TRANSFER OF ETHER USING

DAICOIN(CRYPTOSHAW)

A PROJECT REPORT

submitted by

DEON SAJI (CHN15CS040)
MANIMARAN N (CHN15CS070)
SHARAD JOE (CHN15CS108)
NEERAJ KARLUS (CHN15CS082)
to

The APJ Abdul Kalam Technological University
in partial fulfillment of the requirements for the award of the Degree

of

Bachelor of Technology

In

Computer Science and Engineering

Department of Computer Science and Engineering

College of Engineering, Chengannur, Kerala -689121

May 2019

DECLARATION

We undersigned hereby declare that the project report "Transfer of either using daicoin (CryptoShaw) ", submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by us under supervision of Ms.Arathy U.P, Assistant Professor. This submission represents our ideas in our own words and where ideas or words of others have been included, We have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Place: CHENGANNUR   DEON SAJI
Date:2019/06/11   MANIMARAN N
                                          SHARAD JOE
                                          NEERAJ KARLUS

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COLLEGE OF ENGINEERING,CHENGANNUR

CERTIFICATE

This is to certify that the report entitled **"Transfer of either using daicoin (CryptoShaw)"** submitted by **DEON SAJI**, **MANIMARAN N**, **SHARAD JOE**, **NEEAJ KARLUS** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Department of Computer Science and Engineering, College of Engineering, Chengannur, Kerala -689121 is a bonafide record of the project work carried out by them under my/our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Ms. Arathy U.P   **Ms.Shiny B**
Assistant Professor   Assistant Professor
Project Supervisor   Project Co-ordinator

Dr. Smitha Dharan
Professor and Head

ACKNOWLEDGEMENT

First and foremost we wish to express our wholehearted indebtedness to God Almighty for his gracious constant care and blessings showered over us for the successful completion of this project.

We are deeply indebted to **Dr. Jacob Thomas V**, Principal, College of Engineering, Chengannur and Associate Professor **Dr. Smitha Dharan**, Head of the Department of Computer Science and Engineering, College of Engineering, Chengannur, for providing and availing all the required facilities for undertaking the project in a systematic way.

We would like to express my deep gratitude to our staff-in-charge **Ms. Manjusha Nair S**, Assistant Professor, for the incite and encouragement given by her to improve the project. We are thankful to our guide **Ms. Arathy U.P**, Assistant Professor for providing good suggestions and valuable advices to improve the project.

Gratitude is extended to all teaching and non teaching staffs of Department of Computer Science and Engineering, College of Engineering, Chengannur, for the sincere directions imparted and the cooperation in connection with the project.

We are also thankful to our parents for the support given in connection with the project. Gratitude may be extended to all well-wishers and friends who supported us.

<div align="right">

DEON SAJI
MANIMARAN N
SHARAD JOE
NEERAJ KARLUS

</div>

ABSTRACT

Presently there is no stable system to transfer ether from one user to another. Dai coin is a cryptocurrency which has a stable market value which makes it unique from other cryptocurrencies so that we can use it for transferring ether. We are developing a platform to convert ether in-to equivalent daicoin. We can transfer the daicoin between users in a way similar to how GOOGLE PAY transfers real-world money.

Contents

List of Figures

CHAPTER 1

INTRODUCTION

1.1 Blockchain

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. Blockchain is considered a type of payment rail. Private blockchains have been proposed for business use. Sources such as the Computerworld called the marketing of such blockchains without a proper security model "snake oil".
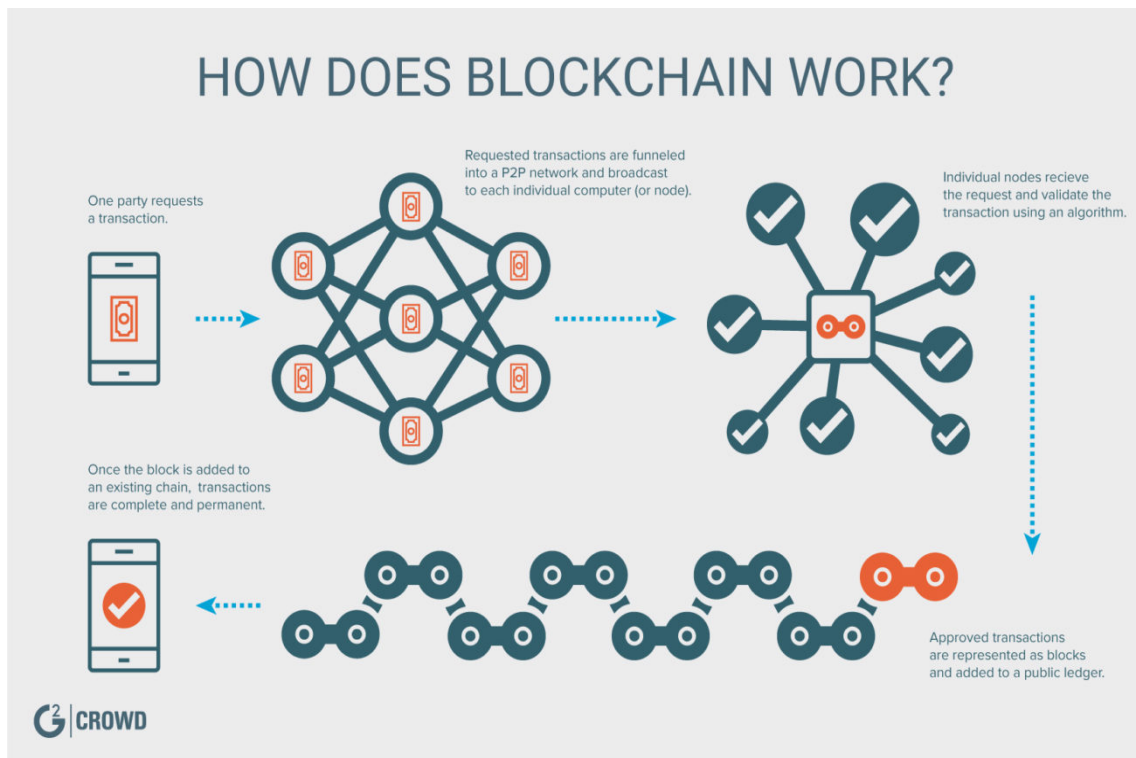
Figure 1.1.1: Working of Blockchain

1.2 CRYPTOCURRENCIES

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies are a kind of alternative currency and digital currency (of which virtual currency is a subset). Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems.

The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency. Since the release of bitcoin, over 4,000 altcoins (alternative variants of bitcoin, or other cryptocurrencies) have been created.

1.2.1 Bitcoin

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

Figure 1.2.1: Market rice(USD) Average USD market price across major bitcoin exchanges. Source: blockchain.com

1.2.2 Dai Coin

In later December of 2017, the company Maker released their long-awaited system for a decentralized stablecoin named "Dai".Dai is an Ethereum token whose vaue is pegged to 1 USD and will always be worth 1 USD, regardless of how much Dai is in existence. There is no centralized authority like Tether that backs its value, and no traditional bank that backs each Dai with a real US dollar. There is nothing that can be shut down, and no centralized authority that needs to be trusted. Dai lives entirely within the Ethereum blockchain using smart contracts.

The way Dai accomplishes this without centralized trust is incredibly clever and interesting, and in this post I will try my best to explain why Dai can be trusted and why it's a game changer for cryptocurrencies.

1.2.3 Ethereumn

Ethereum is a global, open-source platform for decentralized applications. On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world. It supports a modified version of Nakamoto consensus via transaction-based state transitions. Ether is a token whose blockchain is generated by the Ethereum platform.

Figure 1.2.2: Market prie variation analysis of ethereum

1.2.4 Litecoin

Litecoin is a powerful, political and economical tool which anyone, anywhere can use without permission to transact with anyone else in the world and partake in a genuinely global economy. The Litecoin blockchain is the largest global scrypt based network, operating with 100

Figure 1.2.3: Market price variation analysis of litecoin

1.2.5 Stellar

Stellar is a platform that connects banks, payments systems, and people. Integrate to move money quickly, reliably, and at almost no cost. With a team of top technology and finance professionals, the nonprofit Stellar.org expands access to low-cost financial services to fight poverty and maximize individual potential.

Figure 1.2.4: Market price variation analysis of stellar

DAI AS A GAME CHANGER

USD (Dai) can now be transferred instantly, across borders, and without fees (other than ETH gas fees).

Merchants can accept Dai with all the benefits of blockchain technology without the enormous risk of volatility. For example, merchants no longer need to worry about the price of Bitcoin fluctuating 15 percentage between when they receive payment and convert into fiat currency. If a merchant charges 19.99 USD for a T-Shirt and receives 19.99 Dai, they can be confident that they have 19.99 USD whether they cash out their Dai that same day or in 2 months.

Similarly, customers no longer have to worry about spending an asset that consistently goes up in value. The way most merchants currently accept cryptocurrencies as payment is to use a middleman like BitPay, which has all of the negatives associated with traditional payment processors. These include processing fees, limits, and rules on what industries they do business with. With middlemen like BitPay, merchants are simply offering another method of payment for their customers, but see no upside other than extra sales. Even worse, if BitPay decides they don't like you, they can shut you off without any warning for any reason.

With Dai, a merchant can process payments directly, as if they were receiving cash. If they choose to use a third-party, it's only to provide value-added services like e-commerce integrations, accounting software, and wallet management. No one can shut off the merchant's ability to receive payment.

Tether, or any other centralized stablecoin, can be hacked, shutdown, steal your money, and is always operating at the whims of politics and human fallibility. Indeed, there is an enormous amount of speculation that Tether is operating fraudulently. Not-so with Dai. As a true decentralized stablecoin, you only need to trust the blockchain.

2.1   How Dai Works

Dai is a masterpiece of game theory that carefully balances economic incentives in the pursuit of one goal, a token that is continuously approaching the value of 1 USD.

When Dai is worth above 1 USD, mechanisms work to decrease the price. When Dai is worth below 1 USD, mechanisms work to increase the price. The rational actors that take part in these mechanisms do so because they earn money anytime Dai is not perfectly worth 1 USD. This is why Dai is always floating slightly above or below 1 USD, an endless wave function bouncing infinitely close to 1 USD, but never quite achieving it. The farther Dai goes from 1 USD, the more incentive there is to fix it. This is the magic of Dai.

2.2   How Dai is Created

Dai is simply a loan against Ethereum. First, ETH is turned into "wrapped ETH" (WETH), which is simply an ERC20 wrapping around ETH. This "tokenizes" ETH so it can be used like any other ERC20 token.

Next, WETH is turned into "pooled ETH" (PETH), which means it joins a large pool of Ethereum that is the collateral for all Dai created. Once you have PETH, you can create a "collateralized debt position" (CDP), which locks up your PETH and allows you to draw Dai against your collateral, which is PETH.

As you draw out Dai, the ratio of debt in the CDP increases. There is a debt limit that sets a maximum amount of Dai you can draw against your CDP.

Once you have Dai, you can spend or trade it freely like any other ERC20 token.

<div align="center">

CHAPTER 3

LITERATURE REVIEW

</div>

3.1 Asynchronous Mining of Ethereum Cryptocurrency, Pavel V. Sukharev; Dmitry S. Silnov

Cryptocurrency mining is an important process that ensures the reliability of cryptocurrency system. A significant computing power is used in cryptocurrency mining. One of the most important tasks in cryptocurrency mining is to ensure the maximum performance of used computing capacities. In this paper we review the existing Ethereum mining algorithm and search for possibilities for speeding up the mining by applying a new asynchronous mining algorithm.

3.2 Managed Blockchain Based Cryptocurrencies with Consensus Enforced Rules and Transparency, Peter Mell

Blockchain based cryptocurrencies are usually unmanaged, distributed, consensus-based systems in which no single entity has control. Managed cryptocurrencies can be implemented using private blockchains but are fundamentally different as the owners have complete control to do arbitrary activity without transparency (since they control the mining). In this work we explore a hybrid approach where a managed cryptocurrency is maintained through distributed consensus based methods. The currency administrator can perform ongoing management functions while the consensus methods enforce the rules of the cryptocurrency and provide transparency for all management actions. This enables the introduction of money management features common in fiat currencies but where the managing entity cannot perform arbitrary actions and transparency is enforced. We thus eliminate the need for users to trust the currency administrator but also to enable the administrator to manage the cryptocurrency. We demonstrate how to implement our approach through modest modifications to the implicit Bitcoin specification, however, our approach can be applied to most any blockchain based cryptocurrency using a variety of consensus methods.

3.3 A Study of Current Cryptocurrency Systems, R. Raju ; M. SaiVignesh ; K. Infant Arun Prasad

Cryptocurrencies have transpired as one of the trending financial software systems. They depend on a secure and consigned ledger data structure; mining being an indispensable part of such systems. Mining reconsiliates records of past transactions to the distributed register known as the Blockchain, that allows users to reach secure, robust and concord for each transaction. Mining also introduces wealth in the form of new units of currency named as "bitcoins". Cryptocurrencies lack a central delegate or authority to mediate transactions because they were designed as peer to-peer end sub-systems. They rely on miners to validate and scrutinize their transactions. Hence Cryptocurrencies require a strong, secure mining algorithms. In this article we survey, compare and contrast the current mining techniques as used by major Cryptocurrencies. We scrutinize the strengths, weaknesses, and possible threats to mining strategy. Overall, a perspective on how Cryptocurrencies mine the datasets, where they have comparable performance and assurance, and where they have unique threats and strengths are outlined.

RECENT TRENDS IN CRYPTOCURRENCY MARKETS

Most cryptocurrencies are pegged to Bitcoin and, due to Bitcoin's huge price swings and volatility, this affects the prices of other cryptocurrencies. The idea behind the stablecoin is to have a coin with a fixed price that isn't subject to sudden price swings. This "stablecoin" is then pegged to, and backed by, actual fiat currency to guarantee its stability.

The most notable of all stablecoins is Tether, and most exchanges now pair every major cryptocurrency and some smaller altcoins to Tether's USDT which is equal to a dollar.

This is generally supposed to be a good thing, because, due to being backed by the dollar, pegging a cryptocurrency to Tether makes it more stable than pegging it to the more volatile Bitcoin. Well, this should be the case assuming that Tether is actually indeed backed 1:1 by the dollar as is generally assumed. However, damning reports to the contrary have emerged.

Over the last 5 years the global market cap of cryptocurrencies has seen tremendous growth. A lot of cryptocurrencies have come and gone over this period. Despite this, investors are more interested than ever before in altcoins. Only time will tell whether a large number of cryptocurrencies can coexist or if we'll see a smaller number of coins gain dominance.

The price dip forces people to turn into something that's more stable and cryptoshaw will provide all the users with Dai which is stable.

CRYPTO SHAW

A web exchange platform for the conversion of cryptocurrencies in the form of Dai.A platform that is not affected by the current market rates during transaction. Every Dai is backed by another asset of value. Our collateral portfolio is diversified, allowing multiple assets to guarantee the value of each Dai. Anyone can view the information about the locked collateral backing each Dai, including its safety profile. Dai is a reliable source of stability in the face of volatility. Every Dai is backed in excess by collateral at all times, so you never have to worry about its value moving up or down.

5.1 Benefits Of CyptoShaw

Figure 5.1.1: Benifits of Cryptshaw

User Friendly - It is based on a simple User Interface that has send and request options. Any cryptocurrency can be converted into dai which is highly stable. The user need not be a cryptogeek to use this pltform. The User don't have to worry aboout the undrlying technologies and processes.

5.2   Major Challenges

Proper management of gas

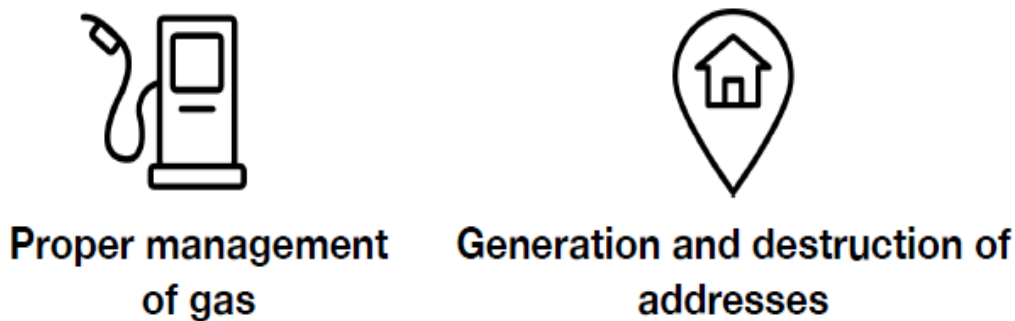Generation and destruction of addresses

Figure 5.2.1: Major Challenges of CryptoShaw

"Gas" is the name for a special unit used in Ethereum. It measures how much "work" an action or set of actions takes to perform: for example, to calculate one Keccak256 cryptographic hash it will take 30 gas each time a hash is calculated, plus a cost of 6 more gas for every 256 bits of data being hashed. Every operation that can be performed by a transaction or contract on the Ethereum platform costs a certain number of gas, with operations that require more computational resources costing more gas than operations that require few computational resources.

The reason gas is important is that it helps to ensure an appropriate fee is being paid by transactions submitted to the network. By requiring that a transaction pay for each operation it performs (or causes a contract to perform), we ensure that network doesn't become bogged down with performing a lot of intensive work that isn't valuable to anyone. This is a different strategy than the Bitcoin transaction fee, which is based only on the size in kilobytes of a transaction. Since Ethereum allows arbitrarily complex computer code to be run, a short length of code can actually result in a lot of computational work being done. So it's important to measure the work done directly instead of just choosing a fee based on the length of a transaction or contract.

So if gas is basically a transaction fee, how do you pay it? This is where it gets a little tricky. Although gas is a unit that things can be measured in, there isn't any actual token for gas. That is, you can't own 1000 gas. Instead, gas exists only inside of the Ethereum virtual machine as a count of how much work is being performed. When it comes to actually paying for the gas, the transaction fee is charged as a certain number of ether, the built-in token on the Ethereum network and the token with which miners are rewarded for producing blocks.

There is also a chance that the random address generated may be repeated again. This must be avoided. Each use should be given a truly unique address.

5.3 Data Flow Diagram

Figure 5.3.1: DFD level 0

Level 1

Request Dai		Transfer funds to Address
↓		↑
Adress Generation	→	Conversion to Dai
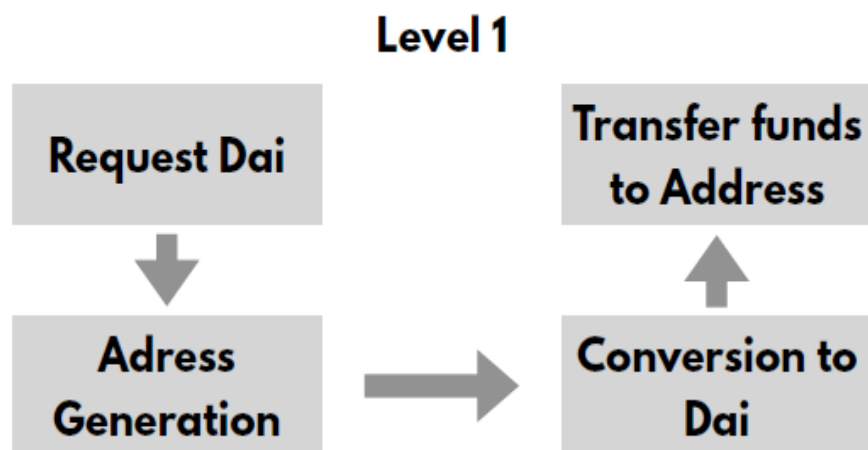
Figure 5.3.2: DFD level 1

5.4   Use Case Diagram

CryptoShaw

Login — Service Authenticator

Request/Send

Address Generation — Wallet Address generator

Conversion To Dai → Store The Dai
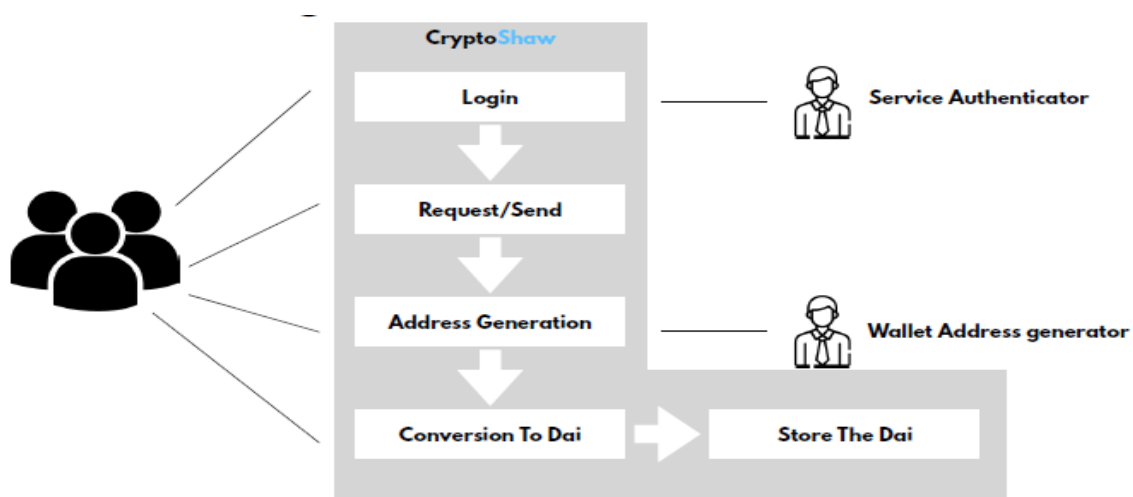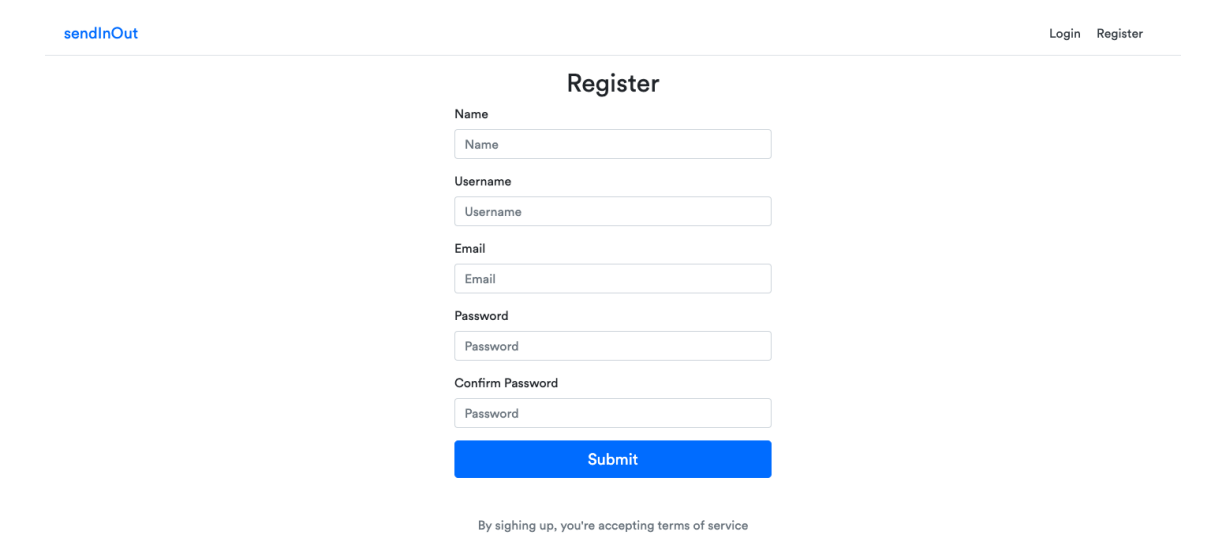
Figure 5.4.1: Use case diagram

5.5   An Overview of Cryptoshaw

5.5.1   User registration
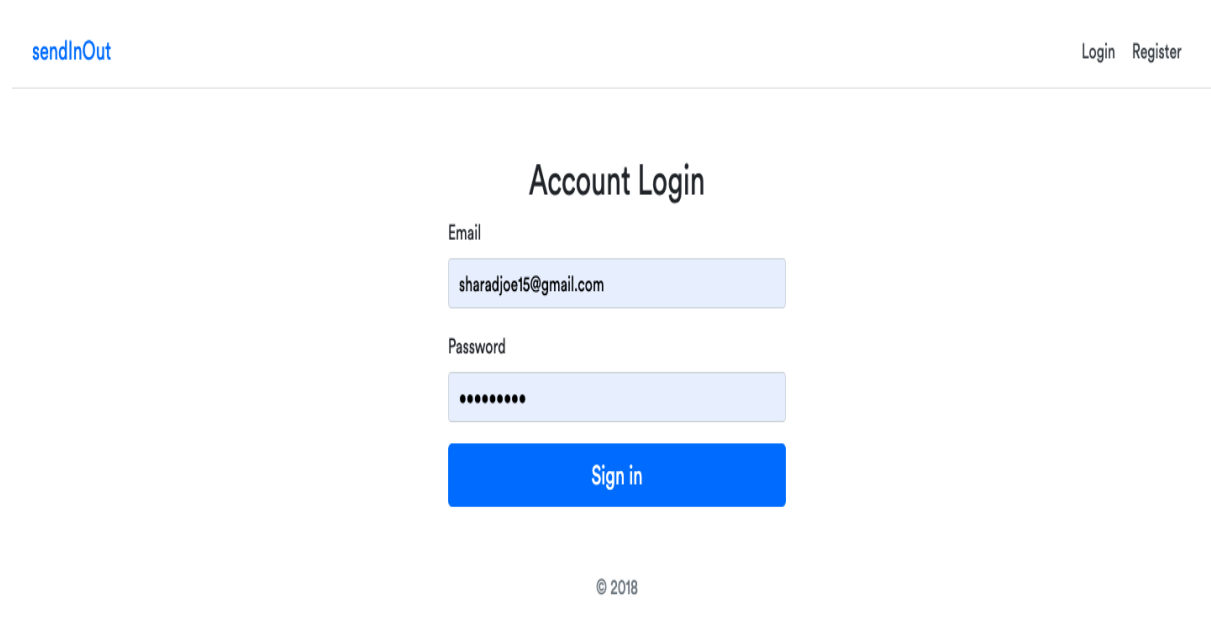
Figure 5.5.1: Use registration UI

5.5.2   User login

Figure 5.5.2: Use login UI

5.5.3   Transfering cryptocurrency using daicoin

Figure 5.5.3: CryptoShaw UI

"Gas" is the name for a special unit used in Ethereum. It measures how much "work" an action or set of actions takes to perform: for example, to calculate one Keccak256 cryptographic hash it will take 30 gas each time a hash is calculated, plus a cost of 6 more gas for every 256 bits of data being hashed. Every operation that can be performed by a transaction or contract on the Ethereum platform costs a certain number of gas, with operations that require more computational resources costing more gas than operations that require few computational resources.

The reason gas is important is that it helps to ensure an appropriate fee is being paid by transactions submitted to the network. By requiring that a transaction pay for each operation it performs (or causes a contract to perform), we ensure that network doesn't become bogged down with performing a lot of intensive work that isn't valuable to anyone. This is a different strategy than the Bitcoin transaction fee, which is based only on the size in kilobytes of a transaction. Since Ethereum allows arbitrarily complex computer code to be run, a short length of code can actually result in a lot of computational work being done. So it's important to measure the work done directly instead of just choosing a fee based on the length of a transaction or contract.

So if gas is basically a transaction fee, how do you pay it? This is where it gets a little tricky. Although gas is a unit that things can be measured in, there isn't any actual token for gas. That is, you can't own 1000 gas. Instead, gas exists only inside of the Ethereum virtual machine as a count of how much work is being performed. When it comes to actually paying for the gas, the transaction fee is charged as a certain number of ether, the built-in token on the Ethereum network and the token with which miners are rewarded for producing blocks.

There is also a chance that the random address generated may be repeated again. This must be avoided. Each use should be given a truly unique address.

CHAPTER 6

PLATFORM AND FRAMEWORKS

INVOLVED

6.1 Backend

Express:- It is a minimal and flexible Node.js web application framework that provides a robust set of features for web and mobile applications. Express provides a thin layer of fundamental web application features, without obscuring Node.js features.Many popular frameworks are based on Express.

MongoDB:- It is a document database with the scalability and flexibility that you want with the querying and indexing. MongoDB stores data in flexible, JSON-like documents, meaning fields can vary from document to document and data structure can be changed over time. The document model maps to the objects in your application code, making data easy to work with.

MongoDB is a distributed database at its core, so high availability, horizontal scaling, and geographic distribution are built in and easy to use.

Web3js:- web3.js is a collection of libraries which allow you to interact with a local or remote ethereum node, using a HTTP or IPC connection.

Mongoose:- Mongoose is an Object Data Modeling (ODM) library for MongoDB and Node.js. It manages relationships between data, provides schema validation, and is used to translate between objects in code and the representation of those objects in MongoDB.

6.2   Frontend

Bootstrap:- It is is the most popular CSS Framework for developing responsive and mobile-first websites. Bootstrap 4 is the newest version of Bootstrap.

Reactjs: ReactJS basically is an open-source JavaScript library which is used for building user interfaces specifically for single page applications. It's used for handling view layer for web and mobile apps.

React also allows us to create reusable UI components. React allows developers to create large web applications which can change data, without reloading the page. The main purpose of React is to be fast, scalable, and simple. It works only on user interfaces in application. This corresponds to view in the MVC template. It can be used with a combination of other JavaScript libraries or frameworks, such as Angular JS in MVC.

CHAPTER 7

CONCLUSION

Dai is an asset-backed, hard currency for the 21st century. The first decentralized stable-coin on the Ethereum blockchain. With Dai, anyone, anywhere has the freedom to choose a money they can place their confidence in. A money that maintains its purchasing power. Dai is a reliable source of stability in the face of volatility. Every Dai is backed in excess by collateral at all times, so you never have to worry about its value moving up or down. Every Dai is backed by another asset of value. Our collateral portfolio is diversified, allowing multiple assets to guarantee the value of each Dai. Anyone can view the information about the locked collateral backing each Dai, including its safety profile. During periods of high market instability, Dai offers a safe harbor to store value without having to exit the crypto space. High volatility creates an uncertain lending environment as borrowers and lenders cannot comfortably plan for the future. Dai's low volatility makes them a perfect medium for a stable, predictable loan.

No market worry for anyone usingour platform. The way dai works ensure no loss as dai has a constant value in the varying market. No dip or hike in price for Dai.

REFERENCES

[1] dhttps://makerdao.com/dai/

[2] Asynchronous Mining of Ethereum Cryptocurrency, Pavel V. Sukharev ; Dmitry S. Sil-
     nov,2017

[3] A Study of Current Cryptocurrency Systems, R. Raju ; M. SaiVignesh ; K. Infant Arun
     Prasad,2018

[4] Managed Blockchain Based Cryptocurrencies with Consensus En- forced Rules and Trans-
     parency, Peter Mell.s