owner of the image. The image can be seen by anyone and the image is also copyrighted to the company instead of the token holder so the ownership has no real world value. It only serves for creating a collection of images and for price speculation.

Normally noone would expect something like this to become popular but back in 2017 crypto kitties crashed Ethereum after their popularity escalated [74] with some kitties being sold for over $40 000 [75]

There is a number of other collectibles such as crypto punks but the most curious case is unisocks. The token holders can redeem the token for a pair of socks and they are now worth over $40 000 per token [76]. While price speculation is definitely a factor it started with collectors wanting to have the token itself rather than the socks.

6 Sustainability

The sustainability matrix Table1 represents the types of effects the project has on various areas (environmental, economics and social) and following. It divides into 3 categories:

- PPP: Project Put in Production: it involves the planning, organisation and execution of the project.

- Useful Life: This involves the time period between the start of the project till its end of life

- Risks: The impact of the entire process involving everything from the development till the end of life.

Following, each will be discussed in higher detail.

	PPP	**Useful Life**	**Risks**
Environmental	Design resource consumption	Ecological footprint	Environmental Risks
Economic	Design cost	Viability	Monetary Costs
Social	Personal impact	Social impact	Social risks

Table 1: Sustainability matrix. Key: PPP=Project Put in Production.

6.1 Environmental Dimension

Regarding PPP: Have you estimated the environmental impact of the project? The only equipment being used in this project is the personal laptop. According to [80] an average laptop consumes 60W/h so considering 540 hours for the project the electric consumption will be 32400W. The cloud is also used for hosting but only for demonstration purpose and offline outside of that so we can ignore it. There are many concerns over bitcoin's power consumption with one side saying its consumes more power than the entirety of Argentina [81] and others saying it is way better than anything we've ever had with Bitcoin consuming less than 10% of the traditional banking [82]. This is where the majority of the discussion is.

According to [79] Ethereum consumes almost 52TWh/year (bitcoin 110TWh/year [12]) which is comparable to Portugal's consumption per year and its carbon footprint is 24.67 Mt CO2. We also know that it is on overage 119.4 kWh per transaction, equivalent to the power consumption of an average U.S. household over 4.04 days. In other words the less transactions the less consumed energy.

Regarding PPP: Did you plan to minimize its impact, for example, by reusing resources?

This project provides only the basic template for the simplest smart contract that can then be adjusted in accordance to the campaign's/company's needs. As far as environmental costs are concerned the only possible way to reduce the impact would be to reduce the number of transactions as possible. This would not be a worthwhile venture but it's possible to do so by accumulating several small donations and sending them in the same transaction such as making groups of people who donate at once or partnering with larger scale donors.

How will your solution improve the environment in respect to other existing solutions?

Ethereum currently uses PoW which is a lot more wasteful than its upcoming Casper (a hybrid consensus mechanism). The developers are estimating energy usage cut by 99.95% [83] with Casper. It is difficult to find a good centralised example to compare against. Cardano, however, provides some more data for comparison.

The initial goal of this project was also to write smart contract with Cardano which unfortunately has yet to release its smart contracts but it will soon. Lets look at its energy consumption as it will be relevant in the very near future. Cardano is the third greenest blockchain with the other 2 blockchains being projects made specifically for being green energy oriented [84]. Donations with Cardano will be orders of magnitude environmentally friendlier than using fiat currencies.

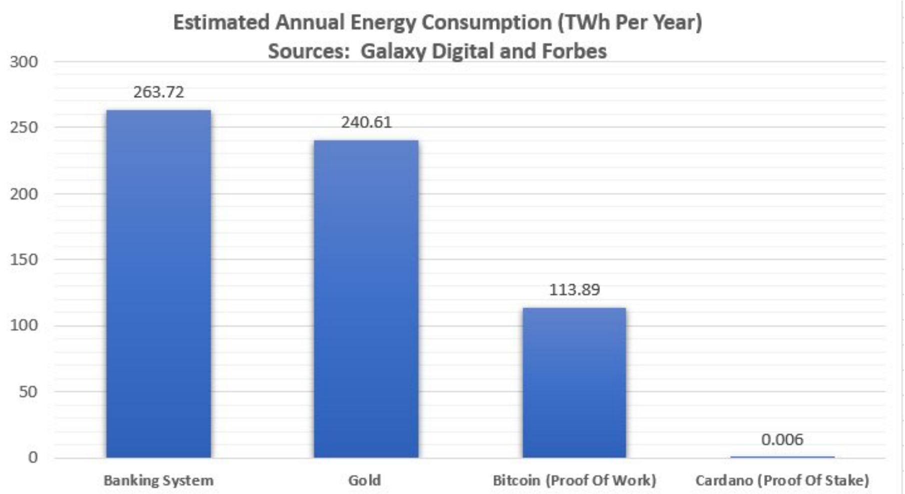
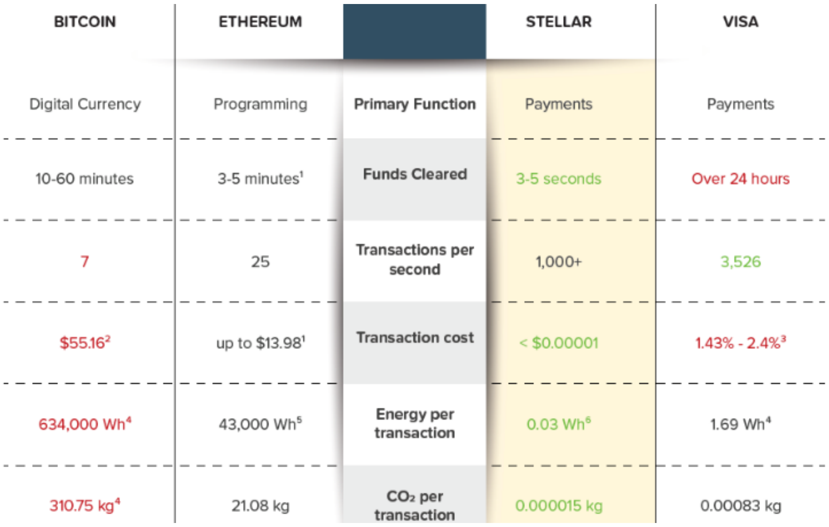


Figure 16: Cardano energy use in comparison. [85]

The 4th place is Stellar and the 5th is Ripple. Both are banking blockchains as described in the 5.4. Stellar is smart contract compatible so if it is used here is a comparison compared to traditional banking 17



BITCOIN	ETHEREUM		STELLAR	VISA
Digital Currency	Programming	**Primary Function**	Payments	Payments
10-60 minutes	3-5 minutes[1]	**Funds Cleared**	3-5 seconds	Over 24 hours
7	25	**Transactions per second**	1,000+	3,526
$55.16[2]	up to $13.98[1]	**Transaction cost**	< $0.00001	1.43% - 2.4%[3]
634,000 Wh[4]	43,000 Wh[5]	**Energy per transaction**	0.03 Wh[6]	1.69 Wh[4]
310.75 kg[4]	21.08 kg	**CO_2 per transaction**	0.000015 kg	0.00083 kg

Figure 17: Stellar electric costs in comparison [86]

6.2 Economic Dimension

Regarding PPP: Reflection on the cost you have estimated for the completion of the project:

The costs estimated in the section 7.2 provide the costs from the point of view of an average worker but I had only started with smart contracts and have limited experience so the cost should definitely be much lower for an average smart contract developer. Also the costs include the technical writer who wouldn't necessarily be needed depending on the circumstances.

The overall cost is relatively small involving most of the budget going towards labour cost therefore it can be said the project does relatively well in this category.

Regarding Useful Life: How are currently solved economic issues (costs...) related to the problem that you want to address (state of the art)?

Currently the conventional centralised systems host their systems either on their own hardware equipment or outsourcing it, for example cloud hosting. Most decentralised systems host the front-end but remove the core of the operation to the blockchain hence making the smart contract stay in the system forever. The useful life will be limited to the website's charity campaign time length.

Regarding Useful Life: How will your solution improve economic issues (costs ...) with respect other existing solutions?

In this particular situation the crypto donations are added as an extra feature while the conventional fiat donations still have to be available so from the economic point of view it's only an added cost of development.

6.3 Social Dimension

Regarding PPP: What do you think you will achieve -in terms of personal growth- from doing this project?

I've started learning blockchain as a side project for one of the university subject and at some point I started learning more and more not just about the technology but also the culture of it. I've discussed at it length in section 5.5. There are so many projects building and I consider the current times similar to the early industrial revolution. Not only many projects but also enourmous communities to share thoughts and ideas with. Even if i never end up being a blockchain developer due to intricacies of life i will for a long time follow many of these projects as a small scale investor.

Regarding Useful Life: How is currently solved the problem that you want to address (state of the art)? How will your solution improve the quality of life (social dimension) with respect other existing solutions?

The conventional centralised solutions in my view have not achieved the desired result for cyber security and transparency and, by extension, efficiency.

One could argue the current centralised system is designed to not be cyber-secure as well as provide little to no transparency.

In this particular project the crypto payments are only added as a feature what everything about the website can be decentralised. The domain name can be decentralised with the use of for example https://unstoppabledomains.com/ and the file storage for the website itself using Filecoin. The completely decentralised approach can provide great cyber security and transparency against fraud and corruption

Regarding Useful Life: Is there a real need for the project?

Due to the current inefficiencies and corruption there is very much a need for such improvements. In this particular project for fundraising only a small portion of the donations will be in crypto currencies but we are talking about larger donations with institutional investors then we can have numerous benefits as described in supply-chain blockchains 5.2 and banking 5.4.

It is especially useful to use crypto currencies and smart contracts in countries where the local banking system and the currency is too unstable [37] like Africa and South America.

7 Conclusion

The Gantt diagram 19 includes no dependencies as I didnt consider the tasks being particularly dependent upon each other, they were all separate parts that can be done individually.

As this is a project written by 1 person no work organisation tools have been used such as Asana or Trello that have most effectiveness in a team environment.

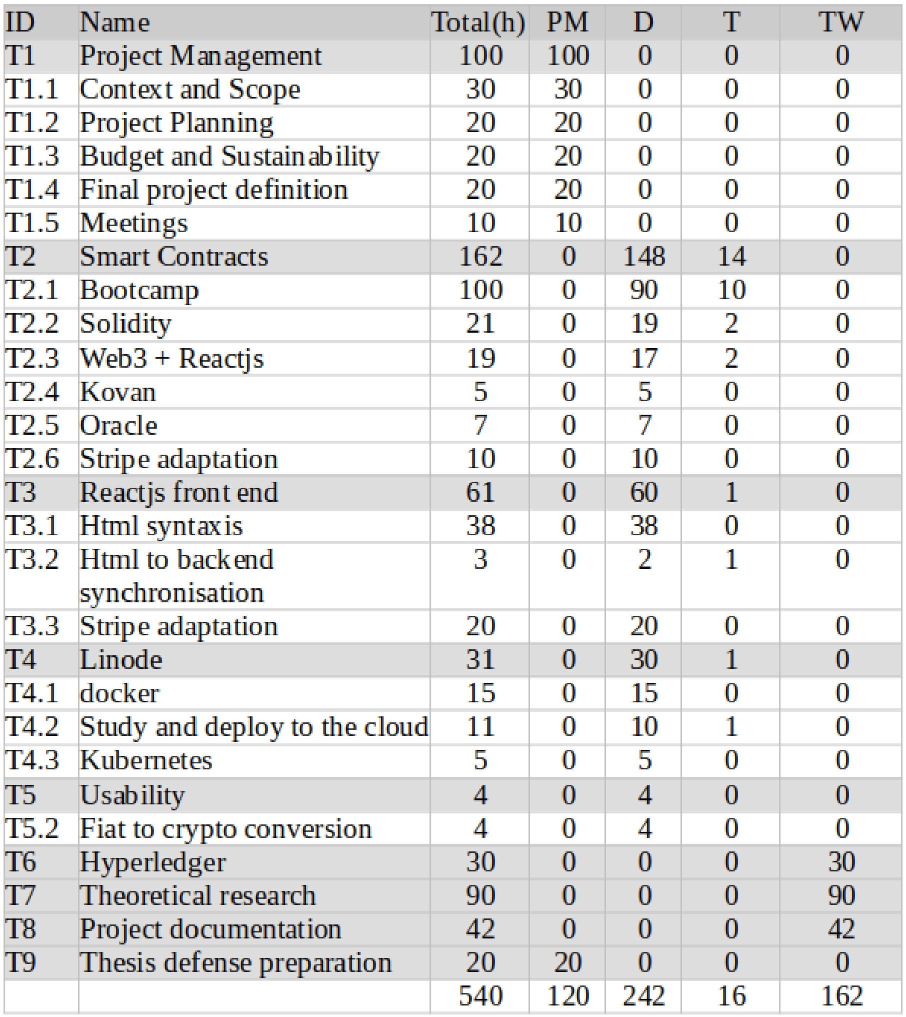
The dockerhub has been used as a backup as well as a public and private repositories. It makes it a lot easier for hosting as the user doesnt have to execute the hosting service, it's only a matter of pulling the docker image and starting it.

7.1 Objectives' progress

- **T1 Project Management**. This is my first experience writing a project like this so it has been personally helpful

- **T2 Smart Contracts**. Overall it went according to plan. I have started the bootcamp to learn smart contracts development before i started T1 so how much time has been spent on it is only an estimate. It started slow due to a lot of theoretical work but overall worked out without hick-ups.

  Adapting the smart contract to work with Stripe to record the history of transactions was something planned after the initial planning. The stripe donations come with a fee of 2.9% so it might be better to look for another provider. I chose the most popular option for development as fiat payments were not the primary objective of this project. Also when using blockchain to record every fiat payment it comes at a cost of around



ID	Name	Total(h)	PM	D	T	TW
T1	Project Management	100	100	0	0	0
T1.1	Context and Scope	30	30	0	0	0
T1.2	Project Planning	20	20	0	0	0
T1.3	Budget and Sustainability	20	20	0	0	0
T1.4	Final project definition	20	20	0	0	0
T1.5	Meetings	10	10	0	0	0
T2	Smart Contracts	162	0	148	14	0
T2.1	Bootcamp	100	0	90	10	0
T2.2	Solidity	21	0	19	2	0
T2.3	Web3 + Reactjs	19	0	17	2	0
T2.4	Kovan	5	0	5	0	0
T2.5	Oracle	7	0	7	0	0
T2.6	Stripe adaptation	10	0	10	0	0
T3	Reactjs front end	61	0	60	1	0
T3.1	Html syntaxis	38	0	38	0	0
T3.2	Html to backend synchronisation	3	0	2	1	0
T3.3	Stripe adaptation	20	0	20	0	0
T4	Linode	31	0	30	1	0
T4.1	docker	15	0	15	0	0
T4.2	Study and deploy to the cloud	11	0	10	1	0
T4.3	Kubernetes	5	0	5	0	0
T5	Usability	4	0	4	0	0
T5.2	Fiat to crypto conversion	4	0	4	0	0
T6	Hyperledger	30	0	0	0	30
T7	Theoretical research	90	0	0	0	90
T8	Project documentation	42	0	0	0	42
T9	Thesis defense preparation	20	20	0	0	0
		540	120	242	16	162

Figure 18: Project tasks. Key: PM= project manager. D= developer. T= tester. TW= technical writer

2 euros given the current ether price. Obviously this is currently not a viable solution. In the future the Ethereum team is planning to solve this problem but it's unclear if and when it will happen.

For larger institutional investors this template would only be enough for a single operation but even if it is one single case it can still have a lot of benefits. For example it could create a smart contract per every simple partnership it has and publish it on the website letting users know how the donations are going to come through. This is where the oracles will be useful as many of those partnership will have contingency clauses on

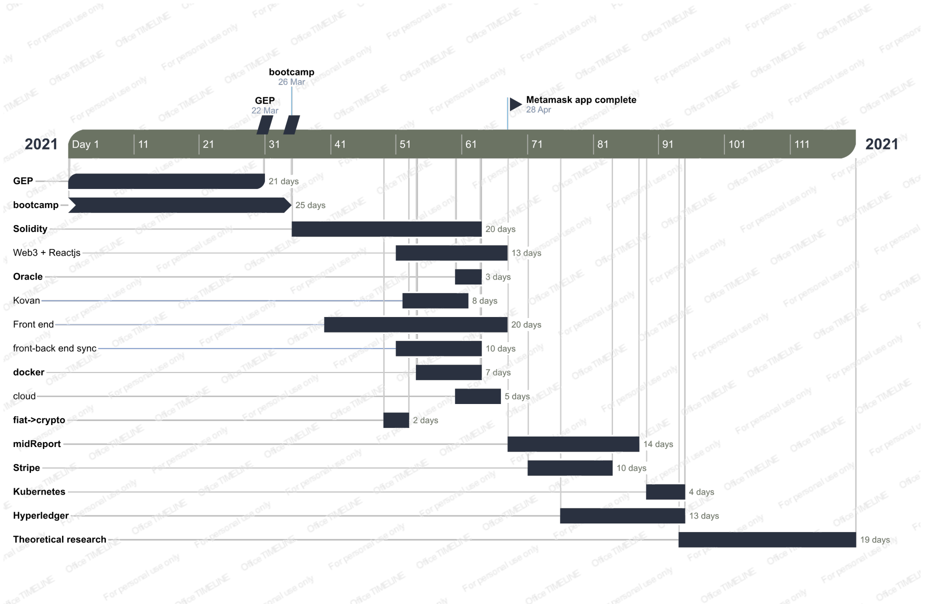


Figure 19: Project timeline

them. Unfortunately, i did not dive deep into how to use oracles. The decentralised oracles will be particularly difficult to set up.

- **T3 Reactjs front end**. Given previous experience i managed to do finish this part on time. Otherwise i would spend 3 times longer. The front end could use more work as it is only bare bones. However, i did not think it was worthwhile to invest any more time into it. The blog, about and contact page are pretty much finished and the website is well adapted for mobile support so the front end part is quite decent.

  Everything here is being done as a template and a proof of concept. The html fields are filled with "lorem ipsum" that can be substituted with whatever the campaign wants, the oracle question is only a test question and the smart contract implements the basic functionalities without going into specifics of any particular case. As a template it accomplishes everything that can be done without having a specific goal in mind.

- **T4 Linode**. Because the template is containerised on docker it allows me to not have to use the popular options like AWS or Azure and host it on Linode. Linode is a lot less complicated to setup than AWS and what i get for $5/month on Linode i would get for $99.27 according to [11]. AWS is flexibile as well as complicated in its pricing, so it will probably be lower $99.27 when adjusted specifically for my needs but it's too time consuming to try and test it.

- **T5 Usability**. ”changelly.com” link has been provided in the comments together with the address of the smart contract for direct donations without using the Metamask. User guides were omitted as it directly depends on the campaign management team. It would require to perform marketing and promotion research that is irrelevant to this particular project.

- **T6 Hyperledger** This part substitutes the ”alternative platforms” from earlier. Instead of Cardano i started learning Hyperledger Fabric after finishing my Ethereum version and also decided against it after realising i will not be able to do it on time. I started learning how to write Ethereum smart contracts in november and finished the website prototype in mid April. Trying to learn Hyperledger or Cardano and develop something usable in this timeframe was going to be rather ambitious.

- **T7 Theoretical research**. The remaining time i spent on theoretical research to provide better context to blockchain use. That includes sections 4 and 5.

  This section has been my exploration phase. Upon seeing how Hyperledger uses PoA consensus i thought that i didn’t like their approach so i started looking for alternatives and i found them. The trouble is, they are a lot more complicated to build and to learn than hyperledger. I am convinced hyperledger remains the dominant technology for building private blockchains. That, however, i believe will soon change. I had to investigate many other alternatives to know which to settle on. Algorand hosts smart contracts for financial systems, VeChain hosts smart contract for its partners in supply-chain area, Cardano is about to launch its smart contracts currently planned for September of this year and Polkadot is not too far behind. All of them can compete with Ethereum.

  Without all of this research into the development of culture of blockchain projects i would not be able to identify where i should invest my time. Even now i my understanding of blockchain projects is only surface-level. Every platform where i would want to write smart contracts requires a deeper understanding of its inner functions than i have now.

7.2 Costs

Personnel costs. Referencing [figure 18] and their salaries [table 2] we can calculate the overall costs. The project manager’s, tester’s and technical writer’s salaries are taken from [77] while developer’s from [78] .

Amortization. One of the aspects to take into account is the amortization of the physical resources. The only physical resource involved here, apart from cloud computing which will be discussed later, is the Acer Aspire e15 laptop. The non official lifespan average is 4-5 years for a typical laptop so we take 4.5years or 54 months. A new version of it is worth roughly 400€. We will assume 5 months of use hence it will be worth 400€ * 5/54 = **37€**.

Role	Salary €	Salary+SS	cost/hour	Role played by
Project Manager	48 923	63 600	30.58	S, T, GEPT
Developer	61 320	79 716	38.325	S
Tester	33 965	44 154.5	21.23	S
Technical Writer	26 765	34 794.5	16.73	S

Table 2: Average market salary by occupation. cost/hour is salary/2080 hours in a year. SS (social security) adds 30% to the salary cost. Key: S = student, T = tutor, GEPT = project organisation tutor/GEP

Cloud Computing will be used at the end of the project for hosting. Linode offers 5$/month (or **4.2€**/month) which will be sufficient.

Utilies. The bills of an average room in barcelona for electric, water, internet and rent(counted as workspace) costs tend to be 20€, 10€, 27€, 400€ per month respectively. The project duration is 5 months hence the cost will be calculated by x5 of every monthly cost. Combining the utility fees it sums up to 457€. In total 457€x5 = **2285€** for 5 months.

Maintenance. From experience, the equipment (in this project this only involves a personal laptop) requires some degree of maintenance that involves dealing with broken parts like a broken screen or charger and some software maintenance to keep it going roughly every 3 months. Broken components on average cost 50€ per year and the maintenance takes roughly 3 hours every 3 months. In 5 months of the project duration the repair will be 50/12 * 3 = 12.5€ and the maintenance 3h/3 * 5 = 5h = 191.625€ (maintenance is assumed to be performed by the developer himself with 38.325€ hourly wage like before). Sums up to **204.125€**.

Total will be shown in the table 3.

Type	Cost(€)
Project Manager	3669.6
Developer	9274.64
Tester	339.68
Technical Writer	2710.26
Amortization	37
Cloud	4.2
Utilities	2285
Maintenance	204.125
Total	**18524.505**

Table 3: Total cost. note: the prediction was 23021.066 €

7.3 Future Work

7.3.1 NFTs

NFTs(nun fungible tokens) for crowdfunding could be quite useful. One example would be that upon donating something to the charity the organisation could give out NFTs. So the donor receives a token in exchange for the donated item and the item is bound to the token. The token could be sent either directly to someone who needs it or to an organisation that manages it all. When the token owner sends the token now the receiver owns the item and the token can be reclaimed for the item. In other words the token will be used as a way of transfering ownership.

In its current state the tokens are pretty expensive as the gas fees for Ethereum are still high. Hopefully Ethereum will resolve this soon. Otherwise, other platforms are already racing to offer services where Ethereum is failing.

The other issue i found with NFTs is that to use them people would need crypto wallets and while the donors could own crypto wallets a more widespread adoption to be able to transfer the tokens will be more difficult. The blockchain adoption grows ever stronger so maybe in a few years it will be a practical idea.

7.3.2 Ethereum potential

As mentioned previously: VeChain is built on Ethereum and it has its own consensus mechanism, its oriented to enterprises, is built on top of another platform and has smart contract as well as tokens support in other words you could build another VeChain on top of VeChain. It would be a wonderful case study to see how much can be built on a smart contract platform without resorting to creating your own blockchain like Hyperledger Fabric does. With Hyperledger Fabric you would have to either set up physical nodes yourself or use cloud services like AWS that specifically has hyperledger support.

At the moment I have no idea how this could be done nor do I know how it works beyond its basic principle. Once I know enough about it i could perhaps have an idea what else to do with the most basic smart contract that i built in this project

7.3.3 Oracles

right now the most popular choice is chainlink. Each oracle is different and learning to use each of them will be completely different. It would take me around a month to properly setup and understand the functioning of chainlink to be able to properly create a basic data feed to a smart contract. The nodes are in the business of providing reliable information so it is a technological design as well as a business deal.

7.3.4 Other platforms

Cardano has been my aspiration from the very beginning but unfortunately it has yet to release its smart contract support. Cardano was founded by one of the Ethereum cofounders who left to bring his own vision to life. Cardano has a strong community support, it is moving very fast with development in comparison to other projects and promises a lot more scalability, transactions per second, token support and smart contract flexibility with selectively added metadata.

Algorand offers smart contract support and CBDCs are gaining popularity lately. It would be worthwhile to investigate how much can be done in this area.

Stellar. While I have not yet investigated enough about stellar, I know that it offers smart contract support for quick, secure and international payments. For potential banking solutions it could prove useful to see how it can be used.

8 Bibliography

References

[1] https://analyticsindiamag.com/origin-bitcoin-brief-history/

[2] https://www.infosys.com/insights/ai-automation/blockchain-adoption-journey.html

[3] https://www.mstweaks.com/the-biggest-threat-to-cybersecurity-social-engineering/

[4] https://www.fundable.com/learn/resources/guides/crowdfunding/crowdfunding-history

[5] https://ethereumworldnews.com/the-number-of-cryptocurrency-wallets-has-been-increasing-exponentially-statista-report/

[6] https://doublethedonation.com/tips/matching-grant-resources/nonprofit-fundraising-statistics/

[7] https://www.mordorintelligence.com/industry-reports/crowdfunding-market

[8] https://www.primetimecrime.com/Recent/Greed%20Corruption/nonprofitindustry.htm

[9] https://reality.eth.link/

[10] https://stripe.com/docs/keys

[11] https://www.linode.com/estimator/

[12] https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

[13] https://strom-report.de/electricity-prices-europe/

[14] https://braiins.com/blog/how-much-would-it-cost-to-51-attack-bitcoin

[15] https://news.bitcoin.com/65-of-global-bitcoin-hashrate-concentrated-in-china/

[16] https://bitnewstoday.com/news/bitcoin-miners-plans-to-leave-china-due-to-upcoming-tightening-of-regulation/

[17] https://forkast.news/hash-power-51-attack-rent-huge-vulnerability-proof-of-work-blockchain/

[18] https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack

[19] https://decrypt.co/41044/repeated-51-hacks-on-ethereum-classic-are-increasingly-frustrating-says-etc-labs-ceo

[20] https://forkast.news/hash-power-51-attack-rent-huge-vulnerability-proof-of-work-blockchain/

[21] https://99bitcoins.com/51-percent-attack/

[22] https://bitinfocharts.com/monero/

[23] https://bitinfocharts.com/bitcoin/

[24] RandomX was implemented 2020.11.20, see the hashrate growth from this date https://www.coinwarz.com/mining/monero/hashrate-chart

[25] https://cointelegraph.com/news/harvard-law-bfi-throws-10-5m-votes-behind-own-proposal-to-fund-defi-lobby-with-uni

[26] https://www.computerweekly.com/news/450414239/Businesses-blame-rivals-for-DDoS-attacks

[27] https://www.coindesk.com/filecoin-chainlink-integration-smart-contract-enabled-blockchains

[28] https://cryptopotato.com/why-ban-bitcoin-when-its-used-globally-pakistani-high-court-challenges-crypto-ban/
https://www.dcforecasts.com/altcoin-news/argentina-ordered-exchanges-to-provide-monthly-reports-on-users/
https://www.aljazeera.com/economy/2021/4/16/turkey-bans-crypto-payments-and-bitcoin-feels-the-pain
https://www.bloomberg.com/news/articles/2021-05-30/crypto-traders-defy-china-s-crackdown-with-secretive-bets

[29] https://www.dailywire.com/news/el-salvador-makes-history-becomes-first-country-to-make-bitcoin-legal-tender
https://www.tronweekly.com/cardano-chooses-georgia-as-the-starting-point-for-mass-adoption-tech-will-be-used-in-the-education-sector/

https://www.cryptoglobe.com/latest/2021/04/cardano-ada-helping-ethopia-with-the-worlds-largest-blockchain-deployment/
https://news.bitcoin.com/cardanos-cfund-first-capital-goes-to-israeli-fintech-startup-coti/
https://cardanojournal.com/atala-project-crypto-adoption-behind-the-corner-69
https://ripple.com/insights/santander-partners-with-ripple-to-bring-certainty-and-speed-to-international-payments/

[30] https://finance.yahoo.com/news/coinbase-suspend-xrp-trading-following-223007471.html

[31] https://coinmarketcap.com/headlines/news/A-Significant-Win-For-Ripple-Labs-As-The-SEC-Lawsuit-Continues/

[32] https://www.sec.gov/news/press-release/2020-146

[33] page 4 https://www.sullcrom.com/files/upload/sc-publication-doj-cryptocurrency-enforcement-framework.pdf

[34] https://www.cryptonewsboy.com/2020/10/08/chainalysis-and-texas-firm-win-million-dollar-irs-contract-to-crack-monero/

[35] https://cryptocoin.news/news/monero-gets-delisted-from-major-exchanges-45938/

[36] https://www.crowdfundinsider.com/2021/05/176018-monero-xmr-and-bitcoin-btc-trustless-atomic-swaps-now-live-comit-network-reveals/

[37] https://www.mckinsey.com/industries/financial-services/our-insights/counting-the-worlds-unbanked

[38] https://defipulse.com/

[39] page 42 plan on allocating more capital https://www.pwc.com/gx/en/financial-services/pdf/3rd-annual-pwc-elwood-aima-crypto-hedge-fund-report-(may-2021).pdf

[40] https://cointelegraph.com/news/aaves-path-to-decentralization-hopes-to-attract-institutional-investors
https://cointelegraph.com/news/defi-lending-platform-aave-reveals-private-pool-for-institutions

[41] https://www.crowdfundinsider.com/2020/08/165682-billion-dollar-defi-protocol-aave-awarded-electronic-money-institution-license-by-the-uks-financial-conduct-authority/

[42] https://medium.com/cardanorss/proof-of-steak-how-beefchain-uses-cardano-to-empower-ranchers-f05f8c12cb

[43] https://www.businessinsider.com/ever-given-insurer-said-suez-operators-drove-it-before-beached-2021-6?op=1

[44] https://www.cbc.ca/news/business/dairy-covid-19-1.5528331

[45] https://www.cbsnews.com/news/covid-vaccine-pfizer-distribution-logistical-nightmare/

[46] https://www.crypto-news-flash.com/demand-by-fortune-500-governments-for-cardanos-atala-prism-outpaces-labor-supply/

[47] https://thehill.com/opinion/white-house/556250-2-trillion-in-taxes-6-trillion-in-spending-22-trillion-in-borrowing-what

[48] https://www.bbc.com/news/world-us-canada-57285970

[49] https://www.travala.com/payment-options

[50] https://www.coinish.com/news/cryptocurrency/surfshark-a-new-vpn-on-the-block-accepts-btc-eth-xrp/

[51] https://www.expressvpn.com/internet-privacy/bitcoin-anonymity/step-by-step-guide/

[52] https://bitgild.medium.com/buy-gold-with-crypto-5cf7ecaff53a

[53] https://www.europeanmint.com/faq/

[54] https://www.namecheap.com/support/payment/bitcoin/

[55] https://bitcars.eu/pages/about-us-bitcars-buy-cars-with-bitcoin-and-crypto

[56] https://www.autocoincars.com/crypto.html

[57] https://bithome.ch/

[58] https://promotions.newegg.com/nepro/16-6277/index.html

[59] https://idoneus.io/support-hub/can-i-pay-in-btc-or-any-other-cryptocurrency/

[60] https://www.investing.com/news/cryptocurrency-news/paypal-is-hiring-crypto-engineers-amid-rumors-of-bitcoin-integration-2209239
6months later: https://cointelegraph.com/news/paypal-to-offer-crypto-payments-starting-in-2021

[61] https://cointelegraph.com/news/apple-seeks-to-hire-alternative-payments-manager-with-crypto-experience

[62] https://www.foxbusiness.com/personal-finance/coinbase-apple-google-wallets-crypto-purchases

[63] https://blockchair.com/ripple

[64] https://medium.com/@blockeq/transaction-fees-on-stellar-3d5e442fc00a

[65] https://btcmanager.com/dutch-central-bank-leading-role-cbdc-development/
https://finance.yahoo.com/news/russia-central-bank-governor-cbdc-201723820.html
https://finance.yahoo.com/news/china-cbdc-trial-expands-hainan-153128541.html

[66] https://www.forbes.com/sites/billybambrough/2021/06/13/move-over-dogecoin-tesla-billionaire-elon-musk-has-suddenly-sent-the-bitcoin-price-sharpy-higher/

[67] https://www.msn.com/en-us/news/technology/robinhood-can-t-handle-the-dogecoin-rally/ar-BB1fJGDm

[68] https://www.dailydot.com/unclick/dogecoin-jamaica-bobsled-olympics/

[69] https://www.coindesk.com/dogecoin-foundation-raise-50k-kenya-water-crisis

[70] https://nowpayments.io/blog/businesses-accepting-dogecoin
https://gtspirit.com/2021/05/14/us-collector-buys-a-bugatti-with-dogecoin-a-bugatti-bolide/
https://finance.yahoo.com/news/newegg-shoppers-now-pay-dogecoin-035000330.html
https://www.msn.com/en-us/money/markets/a-luxury-us-hotel-chain-will-accept-bitcoin-dogecoin-and-other-cryptocurrencies-as-payment/ar-BB1euoP7
https://finance.yahoo.com/news/pornhub-now-accepts-xrp-doge-210920772.html

[71] https://www.intro.torum.com/

[72] https://blog.coinbase.com/announcing-coinbase-fact-check-decentralizing-truth-in-the-age-of-misinformation-757d2392d61a?gi=88071f501619

[73] https://markets.businessinsider.com/currencies/news/oakland-athletics-as-tickets-100-dogecoin-major-league-baseball-2021-5-1030382996?op=1

[74] https://consensys.net/blog/news/the-inside-story-of-the-cryptokitties-congestion-crisis/

[75] https://nonfungible.com/market/history/cryptokitties

[76] https://bitcoinmarketcap.org/coins/unisocks

[77] https://www.glassdoor.es/Sueldos/index.htm

[78] https://cryptocurrencyjobs.co/blog/how-much-do-blockchain-jobs-pay/

[79] https://digiconomist.net/ethereum-energy-consumption

[80] https://www.netbooknews.com/tips/how-many-watts-laptop-use/

[81] https://mongersmint.com/bitcoins-consume-more-energy-than-all-of-argentina/

[82] https://www.nasdaq.com/articles/how-much-energy-does-bitcoin-really-consume-2021-05-13

[83] https://finance.yahoo.com/news/ethereum-emissions-carbon-climate-bitcoin-proof-of-work-proof-of-stake-cryptocurrency-eth2-100420055.html

[84] https://www.leafscore.com/blog/the-9-most-sustainable-cryptocurrencies-for-2021/

[85] https://heraldsheets.com/cardano-ada-flawlessly-beats-bitcoin-gold-and-banking-system-in-terms-of-energy-efficiency/
https://twitter.com/HukAleksandra/status/1394210467682394114/photo/1

[86] https://www.enterprisetimes.co.uk/2018/04/13/poseidon-with-stellar-blockchain-to-reduce-carbon-footprint/