



Used2Block

Used2Block

REQUIREMENTS SPECIFICATION

Student Number	Name
2015314213	이재원 Jae Won Lee
2013313737	김무성 Mu Sung Kim
2015318385	김현우 Hyun Woo Kim
2015310250	김동환 Dong Hwan Kim
2016315146	이상우 Sang Woo Lee

Contents

1. Preface.....	9
1.1. Readership.....	9
1.1.1. User Requirement Readership	9
1.1.2. System Requirement Readership.....	9
1.2 Document Structure	9
1.2.1. Introduction	9
1.2.2. Glossary	10
1.2.3. User Requirements Specification	10
1.2.4. System Architecture	10
1.2.5. System Requirements Specification.....	10
1.2.6. System Models.....	10
1.2.7. System Evolution.....	10
1.2.8. Appendices	11
1.2.9. Index.....	11
2. Introduction	11
2.1. Needs	12
2.2. System Overview	14
2.3 Expected Effects.....	14
2.3.1. 품질 보증	14
2.3.2. 신뢰성 강화.....	15

2.3.3. 사용자 중심	15
2.3.3. 안정성 강화.....	15
2.3.4. 빠른 거래 속도.....	15
3. Glossary	16
4. User Requirements Definition	17
4.1. Functional Requirements.....	17
4.1.1. Sign in	17
4.1.2. Login/ Logout.....	17
4.2.3. User's profile Management	18
4.2.4. Creating Wallet.....	18
4.2.5. Searching	19
4.2.6. Selling Product.....	19
4.2.7. Buying Product.....	19
4.2.8. Manage product.....	20
4.2.9. Verifying Transaction.....	20
4.2.10. Wallet Management.....	21
4.2 Non-functional Requirements.....	21
4.2.1 Product requirement.....	21
4.2.1.1. Security.....	21
4.2.1.2. Reliability	22
4.2.1.3. Speed	22
4.2.1.4. Usability.....	22

4.2.2 Organization requirement	22
4.2.2.1. Delivery requirement.....	23
4.2.2.2. Implementation requirement	23
4.2.3 External requirements.....	23
4.2.3.1. Interoperability.....	23
4.2.3.2. Ethical requirement.....	23
4.2.3.3. Legislative requirement.....	24
5.1. Frontend Architecture	25
5.2. Backend Architecture	27
5.3. ETH blockchain system.....	28
5.4. Application System.....	28
5.4.1 Transaction Management.....	28
5.4.2 User Management.....	29
5.4.3 Product Management.....	29
5.4.4 Cryptocurrency Management	29
6. System Requirements Definition.....	29
6.1. Functional Requirements.....	30
6.1.1. Sign up (register).....	30
6.1.2. Login	31
6.1.3. Logout.....	32
6.1.4. User's profile Management	32
6.1.5. Creating Wallet.....	33

6.1.6. Searching	34
6.1.7. Selling Product.....	35
6.1.8. Buying Product.....	35
6.1.9. Validation	36
6.1.10. Manage product	37
6.1.11. Product Page	37
6.1.12. Verifying Transaction	38
6.1.13. Wallet Management.....	39
6.1.14. Crypto-Currency Exchange.....	40
6.2 Non-functional Requirements.....	41
6.2.1. Product requirement.....	41
6.2.1.1 Security.....	41
6.2.1.2. Reliability	41
6.2.1.3. Speed	42
6.2.1.4. Usability.....	42
6.2.2. Organization requirement.....	43
6.2.2.1. Delivery requirement.....	43
6.2.2.2. Implementation requirement	43
6.2.3. External requirements	43
6.2.3.1. Interoperability.....	43
6.2.3.2. Ethical requirement.....	44

6.2.3.3. Legislative requirement.....	44
6.3 System Scenario	44
6.3.1. 서비스 가입/접속/접속_종료 시나리오	45
6.3.1.1. 서비스 가입	45
6.3.1.1.1 Initial Assumption	45
6.3.1.1.2 Normal flow of events	45
6.3.1.1.3. What can go wrong.....	45
6.3.1.1.4. System state on completion	45
6.3.1.2. 로그인.....	46
6.3.1.2.1. Initial Assumption	46
6.3.1.2.2. Normal flow of events	46
6.3.1.2.3. What can go wrong.....	46
6.3.1.2.4. System state on completion	46
6.3.1.3. 로그아웃	47
6.3.1.3.1. Initial Assumption	47
6.3.1.3.2. Normal flow of events	47
6.3.1.3.3. What can go wrong.....	47
6.3.1.3.4. System state on completion	47
6.3.2 가상 Wallet 관리 시나리오	48
6.3.2.1. Wallet 관리.....	48
6.3.2.1.1. Initial Assumption	48

6.3.2.1.2. Normal flow of events.....	48
6.3.2.1.3. What can go wrong.....	48
6.3.2.1.4. System state on completion	48
6.3.2.2. Crypto-Currency Exchange.....	49
6.3.2.2.1. Initial Assumption	49
6.3.2.2.2. Normal flow of events.....	49
6.3.2.2.3. What can go wrong.....	49
6.3.2.2.4. System state on completion	49
6.3.3 거래 시나리오	50
6.3.3.1. 판매자의 상품 등록	50
6.3.3.1.1. Initial Assumption	50
6.3.3.1.2. Normal flow of events.....	50
6.3.3.1.3. What can go wrong.....	50
6.3.3.1.4. System state on completion	50
6.3.3.2. 구매자의 검색 및 구매주문	51
6.3.3.2.1. Initial Assumption	51
6.3.3.2.2. Normal flow of events.....	51
6.3.3.2.3. What can go wrong.....	51
6.3.3.2.4. System state on completion	51
6.3.3.3. 블록체인 거래 검증과정	52
6.3.3.3.1. Initial Assumption	52

6.3.3.3.2. Normal	52
6.3.3.3.3. What can go wrong.....	52
6.3.3.3.4. System state on completion	52
6.3.3.4. 해당 거래 모델에 대한 참조용 도식	53
7. System Model.....	54
7.1. Context Models.....	55
7.1.1. Context Diagram	55
7.2. Process Diagram.....	56
7.2.1. Sign up process	56
7.2.2. Overall process.....	57
7.2. Interaction Models.....	58
7.2.1. Use case Diagram	58
7.2.2. Tubular description for each use case	59
7.2.2.1. Sign up	59
7.2.2.2. Login.....	59
7.2.2.3. Search	60
7.2.2.4. View item details	60
7.2.2.5. Purchase item.....	60
7.2.2.6. Write review	61
7.2.2.7. Post item	61
7.2.2.8. Delete item	62
7.2.2.9. View transaction history	62

7.3. Behavioral Models	63
7.3.1. Data-Driven Modeling	63
7.3.1.1. Tourist user.....	오류! 책갈피가 정의되어 있지 않습니다.
7.3.1.2. Member user	오류! 책갈피가 정의되어 있지 않습니다.
8. System Evolution.....	64
8.1. 경매 시스템.....	64
8.2. 품질 보증 시스템	64
8.3. 상품 추천 시스템	65
8.4. 개인정보 보호를 위한 hash 값 활용	65
8.5 모바일 어플리케이션 연동	65
9. Appendices	66
10. Indexes	67
10.1. Tables.....	67
10.2. Figures	67
10.3. Diagrams	67
11. References	68

1. Preface

This chapter comprises of expected readership of the document and gives overall introduction to remaining chapters.

1.1. Readership

This document aims two kinds of readership.

1.1.1. User Requirement Readership

Users of our system is expected to read the user requirements. The corresponding chapter is written from user's point of view. An user would not use our system when the user requirement is full of formal and technical specification. Thus, natural language is used by developers in the team with potential users in mind.

1.1.2. System Requirement Readership

Developers of our system is expected to read and understand the system requirement deeply. The operational constraints and system functionalities are represented using structural language. The system requirement would be used in system design and implementation as a reference, therefore it must be done in a completely formal document.

1.2 Document Structure

1.2.1. Introduction

The domain is defined and the market analysis is the main highlight of this chapter. The abstract structure of the system and functionalities are explained. Moreover,

expected effects of the system implementation is briefed.

1.2.2. Glossary

The technical terminologies used throughout the document are defined with examples from our system. This chapter is for all the stakeholders of our system to read, thus the terminologies are explained in detail.

1.2.3. User Requirements Specification

Functional and non-functional requirements of our system are demonstrated from user's perspective. Diagrams are used along with natural language to help user's understanding.

1.2.4. System Architecture

Architecture of our system is demonstrated. The functionalities are explained based on subsystems.

1.2.5. System Requirements Specification

Based on the user requirement specification, the functional and non-functional requirements are defined. This chapter would be referenced throughout the system design, architecture design and implementation of our system, thus diagrams are used actively.

1.2.6. System Models

Components of our system, relationship among the components and the external environment are expressed using diagrams.

1.2.7. System Evolution

Limitation of system implementation is explained along with the operational constraints. Expected changes in the market are mentioned with possible solutions.

1.2.8. Appendices

Materials that are exempted from the document are combined into this chapter.

1.2.9. Index

Diagrams, charts and figures used in the document are listed with indexes.

2. Introduction

This chapter defines the domain of our system. The market analysis is explained with figures. The structure of the system and functionalities are briefed.

2.1. Needs

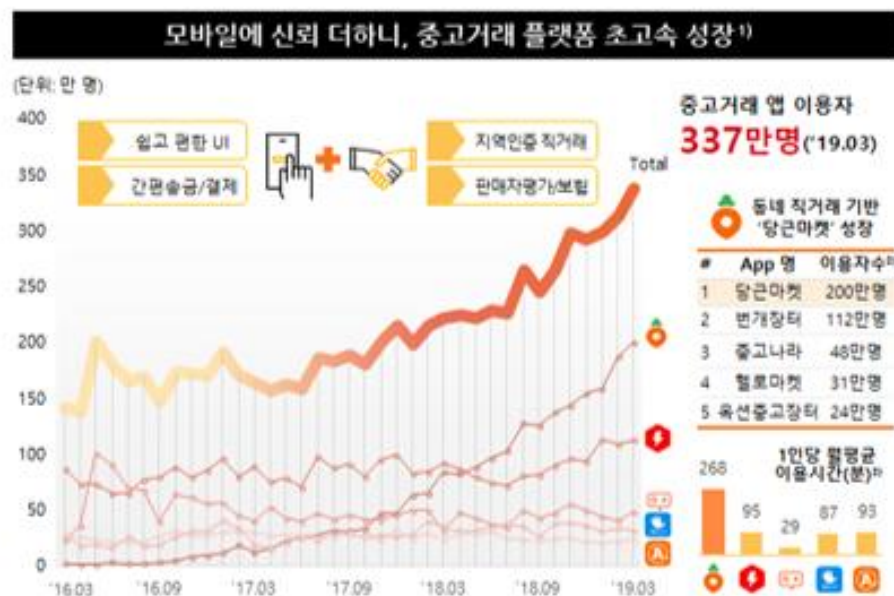


Figure 1. 모바일 중고거래 시장 조사.

미디어 조사기관인 닐슨 코리아에 따르면, 현재 중고거래 앱 이용자는 점차 증가하여 337만명에 이른다고 한다. Figure 1처럼 특히 지역 기반 거래를 중요시하는 당근마켓의 경우 유저가 200만명에 이른다는 통계자료도 있다. 또한 번개장터의 경우 2018년 연간 거래액이 2591억에 이르렀고 우리나라에서 제일 큰 규모의 중고나라의 경우 2018년 연간 거래액이 3421억으로 조사되었다. 중고나라의 모바일 앱은 550만건의 다운로드 수 기록도 보유하고 있다.

시장이 커짐에 따라 이에 관련된 문제도 드러나고 있다. 현재 중고시장에서의 큰 문제는 판매자를 신뢰할 수 없다는 것이다. 정보의 비대칭성 때문에 판매하는 제품이 허위 매물인지 아닌지 판단할 수 있는 수단이 전혀 없기 때문이다. 또한 해당 판매자가 실제

로 매물을 보냈는지, 또는 벽돌을 보냈는지 확인할 방법도 없다.

기존 중고나라에서는 안전거래 제도가 도입이 되었다. 중고나라 사업자가 거래 중계자 역할을 대신해 거래를 참여하고, 구매자가 선 대금 결제 후 제품 수령으로 구매 확정 버튼을 누르면 판매자에게 대금을 지급하는 제도이다. 중고나라 사업자는 이 제도를 통해 거래에 대한 수수료를 받습니다. 예를 들자면, 신용카드 결제, 계좌이체 결제, 무통장 입금 결제는 각 판매금액의 3.74%, 1.65%, 그리고 1건당 275원이 수수료를 챙겨간다.

이 제도의 최대 장점은 구매자가 판매자를 모르더라도 허위 매물 거래의 위험을 예방할 수 있다는 것이다. 물론 돈을 홀딩하는 번거롭고 긴 과정 때문에 이를 판매자가 기피하기도 하고, 안전거래라고 할 지라도 물건이 도착하기 전까지는 상태가 괜찮은 지 확인할 수는 없다.



Figure 2.

만약 거래 과정에서 분쟁이 생겼더라도, 중고거래는 개인과 개인의 거래이기 때문에 법적으로 보호받기도 힘든 상황이다. 사기를 쳐서 물건을 못 받았다면 사기죄로 처벌할 수 있지만, 물건에 판매자가 언급하지 않은 결함이 있거나 혹은 문제가 발생했을 경우, 현재 한국에서는 소비자가 보호받을 방법이 전혀 없는 상황이다.

중고나라 외에도 당근마켓에서는 직거래를 통해 문제를 해결하려고 했다. 현재 사는 지역의 매물만 보여줌으로써 직거래를 유도하고, 상품을 직접 눈으로 확인하며 구매하는 과정을 거쳐 안정성을 획득한다. 하지만, 세탁기, 공기청정기 등 가전제품과 같은 무거운 물건의 경우, 직거래를 통해 거래하기 어려운 게 사실이며, 실제로 구매자와 판매자가 서로 시간을 맞추어 만나는 것도 번거롭다는 의견들이 많았다.

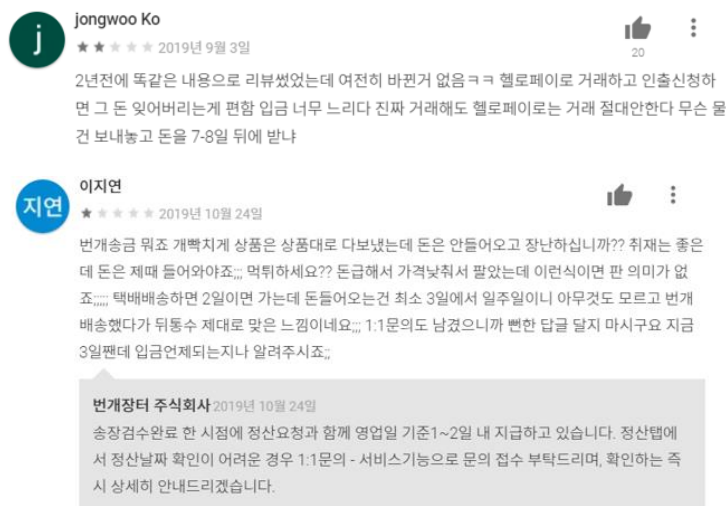


Figure 6.

2.2. System Overview

Used2Block은 PoS 알고리즘을 차용한 새로운 PoC 알고리즘을 중고 시장 거래에 도입함으로써 기존 중고거래시장에 주요 문제점이었던 신뢰성을 강화한다. 또한 안전거래 과정을 생략하고 PoC을 통해 거래를 증명하기 때문에 안전거래의 주요 문제점인 느린 거래 속도를 높일 수 있다.

PoC란 Proof of Collective Intelligence의 준말로 집단 지성의 증명이라는 뜻이다. 즉, 중고 거래에 집단 지성을 이용해 해당 거래가 안전한 지 여부를 판단하는 과정을 도입하여 기존의 1대 1 거래가 아닌 1대 N 중고 거래를 선보인다. 해당 과정에 참여한 인원은 모두 가상화폐를 보상으로 받게 된다.

해당 블록체인은 Oracle 서버와 연동되어 사용자가 쉽게 사용할 수 있도록 Hybrid 형태로 구성된다. 유저는 블록체인을 직접적으로 이용하지 않고 Used2Block 서비스를 이용해 기존의 웹 브라우저를 통해 블록체인에 접근할 수 있다.

2.3 Expected Effects

2.3.1. 품질 보증

- 거래 검증 과정을 통해 판매자의 신뢰도를 증명해 물건의 품질도 따라 증명 가능

하다.

2.3.2. 신뢰성 강화

- 블록 체인 기술을 통해 기록된 판매자의 거래 내역을 통해 판매자의 신뢰성을 가늠할 수 있다.
- 거래 검증이라는 프로세스를 통해 한번 더 판매자의 신뢰성을 검증할 수 있다.

2.3.3. 사용자 중심

- 판매자 신뢰도에 대한 검증이 이루어지는 과정에서, 검증에 참가한 사용자들에게 인센티브가 주어진다.
- 해당 검증에 대한 수수료 비용은 서비스 제공자가 아닌 거래 참여자들에게 돌아간다.

2.3.3. 안정성 강화

- 로그를 남기는 가상 화폐 활용해, 거래에 대한 기록을 항상 남길 수 있다
- 거래 검증에 참여 하는 인원이 많아질 수록 시장이 더 안정적

2.3.4. 빠른 거래 속도

- 기존의 안전 거래가 아닌 Used2Block 서비스의 Consensus Algorithm을 통해 거래를 빠르게 처리
- 빠른 거래 처리로 사용자의 편의성 증대

3. Glossary

4. User Requirements Definition

해당 챕터에서는 시스템이 핵심으로 제공하는 기능적 요구사항인 서비스와 부가적으로 충족시켜야 하는 비기능적 요구사항 두가지로 나누어 설명한다. 해당 챕터에서는 사용자를 대상으로 작성되는 부분으로 구체적인 기술은 지양하며 자연어와 시각 자료를 이용해 설명한다.

4.1. Functional Requirements

4.1.1. SignIn

사용자가 서비스를 이용하기 위해 서버에 회원으로 등록하는 기능이다. 회원가입시에는 사용자가 이메일, 전화번호, 주소, 아이디, 비밀번호를 입력해 진행한다.

4.1.2. Login/ Logout



The image shows a login interface for 'Used2Block'. At the top is a logo consisting of a shopping basket icon with a keyhole and the text 'Used2Block'. Below the logo are two input fields: the first is labeled 'Username' with a person icon, and the second is for a password, indicated by a key icon and four dots. Below these fields is a toggle switch for '자동 로그인' (Auto Login), which is currently turned on. A 'Log in' button is positioned below the toggle. At the bottom, there are four links: '회원가입' (Sign Up), 'ID 찾기' (Find ID), 'Password 찾기' (Find Password), and '회원탈퇴' (Logout).

회원으로 가입된 사용자가 시스템에 인증 받는 절차이다. 인증 과정 이후 해당 사용자는 'Used2Block' 서비스를 이용할 수 있다.

4.2.3. User's profile Management

사용자 자신의 프로필 정보를 확인하고 수정할 수 있는 기능을 제공한다. 해당 페이지에서는 현재 가상 화폐의 잔고, 거래 내역, 개인 정보가 포함된다. 만약 자신의 계정이 존재하지 않는다면 가입 페이지로 이동해 가입을 진행하게 된다.

4.2.4. Creating Wallet

해당 서비스를 이용하기 위해서는 가상 화폐의 소유권을 나타내는 address가 필요하다. 이를 위해 해당 사용자에게 지갑 기능을 담당하는 address와 해당 지갑을 안전하게 보호할 수 있는key를 제공한다. 사용자의 편의성을 위해 key 값을 사용자가 입력하는 단어들의 조합으로 구성하여 제공할 수 있도록 한다.

4.2.5. Searching



사용자가 구매하고 싶은 물건 혹은 검증하고 싶은 물건을 검색할 수 있는 기능이다. 사용자는 원하는 검색어를 입력함으로써 원하는 물건에 대한 리스트를 얻을 수 있다.

4.2.6. Selling Product

판매자가 되어 팔고 싶은 물건을 올릴 수 있는 기능이다. 판매하고자 하는 상품을 올릴 때, 판매자는 상품명, 카테고리, 가격을 입력하고 설명을 같이 기재한다. 이후 “상품 등록 하기” 버튼을 클릭하면 해당 상품은 블록체인 거래 시스템에 등록된다.

4.2.7. Buying Product


판매자가 올린 제품을 구매하는 기능이다. 구매하고자 하는 상품을 선택한 뒤, 수령인, 연락처, 배송지를 입력한다. 이후 블록체인 검증 거래 서비스를 이용하고 싶다면 해당 서비스에 대한 체크박스를 클릭한 뒤 검증 기간과 판매자에게 지급할 수수료를 입력한다. 이후 판매자가 요청을 수락하면 거래 검증이 시작된다. 이후 거래 검증이 문제 없이 종료되면 결제가 이루어진다.

4.2.8. Manage product

자신이 구매하거나 판매 또는 검증한 물건을 관리하는 기능이다. 이전에 판매, 구매 또는 검증을 했던 물품의 리스트가 나타나며 해당 물품을 클릭하면 물품에 대한 정보와 자세한 거래 정보가 기재된다.


4.2.9. Verifying Transaction

[< prev](#)



주문 검증




상품 상태	판매 중
상품 번호	3233535
등록 일시	2019-10-05



쿠쿠 밥솥

User description Here

25,000원 판매자 : 백산수



판매자	백산수
계좌	신한 110-223-2424242
전화 번호	010-0000-000

No.	내용	출처
1	더치트에 검색됨	
2		
3		

신고 하기

블록체인 위에 등록된 거래에 대해 검증하는 서비스이다. 해당 서비스는 판매자, 구매자가 이용하는 것이 아닌 제 3자가 참여하게 된다. 제 3자는 거래에 대한 정보, 즉 판매자가 올린 사진, 판매자의 계좌 번호, 전화 번호 등 다양한 정보를 통해 해당 판매자의 신변을 확보하게 된다. 이를 통해 제 3자는 판매자에 대한 타 플랫폼에서의 거래

내역과 사기 내역을 조회하고 해당 거래를 검증할 수 있다. 거래를 검증하는 과정에서 문제를 발견해내면 인센티브가 지급되며 해당 거래는 파기된다.

4.2.10. Wallet Management

The screenshot displays a user interface for wallet management. On the left, there's a section titled '나의 지갑 관리' (My Wallet Management) with a '충전' (Recharge) button and a bar chart showing '월별 지출 관리' (Monthly Expense Management). Below this is a table for '최근 변동 내역' (Recent Transaction History) with columns EID, DATE, Pname, value, and Balance. The table shows two transactions: one for '소공개' (Sogongae) and another for '프로젝트' (Project). To the right, there's a section for '가상화폐->현금 교환' (Cryptocurrency->Cash Exchange) with input fields for amount and exchange rate, and a '확인' (Confirm) button. A dropdown menu shows '출금 계좌를 골라주세요' (Please select a withdrawal account) with options for '우리 1002-xxx-xxxxxx' and '신한 110-xxx-xxxxxx'.

EID	DATE	Pname	value	Balance
es1231	19.10.01	소공개	-9@	50@
es0111	19.10.03	프로젝트	-10@	40@
.....	19.10.1

가상 화폐 거래를 위해 생성된 Address에 대한 잔고와 거래 내역을 보여주는 기능이다. 생성된 가상 화폐를 충전 및 관리할 수 있으며, 자신의 계좌로 환전이 가능하다. 또한 월별 지출과 최근 변동 내역에 대해 조회가 가능하다. 최근 변동 내역에는 거래 ID, 시간, 이름, 변동량, 잔고가 기재된다. 또한 자신의 은행 계좌를 이용해 가상화폐를 충전하는 기능과 가상화폐를 현금으로 환전하는 기능을 포함한다. 해당 기능을 통해 해당 서비스를 이용하기 위해 필요한 만큼의 가상 화폐를 충전하거나 인센티브로 받은 가상 화폐를 은행 계좌로 환전해 보낼 수 있다.

4.2 Non-functional Requirements

4.2.1 Product requirement

4.2.1.1. Security

해당 시스템은 사용자의 가상화폐를 관리하고 있으므로 특히 보안에 신경써야 한다. 가상화폐의 private key는 서버에 안전하게 저장되어야 하여야 한다. 또한 검증과정 이

후 해당 판매자에 대한 정보를 블록체인에 저장할 때에 정보가 유출되지 않도록 판매자의 계좌와 전화번호를 모두 Hash 값으로 저장한다.

4.2.1.2. Reliability

해당 시스템은 블록체인 위에서 작동하는 Smart Contract와 서버가 연동되는 시스템이기 때문에 두 시스템이 상호 작용함에 있어 안정성을 갖춰야 한다. 블록체인 위에서 작동하는 Smart Contract가 수수료 문제로 정지될 수 있기 때문에 해당 사항을 고려해 수수료를 지속적으로 측정해야한다.

4.2.1.3. Speed

블록체인을 이용하는 시스템이기 때문에 거래에 대한 Speed는 블록체인의 거래 속도와 관련이 크다. 때문에 블록체인 상에서 거래에 대한 수수료를 한도 내에서 최대한 높게 설정하여 거래가 빨리 이루어 질 수 있도록 해야한다.

또한 검증과정에 있어서의 Speed도 중요하다. 해당 과정이 길어지면 기존 안전거래 서비스가 가진 문제점을 해결할 수 없기 때문에 검증 과정 시간을 최대한 줄일 수 있는 검증 알고리즘을 사용해야 한다.

4.2.1.4. Usability

블록체인에 익숙하지 않은 사용자를 위해서 최대한 사용하기 쉽도록 만들어져야 한다. 거래 검증 과정이라든지, 가상 화폐 관리 방법 등 기존의 중고 시장 앱과는 많은 기능적 차이가 존재하기 때문에 해당 기능들에 대해 익숙하지 않은 사용자가 쉽게 사용할 수 있도록 해야한다.

4.2.2 Organization requirement

4.2.2.1. Delivery requirement

해당 시스템은 generic product 로 소비자에게 최대한 빨리 전달되어야 한다. Waterfall model 을 사용해 프로젝트를 설계하지만 Delivery 는 최대한 이른 시간 안에 진행되어야 시장에서 뒤처지지 않을 수 있다.

4.2.2.2. Implementation requirement

먼저 블록체인 상에서 동작하기 위해서는 이더리움과 연동되는 Solidity 를 사용해야한다. 해당 언어를 통해 Smart contract 를 만들고 smart contract 와 연동되는 Web3 를 지원하는 javascript 와 nodejs 를 사용해 웹과 서버를 구축해야 한다.

4.2.3 External requirements

4.2.3.1. Interoperability

해당 시스템은 블록체인 위에 저장된 정보를 사용하기 때문에 서버와의 상호 호환성이 매우 중요하다. 서버에서 사용하는 Oracle과 블록체인이 연동되어 정보를 주고 받고 웹페이지에 블록체인 위의 정보를 운용할 수 있어야 한다.

또한 화폐 간 상호 운용성도 중요하다. 해당 시스템의 가상화폐가 단순히 고립된 화폐가 아니라 비트코인, 이더리움, 리플 등 다양한 화폐와 교환될 수 있도록 해야한다.

4.2.3.2. Ethical requirement

해당 시스템을 사용함에 있어 사용자는 거래에 기록되는 개인정보를 유출해서는 안된다. 해당 정보는 개인정보보호법에 따라 보호되기 때문에 해당 정보를 유출하는 행위는 금지되어야 한다. 또한 사용자 간의 거래에 있어 악의적으로 잘못된 정보를 입력해서는 안된다. 해당 행위는 사기죄에 해당하며 사용자의 혼란을 막기 위해 금지되어야 한다.

4.2.3.3. Legislative requirement

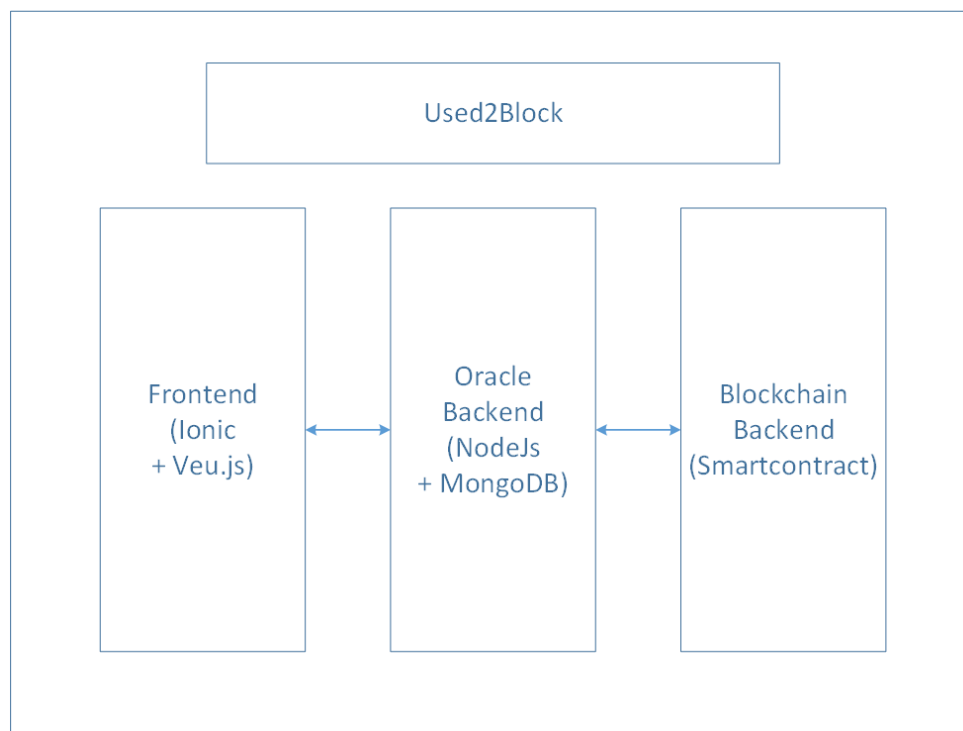
해당 시스템은 사용자가 거래에 입력하는 정보를 거래 검증인에게 공개한다. 이 과정에서 당사자의 동의가 없다면 제 3자에게 제공하는 것은 금지되기 때문에 일부 정보를 공개하기 이전에 사용자의 동의가 필수적이다. 이를 통해 개인정보의 유출을 방지하여 개인의 사생활을 보호해야한다.

해당 시스템은 가상화폐를 제작하고 유통하기 때문에 금융감독원의 허가가 필요하다. 해당 가상화폐는 ICO를 통해 모금을 진행하게 되는데 허가없는 기금 모금 사업은 법률 위반으로 법적인 처벌을 피할 수 없다. 때문에 가상화폐에 대한 금융감독원의 허가를 받아 ICO를 진행해야 한다.

5. System Architecture

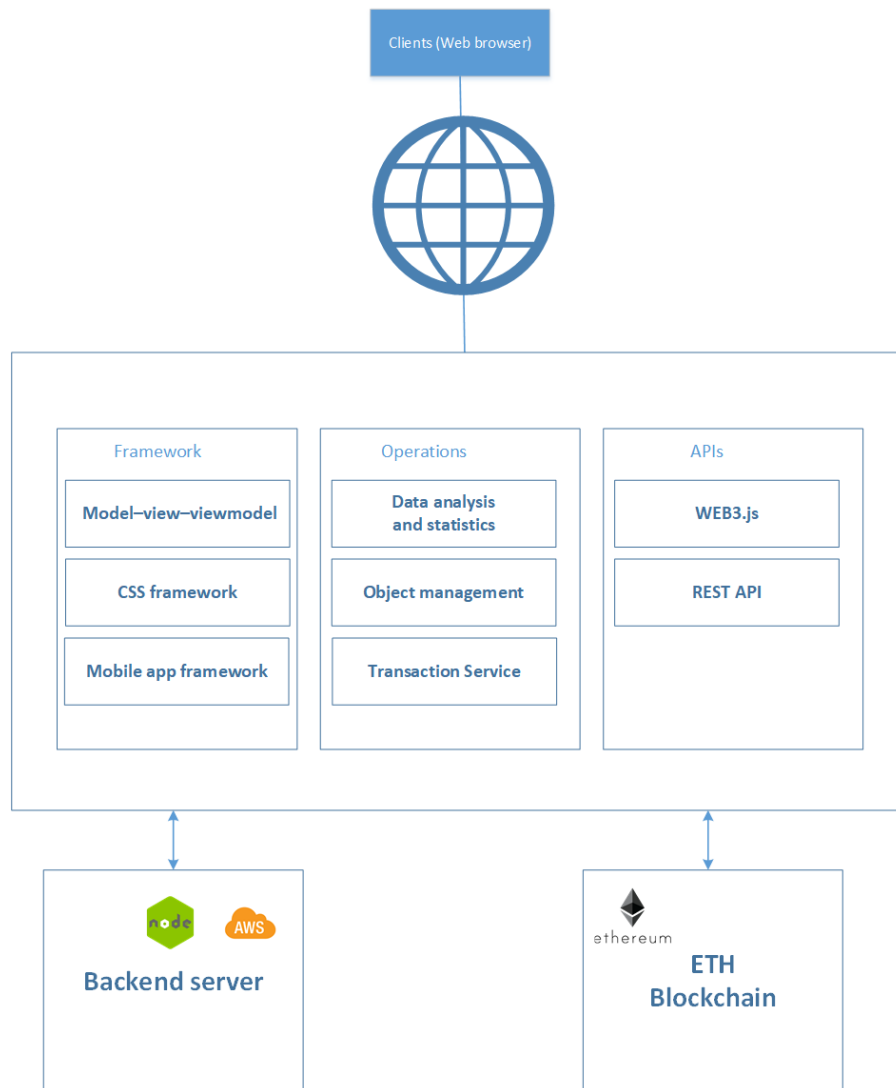
이 챕터에서는 시스템의 전체적인 구조를 기술한다. Requirement Engineering 과정에서 도출한 시스템의 전체적인 구조와 각 서브시스템의 구성, 서브시스템 간의 관계를 설명하며, 각 구조는 다이어그램을 첨부하여 이해를 돕는다.

5.1 Overall Architecture



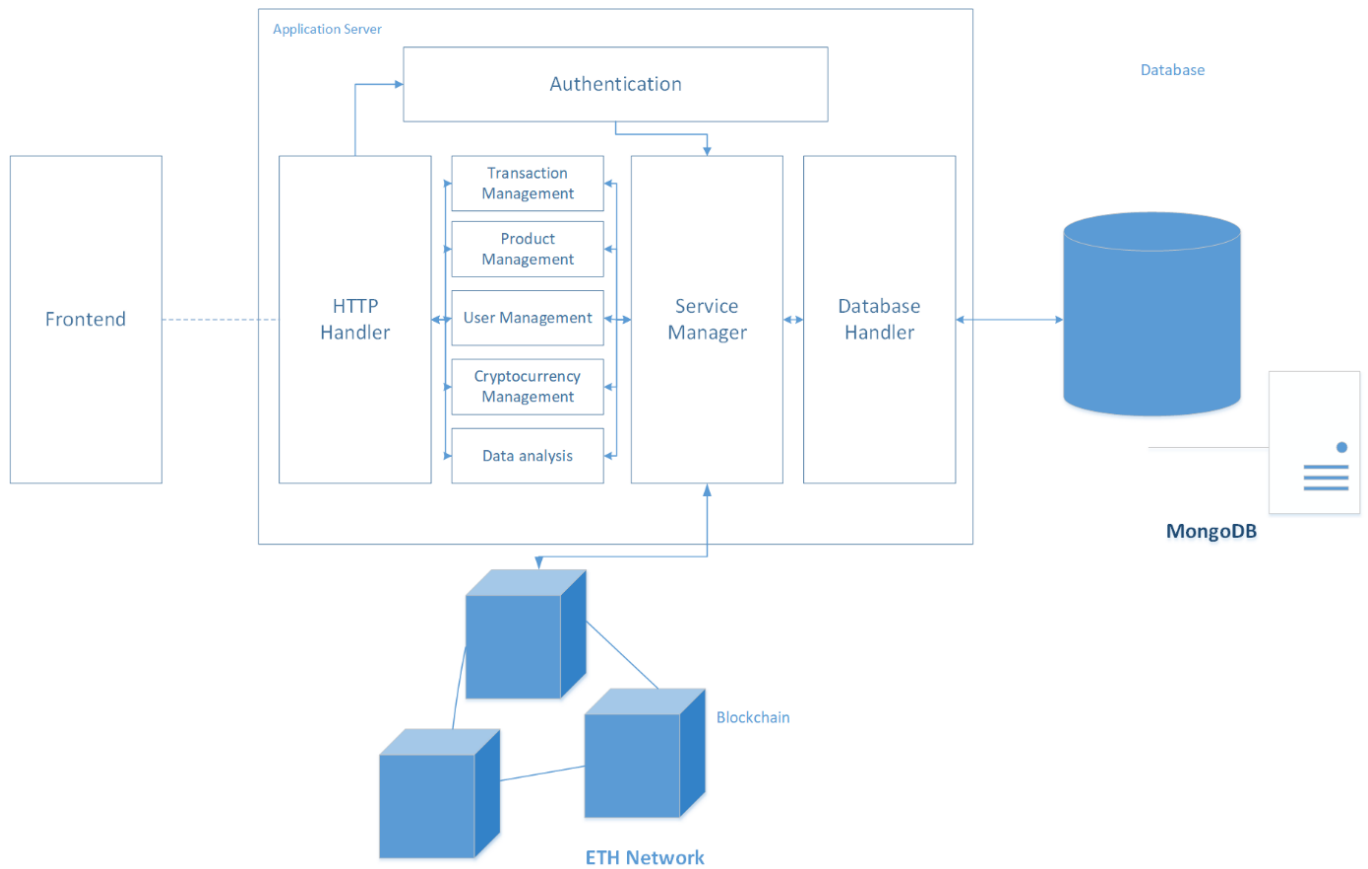
기본적으로 Used2Block 서비스는 크게 세가지 Component로 구성된다. User에게 서비스를 진행할 Frontend, Blockchain Backend의 보조 역할을 담당할 Oracle Backend, 그리고 모든 거래가 발생하는 Blockchain Backend이다.

5.2. Frontend Architecture



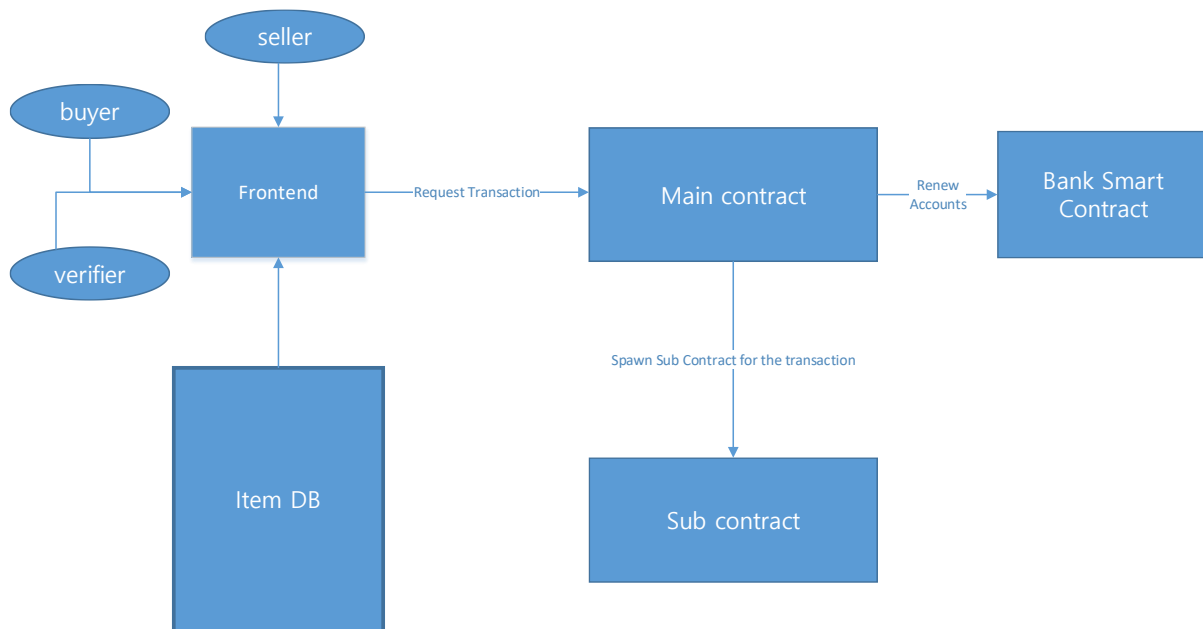
Frontend architecture는 사용자가 시스템과 Interaction하고 데이터를 요청하는 데 필요한 기능을 제공한다. Used2Block에서의 주된 operation은 두가지 종류의 서버와 Interaction하게 된다. 사용자, 상품 관리, 상품 거래라는 object management와 해당 유저의 거래 기록을 분석하는 Data analysis 부분은 Backend server와 Interaction하게 되고, Transaction service는 ETH blockchain과 Interaction할 수 있도록 설계되었다. 또한 API를 통해 각 서버로부터 얻은 정보는 Framework를 이용해 사용자에게 전달되도록 한다.

5.3. Backend Architecture



Backend의 구조는 위 다이어그램과 같이 구성되어 있다. Backend는 HTTP 요청을 받아 Handling 하는 기능을 담당하도록 설계되었다. 기본적으로 Backend는 ETH Network로부터 정보를 갖고 오거나 입력하는 역할을 담당하며, 부가적인 정보를 저장하기 위해 Database를 사용한다.

5.4. ETH blockchain system



블록체인 시스템은 기본적으로 Smart contract로 구성된다. Main Smart Contract는 구매자 혹은 판매자로부터 Transaction request를 받아 request에 대한 정보를 담은 Sub Smart Contract를 생성한다. 해당 Sub Smart Contract에서 Verifier가 Seller의 과거 이력을 확인하는 검증 작업이 일어난다. 검증 작업 이후 신뢰 거래가 이루어졌을 경우 Bank Smart Contract상의 구매자의 가상화폐가 판매자에게 전송된다. 모든 작업이 종료되면 Sub Smart Contract는 소멸한다.

5.5. Application System

5.4.1 Transaction Management

어플리케이션 시스템의 거래 관리는 블록체인 상에서 사용자가 이용했던 거래 내역 데이터를 가져오거나 거래를 진행하는 경우 블록체인 위에 기록하는 역할을 한다.

5.4.2 User Management

User management 는 데이터 베이스 상의 유저에 대한 정보를 관리하는 기능이다. 사용자가 Used2 Block 을 사용함에 있어 필요한 계정을 생성하거나 로그인을 시도하는 경우 데이터베이스로부터 정보를 write 하거나 read 한다. 또한 거래를 진행하면서 거래 상대들로부터 받은 평판 등을 데이터 베이스로부터 가져올 수도 있다.

5.4.3 Product Management

Product Management 는 판매자가 상품 판매를 원할 때 상품의 사진, 상품명, 카테고리, 희망 가격, 설명을 입력하였을 때 블록체인 위에 해당 상품을 올리거나, 이미 등록된 상품을 블록체인 시스템으로부터 가져오게 된다.

5.4.4 Cryptocurrency Management

Cryptocurrency Management 는 사용자가 가진 가상화폐를 관리하는 역할을 한다. 해당 사용자의 가상 화폐에 대한 정보는 블록체인으로부터 가져오며, 환전을 요청했을 경우 블록체인에 사용자의 가상 화폐에 대한 갱신을 요청한다.

6. System Requirements Definition

해당 챕터에서는 시스템이 핵심으로 제공하는 기능적 요구사항인 서비스와 부가적으로 충족시켜야 하는 비기능적 요구사항 두가지로 나누어 설명한다. 개발자를 대상으로 작성되는 부분인만큼 구체적인 기술과 구현에 관한 자연어, 시각 자료, 도표 등을 이용해 상세히 설명한다. 각 System Requirement들은 보다 상세한 내용 서술과 어떤 input을 받고 어떤 동작을 하며, 어떤 output을 산출하는지 등에 관해 기술된다. 또한 해당 요구사항의 조건과 제약을 함께 표현한다.

>>>>>>>>>?테이블 행 값들에 대한 설명

6.1. Functional Requirements

6.1.1. Sign up (register)

Name(이름)	Sign up
Description(설명)	사용자가 서비스를 이용하기 위해 서버에 회원으로 등록하는 기능이다. 이후 사용자는 고유한 식별자를 부여받아 서비스를 이용할 수 있다.
Inputs(입력)	이메일, 전화번호, 주소, 아이디, 비밀번호
Source of Input(근원지)	사용자(User)
Outputs(출력)	유저 계정(account)
Destination for Output(도착지)	Used2Block 데이터베이스
Action(행동, 처리)	주어진 입력 값을 통합해서 고유한 유저의 데이터를 데이터베이스에 저장한다.
Requirements(요구사항)	이메일과 전화번호는 정해진 형식에 맞춰서 입력되어야 한다. (ID@mail_domain), (+82-10-0000-0000) 비밀번호는 보안상 쉽게 노출되지

	않는 조합의 값이어야 한다. (영문, 숫자, 특수기호)
Pre-condition(전치조건)	먼저 입력된 정보와의 중복이 없어야 한다.
Post-condition(후치조건)	유저의 입력 값은 손실 없이 저장되어야 한다.

Table . Sign up table. (Table 숫자는 추합시 적용하겠습니다. 나머지 table들도 부탁드립니다!)

6.1.2. Login

Name(이름)	Login
Description(설명)	Sign up 과정을 거쳐 회원으로 가입된 사용자가 시스템에 인증 받는 절차이다. 인증 과정 이후 해당 사용자는 'Used2Block' 서비스를 이용할 수 있다.
Inputs(입력)	아이디, 비밀번호
Source of Input(근원지)	사용자(User)
Outputs(출력)	Used2Block 웹 페이지 (메인)
Destination for Output(도착지)	User Terminal (웹 브라우저)
Action(행동, 처리)	데이터베이스 내의 데이터와 입력 값을 비교한 뒤, 인증과정을 수행하여 해당 사용자를 식별한다.
Requirements(요구사항)	경우에 따라 추가 인증기능이 필요할 수 있다.
Pre-condition(전치조건)	입력된 사용자의 데이터가 기존의 데이터베이스에 존재해야 한다.
Post-condition(후치조건)	인증이후 Logout 기능의 수행 전 까지 서비스는 제공된다.

6.1.3. Logout

Name(이름)	Logout
Description(설명)	시스템에 인증을 받고 서비스를 이용하던 사용자가 사용을 모두 마친 후 안전하게 'Used2Block' 서비스를 종료하는 행위를 의미한다. 이후 계정은 다음의 Login 기능의 동작까지 안전하게 보호된다.
Inputs(입력)	Logout button의 signal
Source of Input(근원지)	사용자(User)
Outputs(출력)	Logout message
Destination for Output(도착지)	User Terminal (웹 브라우저)
Action(행동, 처리)	서비스 종료 명령을 받은 즉시 인증된 사용자의 인증을 종료하고 기존의 비 인증 상태로 복귀한다.
Requirements(요구사항)	
Pre-condition(전치조건)	
Post-condition(후치조건)	이후 재 인증과정 전까지 해당 사용자 개인의 어떠한 서비스도 수행되지 않는다.

6.1.4. User's profile Management

Name(이름)	User profile
Description(설명)	사용자 자신의 프로필 정보를 확인하고 수정할 수 있는 기능을 제공한다. 해당 페이지에서는 현재 가상 화폐의 잔고, 거래 내역, 개인 정보가 포함된다.
Inputs(입력)	서비스 요청,
Source of Input(근원지)	사용자, Used2Block 데이터베이스
Outputs(출력)	유저 정보, 가상 화폐 정보, 거래 내역,
Destination for Output(도착지)	Used2Block 웹 페이지
Action(행동, 처리)	서비스 요청을 받아 인증 받은 해

	당 유저의 정보(output)를 데이터 베이스로부터 받아와 제공한다.
Requirements(요구사항)	정보요구는 인증을 받은 상태여야 하며, 정보의 제공은 즉시 이루어 져야 한다.
Pre-condition(전치조건)	가입하고 인증 받은 사용자의 상태여야 한다. 사용자의 정보가 데이터베이스에 손실 없이 저장되어 있어야 한다.
Post-condition(후치조건)	변경사항이 있을 시 모두 즉시 반영한다.

6.1.5. Creating Wallet

Name(이름)	Creating Wallet
Description(설명)	가상 화폐는 소유권을 나타내는 address가 필요하다. 이를 위해 해당 사용자에게 지갑 기능을 담당 하는 address와 해당 지갑을 안전하게 보호할 수 있는key를 제공해야 한다. 여기서 key 값은 사용자가 입력하는 단어들의 조합으로 구성하여 제공하며 address는 식별가능한 조합의 일련번호로 시스템이 제공한다.
Inputs(입력)	Sign up 신호, Key 입력,
Source of Input(근원지)	사용자(User), Used2Block 데이터 베이스
Outputs(출력)	완료문구, Address, key value
Destination for Output(도착지)	User Terminal, Used2Block 데이터 베이스
Action(행동, 처리)	Sign up과 동시에, 식별가능한 Address를 제공하고, key 값을 추가로 입력 받는 프로세스를 통해서 해당 사용자의 wallet을 만든다.

Requirements(요구사항)	Address 값은 unique해야한다.
Pre-condition(전치조건)	Sign up과정에서 오류가 없어야 한다.
Post-condition(후치조건)	Address와 Key는 함께 유저 데이터와 함께 저장되고 관리되어야 한다.

6.1.6. Searching

Name(이름)	Searching
Description(설명)	사용자가 구매하고 싶은 물건 혹은 검증하고 싶은 물건을 검색할 수 있는 기능이다. 사용자는 원하는 검색어를 입력함으로써 원하는 물건에 대한 리스트를 얻을 수 있다.
Inputs(입력)	검색하고 싶은 값
Source of Input(근원지)	사용자(User)
Outputs(출력)	검색된 품목들의 List, message.
Destination for Output(도착지)	User Terminal (웹 브라우저, Used2Block page)
Action(행동, 처리)	사용자가 찾기를 원하는 값을 입력 받아 데이터베이스 상에서 저장된 품목의 정보와 비교한다. 일치하는 항목들을 유저에게 다시 출력한다. 일치하는 모든 품목은 일치하는 여부와 등록 순서에 따라서 정렬되어 출력한다. 만일 일치하는 목록이 없을 시, '목록이 없음' 또한 출력한다.
Requirements(요구사항)	쿼리의 처리는 SQL언어로 작동한다.
Pre-condition(전치조건)	
Post-condition(후치조건)	

6.1.7. Selling Product

Name(이름)	Selling Product (상품 등록, 판매요청)
Description(설명)	시스템 상에서 유저가 팔고 싶은 물건을 올릴 수 있는 기능이다. 물건은 블록체인 거래 시스템에 등록되어 다음 작업을 위해 대기한다.
Inputs(입력)	상품명, 카테고리, 가격, 설명, 사진. '등록하기 버튼'의 신호
Source of Input(근원지)	사용자(User - 판매자)
Outputs(출력)	등록된 상품 정보, 상품 데이터
Destination for Output(도착지)	User Terminal, Used2Block 데이터 베이스
Action(행동, 처리)	입력된 데이터를 안전하게 저장하고, 저장된 결과를 Interface에 맞게 출력한다. 저장된 데이터는 즉시 검색에 적용되고, 노출되며, 등록된 페이지는 등록자에게도 노출되어 검증 과정을 거친다.
Requirements(요구사항)	상품의 등록자가 명시된 최소한의 정보들은 모두 입력하게 제약하고, 추가로 정보를 입력하는 것 또한 수용한다.
Pre-condition(전치조건)	
Post-condition(후치조건)	해당상품이 중복되어 등록되지는 않았는지 점검해야 한다.

6.1.8. Buying Product

Name(이름)	Buying Product (구매 주문)
Description(설명)	판매자가 올린 제품을 구매하는 기능이다.
Inputs(입력)	상품, 수령인, 연락처, 배송지,
Source of Input(근원지)	사용자(User - 구매자)

Outputs(출력)	구매 확정 페이지, 거래내역
Destination for Output(도착지)	User Terminal, Used2Block 데이터 베이스
Action(행동, 처리)	구매하고자 하는 상품과 구매자의 배송 정보를 입력하고 나면 구매 상품의 거래를 확정 짓는다.
Requirements(요구사항)	
Pre-condition(전치조건)	
Post-condition(후치조건)	

6.1.9. Validation

Name(이름)	Buying Product (구매 주문) with Validation
Description(설명)	상품을 구매할 때, 블록체인 검증 서비스를 추가로 선택하는 경우에 제공되는 서비스다. 보통의 거래와 달리, 구매자가 동의하고, 판매자에게 지급할 수수료를 입력한 후, 판매자가 요청을 수락해야 한다. 그 후 거래 검증이 문제없이 종료 되고 나서 결제가 이루어진다.
Inputs(입력)	검증 서비스 체크박스 시그널, 수수료, 요청 수락,
Source of Input(근원지)	사용자(User – 구매자, 판매자)
Outputs(출력)	거래 검증 페이지
Destination for Output(도착지)	User Terminal, Used2Block 데이터 베이스
Action(행동, 처리)	검증서비스 요청과 데이터를 받고, 판매자의 동의를 얻은 후 검증 대기 상태로 해당 거래를 이관시킨다.
Requirements(요구사항)	
Pre-condition(전치조건)	검증 서비스 이외의 정보 모두 이미 확인되고 성립된 상태이다.

Post-condition(후치조건)	Verifying Transaction의 기능으로 전달한다.
----------------------	-----------------------------------

6.1.10. Manage product

Name(이름)	Manage Product
Description(설명)	사용자와 관계된 상품들을 관리하는 기능이다. 이전의 판매, 구매, 검증 기록이 제공된다.
Inputs(입력)	Manage page request
Source of Input(근원지)	사용자(User), Used2Block 데이터베이스
Outputs(출력)	Product history_list
Destination for Output(도착지)	User Terminal
Action(행동, 처리)	이용자와 관계된 상품들을 모두 저장된 데이터베이스로부터 검색해서 불러온다.
Requirements(요구사항)	SQL쿼리를 통한 검색의 경우 결과의 검색이 느리지 않도록, 유저에게 interactive하도록 한다.
Pre-condition(전치조건)	유저와 관련된 상품들에 관한 기록이 데이터베이스에 저장되어 있어야 한다.
Post-condition(후치조건)	해당 상품들에 대한 추가 요청이 있을 경우 Product Page로 연결되어야 한다.

6.1.11. Product Page

Name(이름)	Product Page
Description(설명)	상품의 정보를 제공하는 페이지이다. 판매자가 올린 상품이 하나의 개체로서 저장되고 관리된다. 이 개별 product의 페이지들은, 유저가 구매 또는 검증을 위한 검색을 할 시에 접근된다.

Inputs(입력)	Product page request
Source of Input(근원지)	사용자(User)
Outputs(출력)	Product Information
Destination for Output(도착지)	User Terminal
Action(행동, 처리)	이용자가 요청한 상품의 정보를 저장된 데이터베이스로부터 검색 해서 불러온다.
Requirements(요구사항)	
Pre-condition(전치조건)	유저와 관련된 상품들에 관한 기 록이 데이터베이스에 저장되어 있 어야 한다.
Post-condition(후치조건)	

6.1.12. Verifying Transaction

>>>>>>>>>? 블록체인을 어떻게 불러오고 처리하는지.

>>>>>>>>>? 타플랫폼 검색에 대한 처리는

Name(이름)	Verifying Transaction
Description(설명)	블록체인 검증 거래 서비스를 요 청한 경우에 제3자가 참여하여 거 래를 검증한다. 제3자는 거래에 대 한 정보 중 판매자가 등록한 사진, 계좌번호, 전화번호 등을 이용하여 해당 판매자의 거래내역과 사기 내역을 조회하고 거래를 검증한다. 타 플랫폼에서의 기록 또는 블록 체인에서의 거래내용을 통해서 찾 아내면 인센티브가 지급되고 거래 는 안전하게 파기된다.
Inputs(입력)	판매자 사기 정보.
Source of Input(근원지)	사용자(User), 블록체인,
Outputs(출력)	거래 파기 페이지.
Destination for Output(도착지)	User
Action(행동, 처리)	검증자가 판매자의 사기 내역 정

	<p>보를 입력하면 확인을 통해서 판매자와 구매자 사이의 거래를 즉시 파기한다. 검증은 블록체인에 기록된 거래 내역과 웹 페이지와 연결되어 있는 기존의 다른 서비스에서 검증된 결과를 통해서 이루어진다. 제3자는 이를 통해서 인센티브를 지급받을 수 있어야 한다.</p>
Requirements(요구사항)	<p>사기 내역 정보는 그 근거가 충분해야 한다. 타 사이트(ex: 더 치트, 경찰청데이터베이스 등) 또는 블록체인에서 찾아낸 사기내역을 의미한다.</p>
Pre-condition(전치조건)	<p>블록체인 검증 거래 서비스를 요청해야 한다.</p>
Post-condition(후치조건)	<p>이후 검증에 이용된 판매자의 개인 데이터는 더 이상 노출되지 않는다.</p>

6.1.13. Wallet Management

Name(이름)	Wallet Management
Description(설명)	<p>가상 화폐 거래를 위해 생성된 Address에 대한 잔고와 거래 내역을 보여주는 기능이다. 생성된 가상 화폐를 충전 및 관리할 수 있으며, 자신의 계좌로 환전이 가능하다. 또한 월별 지출과 최근 변동 내역에 대해 조회가 가능하다. 최근 변동 내역에는 거래 ID, 시간, 이름, 변동량, 잔고가 기재된다.</p>
Inputs(입력)	Wallet Management Request
Source of Input(근원지)	사용자(User)
Outputs(출력)	Wallet Management Page (잔고, 거래내역, 지출-변동내역-거래ID,

	시간, 변동량)
Destination for Output(도착지)	User Terminal
Action(행동, 처리)	유저의 '가상 지갑'관리 요청을 받아서 데이터베이스와 블록체인으로 부터 저장된 유저의 가상화폐 거래 내역과 잔고를 보여준다.
Requirements(요구사항)	유저의 인증 과정이 필요하다. Key 값을 통한 user authentication을 거쳐야만 열람 및 변경이 가능하다.
Pre-condition(전치조건)	
Post-condition(후치조건)	

6.1.14. Crypto-Currency Exchange

Name(이름)	Exchange
Description(설명)	연동된 은행 계좌를 이용해서 가상화폐를 충전하는 기능과 가상화폐를 현금으로 환전하는 기능을 제공한다. 이를 통해서 서비스 이용을 위한 가상 화폐 충전 또는 은행 계좌로의 환전이 가능하다.
Inputs(입력)	Exchange Request, Direction, Amount
Source of Input(근원지)	사용자(User)
Outputs(출력)	변동내역, 거래량, 잔고
Destination for Output(도착지)	User Terminal
Action(행동, 처리)	유저의 가상화폐-계좌잔액 간의 환전 요청을 받아서 그 양과, 방향을 파악하고 원하는 기능을 수행한다. 그 이후 변경된 내용을 이용자에게 출력한다.
Requirements(요구사항)	거래의 최종의 확인을 요청해야 한다. 해당 계좌와의 거래 서비스가 연동되어 있어야 한다.

Pre-condition(전치조건)	Wallet management 기능에서 환전 기능을 요청한다.
Post-condition(후치조건)	최종적으로 수정된 사항은 다시 데이터베이스와 블록체인에 저장되어야 한다.

6.2 Non-functional Requirements

6.2.1. Product requirement

6.2.1.1 Security

유저 요구사항에 언급했던 것처럼, 가상화폐를 관리하고 있으므로 특히 보안에 신경 써야 한다. 가상화폐의 private key 는 서버에 안전하게 저장되어야 한다. 또한 검증과정 이후 해당 판매자에 대한 정보를 블록체인에 저장할 때에 정보가 유출되지 않도록 판매자의 계좌와 전화번호를 역시 Hash 값으로 저장한다.

여기서 암호 해시는 문서를 요약, 고유 값을 자동으로 생성하는 기술이다. 단 이때 요약은 내용 요약이 아니라 해당 개체에 대한 '식별 정보'로 요약하는 것이다. 총 256 바이트가량의 고유 값이 만들어진다. 한글로 치면 128 자 정도의 문자열(SHA-256 기준) 정도 크기이다. 이런 해시 알고리즘을 통해서 정보 유출을 막을 수 있다.

6.2.1.2. Reliability

해당 시스템은 블록체인 위에서 작동하는 Smart Contract 와 서버가 연동되는 시스템이기 때문에 두 시스템이 상호 작용함에 있어 안정성을 갖춰야 한다.

Used2Block 플랫폼 정보를 저장하고 있는 메인 데이터베이스는 특히 Validation 과정에서, Product 의 정보를 즉각적으로 Block Chain 검증 과정에 제공해 주어야 하고, Smart Contract 결과는 검증과 동시에 거래내역 등의 정보를 서버에 제공하고 다시 기록해서 실시간으로 동기화할 수 있어야 한다.

블록체인 위에서 작동하는 Smart Contract 가 거래를 진행하는 데 있어 부족한 수수료 문제로 Operation 이 정지될 수 있기 때문에 해당 사항을 고려해 블록체인 상 Transaction 에대한 수수료를 지속적으로 측정해야 한다.

6.2.1.3. Speed

여기서의 Speed 는 시스템 Performance 를 의미하는 것은 아니다. 이는 시스템의 활발한 사용을 측정하기 위해 쓰이는 척도이며, 블록체인 거래 속도와 관련이 크다. 때문에 블록체인 상에서 거래에 대한 수수료를 최대한 높게 설정하여 거래가 빨리 이루어 질 수 있도록 해야 한다. 블록체인 검증 거래를 통해서 판매자가 검증을 기다리면서 얻을 이익(수수료)가 상품의 가치에 따라 적절한 가격이어야 하며, 동시에 구매자가 요청함에 있어서 부담되지 않는 수준이어야 한다.

종합적으로 시장 전체의 활성화를 위해서 측정할 수수료의 비율은 전체 시장의 유동성, 가상화폐 가치, 거래되는 상품의 가격에 따라 탄력적으로 책정되어야 한다. 해당 수수료는 약 5 천원 내외의 가치를 지니도록 유지한다.

또한 검증과정에 있어서의 Speed 도 중요하다. 해당 과정이 길어지면 기존 안전거래 서비스가 가진 '늘어진 거래 상황'과 같은 문제를 해결할 수 없기 때문에, 검증 과정 시간을 최대한 줄일 수 있어야 한다. 따라서 검증자가 얻을 수 있는 보상에 있어서도 그 동기를 충분히 유인할 만큼 책정되어야 빠른 검증이 이루어질 것이다. 검증 과정에 있어 사용자의 반응 속도를 고려해 거래 당 1-2 시간 내외로 threshold 를 설정한다.

6.2.1.4. Usability

블록체인에 익숙하지 않은 사용자를 위해서 최대한 사용하기 쉽도록 만들어져야 한다. 블록체인 원리에 대한 사용자가 알아야 할 만큼의 정보가 Tutorial 과 같은 방식으로 제공되어야 한다. 또한 복잡한 작동 원리보다 서비스 이용에 필요한 거래 검증 과정, 가상 화폐 관리 방법과 같은 기존의 중고 시장 앱과는 다른 기능을 교육하고 익숙하게 만드는 데에 투자를 해야 한다.

시스템 구현에 있어서, 복잡한 원리 보다 각 Seller, Buyer, Validator 역할에서 어떤 인터페이스를 어떻게 이용할지에 대한 개별적인 정보가 전달되어야 한다. 앞서 언급한 System Functionality 에 관한 작동법을 첫 로그인 이후부터 제공하며, 사용자 동의로 '그만 볼래요'와 같은 체크박스를 동의할 때까지 인터페이스를 교육해서, 불편함을 감소시켜야 한다.

6.2.2. Organization requirement

6.2.2.1. Delivery requirement

해당 시스템은 generic product로서 소비자에게 최대한 빨리 전달되어야 한다. 플랫폼 서비스인 만큼 최대한 빨리 서비스를 시작해서 더 많은 고객들을 수용해야 하는 필요가 있다. 기존의 서비스 제품들과 경쟁하기 위해서 Waterfall model을 사용해 꼼꼼하게 검증하고 설계하지만, Delivery는 최대한 이른 시간 안에 진행되어야 시장에서 뒤처지지 않을 수 있다.

구체적인 발매 시간은 Working System을 만든 후 Alpha, Beta 그리고 Release Test를 마치고 거의 바로 출시될 수 있게 해야 한다. 또한 플랫폼 서비스의 초반 사용자 유치를 위해서 지속적인 홍보와 설명, 그리고 가상화폐 리워드와 같은 초기 서비스 참여의 유인이 필요하다.

6.2.2.2. Implementation requirement

먼저 블록체인 상에서 동작하기 위해서는 이더리움 네트워크와 연동되는 Solidity를 사용해야 한다. 해당 언어를 통해 Smart contract를 만들고 smart contract와 연동되는 Web3를 지원하는 javascript와 nodejs를 사용해 웹과 서버를 구축해야 한다. 내부 데이터베이스의 검색과 관리를 위해서는 SQL을 사용한다.

프론트엔드 웹 UX/UI 개발을 위해서 React, Vue.js, ionic 등의 개발 툴을 이용한다. 백엔드의 데이터베이스 관리를 위해서는 MongoDB를 사용하고 블록체인 ETH-net은 Remix를 이용해서 구현-관리한다.

6.2.3. External requirements

6.2.3.1. Interoperability

해당 시스템은 블록체인 위에 저장된 정보를 사용하기 때문에 서버와의 상호 호환성이 매우 중요하다. 서버에서 사용하는 Oracle과 블록체인이 연동되어 정보를 주고받고 웹페이지에 블록체인 위의 정보를 운용할 수 있어야 한다. Reliability를 확보하기 위한 노력과 연결되는 요구사항이다.

또한 화폐 간 상호 운용성도 중요하다. 해당 시스템의 가상화폐가 단순히 고립된 화폐가 아니라 비트코인, 이더리움, 리플 등 다양한 화폐와 교환될 수 있도록 해야 한다. 해당 비율을 현재 가치를 비교하여 산정될 예정이다.

6.2.3.2. Ethical requirement

해당 시스템을 사용함에 있어 사용자는 거래에 기록되는 개인정보를 유출해서는 안된다. 해당 정보는 개인정보보호법에 따라 보호되기 때문에 해당 정보를 유출하는 행위는 금지되어야 한다. 또한 사용자 간의 거래에 있어 악의적으로 잘못된 정보를 입력해서는 안된다. 해당 행위는 사기죄에 해당하며 사용자의 혼란을 막기 위해 금지되어야 한다.

구체적인 처벌에 대한 방침은 tit-for-tat 원칙을 선택한다. 선량한 사용자와는 지속적인 유대관계를 유지하며, 수수료와 같은 유인들로 서로의 관계를 견고히 한다. 하지만 사용자의 고의적인 서비스 오용, 개인정보 유출 등의 범죄가 발견되면 해당 개인정보의 계정을 영구 정지시키고 형사처벌과 관련한 수사에 협조한다.

6.2.3.3. Legislative requirement

해당 시스템은 사용자가 거래에 입력하는 정보를 거래 검증인에게 공개한다. 이 과정에서 당사자의 동의가 없다면 제 3 자에게 제공하는 것은 금지되기 때문에 일부 정보를 공개하기 이전에 사용자의 동의가 필수적이다. 개인정보를 공개하는 동의와 불법적인 유출을 막겠다는 동의 내역서가 필요하다.

해당 시스템은 가상 화폐를 제작하고 유통하기 때문에 금융감독원의 허가가 필요하다. 해당 가상화폐는 ICO 를 통해 모금을 진행하게 되는데 허가 없는 기금 모금 사업은 법률 위반으로 법적인 처벌을 피할 수 없다. 때문에 가상화폐에 대한 금융감독원의 허가를 받아 ICO 를 진행해야 한다.

6.3 System Scenario

6.3.1. 서비스 가입/접속/접속_종료 시나리오

6.3.1.1. 서비스 가입

6.3.1.1.1 Initial Assumption

사용자가 가입한 계정이 없거나 혹은 새로운 계정으로 가입하려 한다. 아이디, 전화번호의 조합은 기존의 데이터 베이스에 없다.

6.3.1.1.2 Normal flow of events

사용자는 원하는 아이디, 비밀번호, 전화번호, 계좌번호, 주소, 이메일 등의 '시스템 기능 요구사항 6.1.a'에서 정의된 입력 값을 넣는다. (추후 수정) 웹에서는 데이터베이스로 해당 값들을 조직하여 저장하고 관리한다. 가입시 동시에 가상화폐 관리를 위한 Address 를 생성하고 그 고유 비밀번호 또한 입력 받는다.

6.3.1.1.3. What can go wrong

서비스 가입 시 생성한 정보를 사용자가 분실할 수 있다. 낮은 확률로 데이터베이스에 잘 못 저장될 수 있다.

6.3.1.1.4. System state on completion

이용자는 이후 해당 아이디와 비밀번호를 통해서 서비스 사용의 식별, 인증을 받을 수 있다.

6.3.1.2. 로그인

6.3.1.2.1. Initial Assumptio

사용자가 먼저 만든 계정이 있다.

6.3.1.2.2. Normal flow of events

사용자는 자신의 정보를 입력하고 로그인 버튼을 클릭한다. 데이터베이스에 있는 일치하는 정보가 있는 것을 확인하고, 사용자는 <Used 2 Block>에 접속하여 사용할 수 있게 된다.

6.3.1.2.3. What can go wrong

사용자가 데이터베이스에 존재하지 않는 정보를 입력하는 경우에는, 올바른 ID와 패스워드라는 메시지를 보여주도록 한다.

서버가 정상적으로 작동하지 않는다. 연결이 끊겨 있거나 데이터 베이스에 정보가 누락되어 있다. 이미 다른 User Terminal에서 인증 받은 상태로 남아있다.

6.3.1.2.4. System state on completion

사용자가 서비스에 접속하여서 Used2Block 서비스를 이용한다.

6.3.1.3. 로그아웃

6.3.1.3.1. Initial Assumption

사용자는 인증된 사용자의 계정으로 Used2Block 서비스를 이용하고 있었다.

6.3.1.3.2. Normal flow of events

모든 서비스를 마친 뒤, 사용자는 서비스 접속 종료를 요청한다. 요청된 입력을 통해서 서버는 사용자 계정 인증을 만료하고, 해당 계정에 대한 사용자의 접근 권한을 중단한다. 이용자는 다시 메인 페이지 혹은 로그인 페이지로 이동한다.

6.3.1.3.3. What can go wrong

정상적인 로그아웃이 일어나지 않을 경우에 계속해서 해당 User Terminal 에 인증된 상태로 유지되어 보안을 위협받는다.

6.3.1.3.4. System state on completion

다음 인증 시까지 해당 계정은 안전하게 보호된다.

6.3.2 가상 Wallet 관리 시나리오

6.3.2.1. Wallet 관리

6.3.2.1.1. Initial Assumption

회원가입 시 생성된 가상화폐 관리용 Address 와 유저만이 알고 있는 key 값이 존재한다.

6.3.2.1.2. Normal flow of events

Wallet 페이지 열람 요청을 사용자가 요구한다. 요구된 요청을 시스템은 처리한다; 해당 사용자의 거래내역, 잔고, 잔고변동내역 등의 시스템 요구사항에서 명시된 정보들을 페이지에 출력한다. 이용자는 원하는 정보를 얻고 페이지를 떠나거나 다른 작업을 수행한다.

6.3.2.1.3. What can go wrong

사용자가 key 값을 분실하여 접근할 수 없다.

거래내역 정보를 블록체인 또는 데이터베이스로부터 읽어올 수 없다.

6.3.2.1.4. System state on completion

페이지 종료 시점까지 Wallet 페이지를 통해서 사용자는 개인의 잔액, 거래내역, 잔고 변동내역 등을 확인할 수 있다.

6.3.2.2. Crypto-Currency Exchange

6.3.2.2.1. Initial Assumption

현재 사용자는 인증 받은 Wallet Management 상태에 있다.

6.3.2.2.2. Normal flow of events

사용자가 금액, 환전 방향을 정해서 환전 거래를 요청한다.

시스템은 거래내용 확인을 요청하고 사용자의 확인 끝에 해당 환전 거래를 수행한다. 변경된 내역은 즉각 반영된다.

6.3.2.2.3. What can go wrong

재차 확인 했음에도 불구하고 유저가 잘못된 거래를 스스로 할 수 있다.

시스템상의 오류로 인하여 데이터 베이스와 블록체인에 거래 내역이 일관되게 반영, 기록되지 않는다.

6.3.2.2.4. System state on completion

사용자가 원하는 환전이 끝나고 Wallet management 페이지로 돌아가서 거래 최종 결과를 출력한다.

6.3.3 거래 시나리오

6.3.3.1. 판매자의 상품 등록

6.3.3.1.1. Initial Assumption

등록하고자 하는 물건이 중복되어 등록되지 않는다. 따라서 판매자는 등록 전에 확인이 필요하다.

6.3.3.1.2. Normal flow of events

상품명, 카테고리, 가격, 설명, 사진 등 시스템 요구사항에서 명시했던 입력 값들을 판매자는 입력한다.

입력된 값들을 이용해서 새로운 판매 상품이 등록되고 이는 개별적인 Product Page 로 관리된다. 데이터 베이스에 저장된 상품 정보는 다른 구매자, 판매자, 검증자 통칭해서 유저에게 검색되고 열람될 수 있다.

6.3.3.1.3. What can go wrong

상품정보가 올바르지 않을 수 있다.

중복된 상품이 등록되어 시스템 전체의 공간을 불필요하게 차지할 수 있다.

상품 등록에 제한이 없지만 바람직하지 않은(법률적, 윤리_보편적 관점에서 어긋나는) 거래 상품이 등록될 수 있다.

6.3.3.1.4. System state on completion

완성된 상품 페이지는 접근이 가능하며, 검색을 통해서도 정보 접근이 가능하다.

판매자는 다시 유저 페이지, 또는 새로운 상품 페이지로 연결된다.

6.3.3.2. 구매자의 검색 및 구매주문

6.3.3.2.1. Initial Assumption

구매자가 원하는 물건이 있고, 판매자는 팔고 싶은 동일한 물건을 등록했다.

6.3.3.2.2. Normal flow of events

구매자는 사고자 하는 물건을 Used2Block 데이터 베이스에서 검색한다.

검색을 통해 얻어진 상품 중 원하는 상품을 골라서 Product Page 를 열람, 상품 정보를 획득한다.

원하는 상품임을 확인한 구매자는 구매주문을 넣는다. 이 때, 구매자의 선택과 판매자의 동의에 따라 거래가 블록체인-검증거래 또는 일반 거래로 이루어질 지 선택된다. 블록체인-검증거래의 경우 별도의 검증 과정을 거친다. (이는 다음 시나리오 부분에서 서술된다)

6.3.3.2.3. What can go wrong

판매자가 판매를 원하지 않아서 거래가 성사되지 않는다. 또는 다른 요인으로 인해서 판매자가 판매 거래를 확인, 수락하지 않는다.

허위매물이 발생한다. 이를 검증과정 없이 놓칠 수 있다.

6.3.3.2.4. System state on completion

블록체인_검증과정으로 이관되거나 간편 거래가 성립되어 구매자와 판매자 모두 참여한 거래가 시작된다.

6.3.3.3. 블록체인 거래 검증과정

6.3.3.3.1. Initial Assumption

Buyer 와 Seller 가 합의하에 거래가 진행되었다. 해당 거래에 대한 검증 기간, 판매자가 올린 사진, 판매자의 전화번호, 계좌 등이 기재된다.

6.3.3.3.2. Normal

구매자와 판매자의 거래 시작 그리고 검증 요청에 따라 다시 상품은 검증을 위한 대기 상태에 놓이며 검색될 수 있다. 3rd Party, 즉 거래 검증인들은 해당 거래에 기재된 판매자에 대한 정보를 통해 사기 기록을 검색을 진행한다. 사기기록은 타 서비스 플랫폼의 정보 혹은 해당 블록체인에 기록된 거래내역을 통해서 이루어진다.

검증 기간이 종료될 때까지 해당 판매자에 대한 사기 관련 기록이 없어 report 가 발생하지 않으면 해당 거래는 정상적으로 진행된다.

또는 검색을 통해 해당 판매자에 대한 사기 기록이 발견되면 해당 거래를 파기한다.

검증에 소요되는 수수료를 구매자가 일부 지불하고, 판매자와 검증자는 시스템으로부터 수수료를 가상화폐로 받는다.

6.3.3.3.3. What can go wrong

3rd party 가 거래를 검증하는 도중, Buyer 또는 Seller 가 해당 거래를 취소할 수 있다. 이럴 경우를 대비해 거래 검증 도중에는 취소가 불가능하게 한다.

3rd party 가 잘못된 정보를 Report 할 수 있다. 해당 내용에 대한 근거를 기록하도록 해 유저들이 해당 report 를 한번 더 판단할 수 있도록 한다.

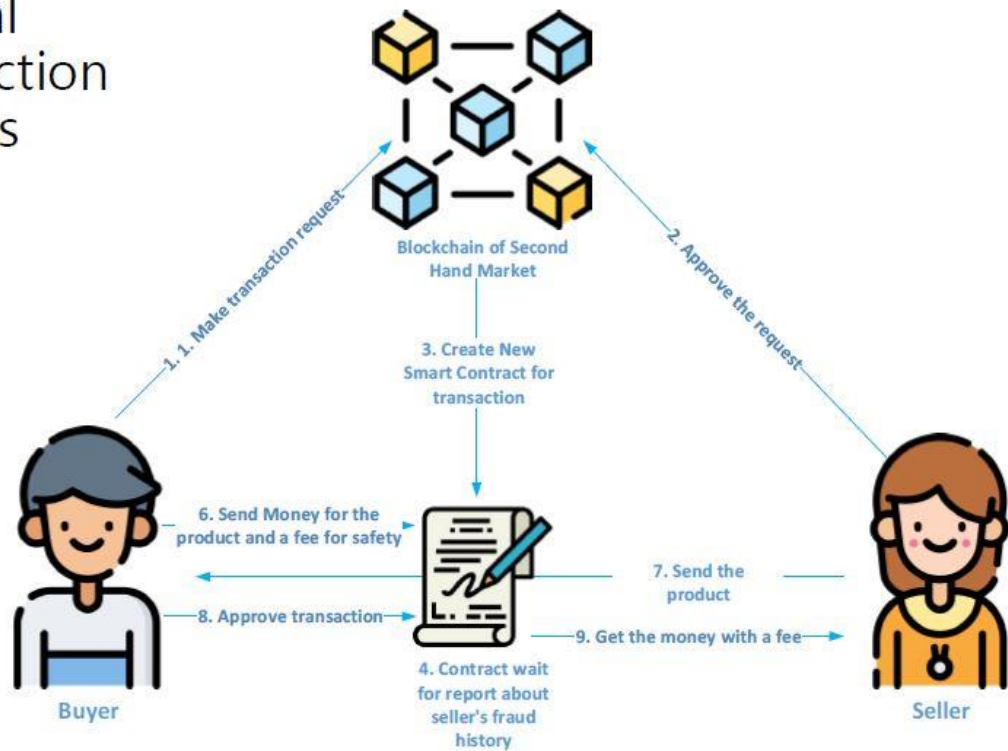
거래 검증에 아무도 참여하지 않을 수 있다. 이럴 경우 해당 거래는 미 검증 상태로 자동 파기된다.

6.3.3.3.4. System state on completion

거래 검증 과정이 정상적으로 진행되어 Buyer 와 Seller 가 서로를 신뢰하게 되고 초기 블록체인에 기재된 내용으로 거래를 진행한다.

6.3.3.4. 해당 거래 모델에 대한 참조용 도식

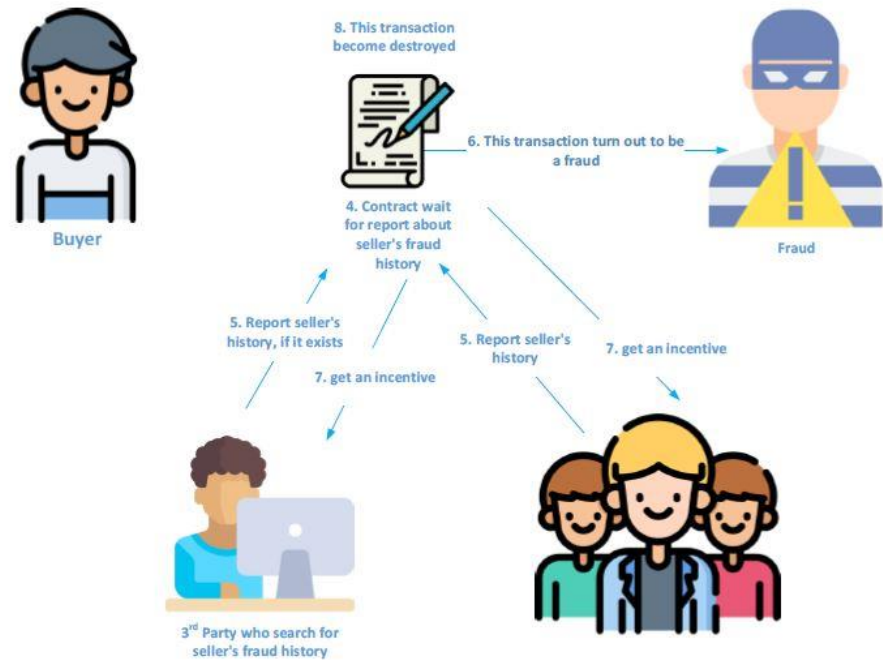
Normal Transaction Process



<그림 1. 일반거래>

1. 거래자의 거래 요청 – 2. 판매자의 승인 – 3. Smart Contract 문서 생성– 4. 송금 – 5. 배송 – 6. 구매자의 상품 확인 후 거래의 승인 – 7. 판매자의 수금.

Detecting Abnormal Transaction Process



<그림 2. 검증거래 모형>

1. 거래자의 거래 요청 - 2. 판매자의 승인 - 3. Smart Contract 문서 생성- 4. 판매자의 사기 관련 검증 대기 - 5. 제3자의 검색 및 검증 - 6. 성공 시 인센티브 부여/거래파기 - 7. 구매자의 상품 확인 후 거래의 승인 - 8. 판매자의 수금.

7. System Model

In this chapter, the relationship between the various system components, the entire system, and the environment surrounding the system is described by a variety of diagrams.

7.1. Context Models

7.1.1. Context Diagram

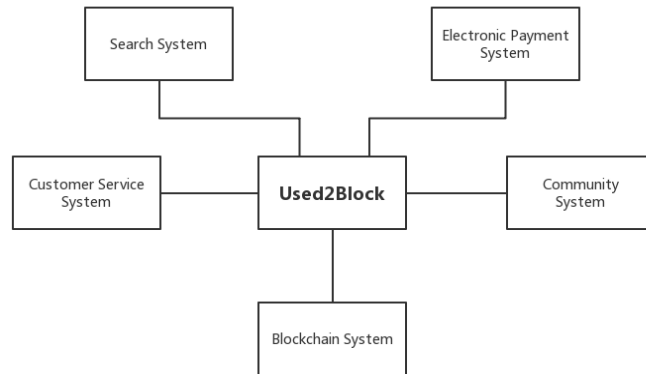


Diagram 1: Overall context diagram

7.2. Process Diagram

7.2.1. Sign up process

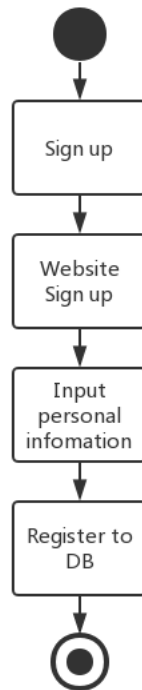


Diagram 2: Sign up process

7.2.2. Overall process

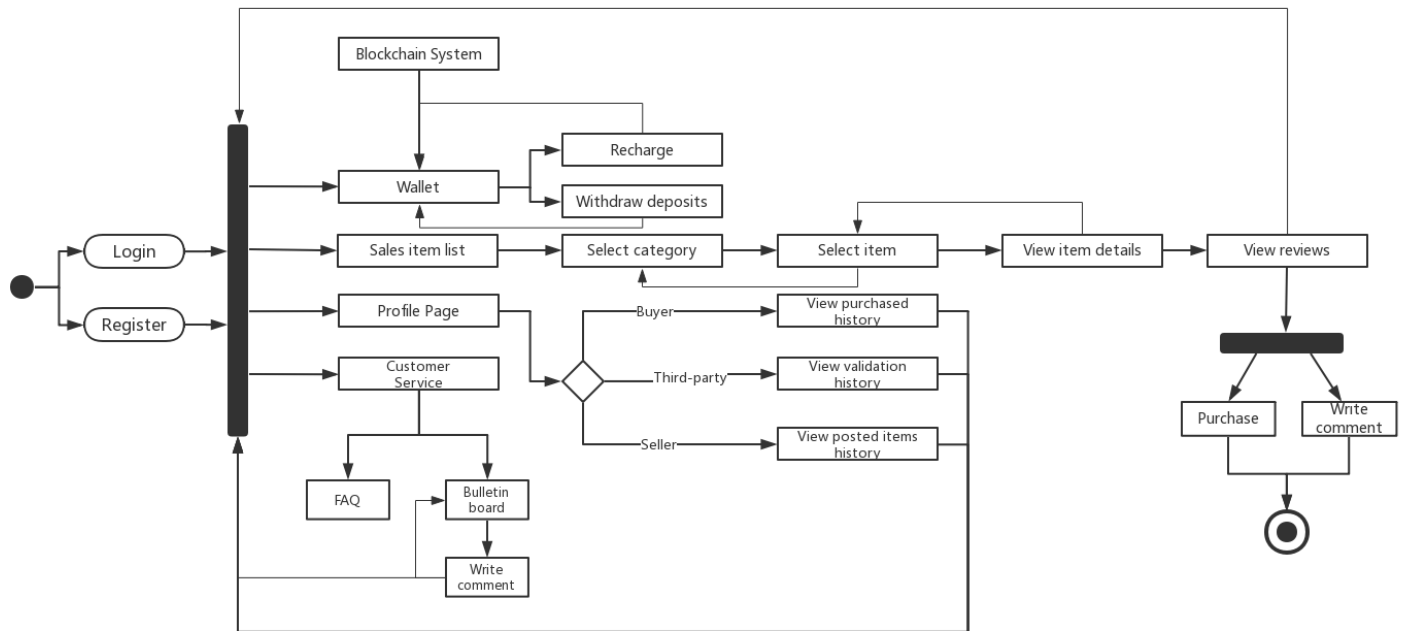


Diagram 3: Overall process

7.2. Interaction Models

7.2.1. Use case Diagram

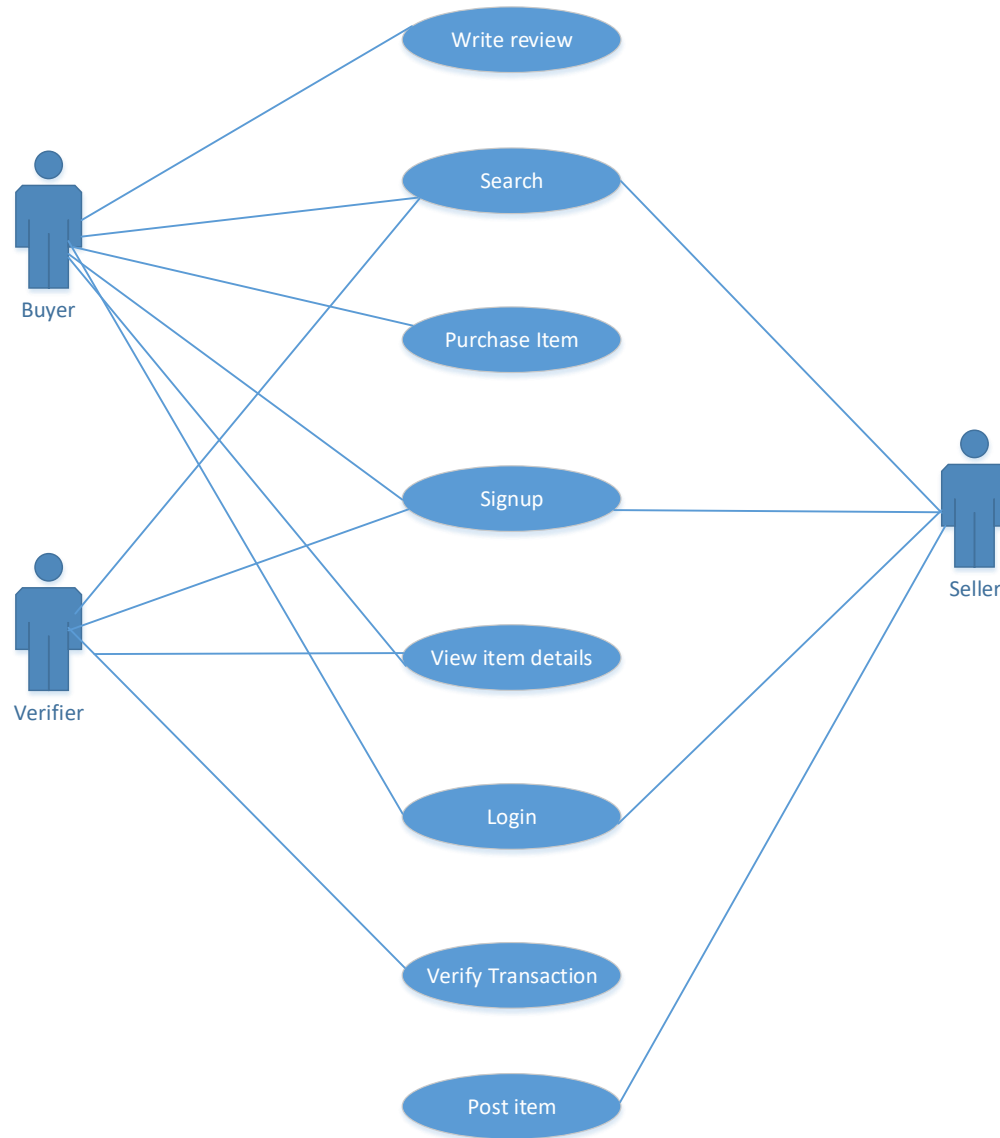


Diagram 4: Use case process

7.2.2. Tubular description for each use case

7.2.2.1. Sign up

Use Case	Sign up
Actor	Buyer User, Seller User, verifier User
Description	<ul style="list-style-type: none">- Ability to request and receive personal information from the user to obtain membership and save this information in the user database- When a user registers for the Used2block service, they must enter their mobile number in their member information.
Data	User's ID and password.
Stimulus	When running the service, request to register at the login screen, and then enter the necessary information to execute the membership.
Response	<ul style="list-style-type: none">- Print out the information needed to join the form on the screen.- If the form entered by the user is the correct information, a completion message will be displayed after updating to the user database.

Table 7-1. Tubular Table: Sign up

7.2.2.2. Login

Use Case	Login
Actor	Buyer User, Seller User, verifier User
Description	It is a process of determining whether the connected user is consistent with user information registered in the system.
Data	User's ID and password
Stimulus	Login request on login screen when running the service
Response	<ul style="list-style-type: none">- ID / PW input form required for login on login page- The information entered by the user is compared with the information stored in the user database.- If it matches, the login success message is displayed, if not, the failure message is displayed.

Table 7-2. Tubular Table: Login

7.2.2.3. Search

Use Case	Search
Actor	Buyer User, Seller User, verifier User
Description	A user searches for a product by name, category, or product description.
Data	User's search keywords
Stimulus	Users enter their search criteria and press the search button.
Response	<ul style="list-style-type: none"> - Modified search criteria, the database SQL query and returns processing to the list of items that match after executing the query. - If no products match the search criteria, an empty list is returned, and an error message is issued stating that no products are found.

Table 7-3. Tubular Table: Search

7.2.2.4. View item details

Use Case	View item details
Actor	Seller User, verifier User
Description	Check the product details listed in the recommendation list, ranking, search, etc.
Data	Product information category.
Stimulus	The user clicks on a product list entry.
Response	The product ID is used to retrieve the product information with the corresponding ID from the database.

Table 7-4. View item details

7.2.2.5. Purchase item

Use Case	Purchase item
Actor	Buyer User
Description	The buyer purchase an item of a seller.
Data	Buyer's address and a period of verification.
Stimulus	The user clicks on one of the shopping lists.

Response	<ul style="list-style-type: none"> - Go to the corresponding product page. - If the corresponding product is deleted or different from the stored condition, the connection is interrupted and an error message is displayed.
-----------------	---

Table 7-5. Purchase item

7.2.2.6. Write review

Use Case	Write review
Actor	Buyer User
Description	The user writes a review for a product.
Data	User's review, etc.
Stimulus	The user clicks a review button for a specific product and enters a review title and description.
Response	<ul style="list-style-type: none"> - Registers a user's new review in the review database and executes the analysis for the review in the Review Analysis System. - If the review is too short or uses slang, an error message is generated without registering the review.

Table 7-6. Write review

7.2.2.7. Post item

Use Case	Post item
Actor	Seller User
Description	Service that seller user proceeds to sell product.
Data	User's product price, quantity, media files, etc.
Stimulus	The seller enters product-uploading page and registers a specific product with descriptions
Response	When the seller user uploads the product details, the product is stored onto DB with the product name, price, specifications, etc.

Table 7-7. Post item

7.2.2.8. Delete item

Use Case	Delete item
Actor	Seller User
Description	The user deletes the items that have been posted.
Data	Reason for deletion.
Stimulus	When the user selects the item to be removed, click the button of the product to be removed.
Response	The item information of the item selected by the user is deleted from the item list.

Table 7-8. Delete item

7.2.2.9. Verify transaction

Use Case	Verify transaction
Actor	Verifier User
Description	The Verifier validate the history of past transactions of a seller.
Data	Date of past transactions, product url, etc.
Stimulus	After the verifier finds the transaction history of a seller, click the Post button to inform a buyer of the history.
Response	<ul style="list-style-type: none"> - If the report is successful, buyer decide whether to continue a transaction or not. - If there is no report, or the transaction destroyed.

Table 7-9. Verify transaction

7.3. Behavioral Models

7.3.1. Data-Driven Modeling

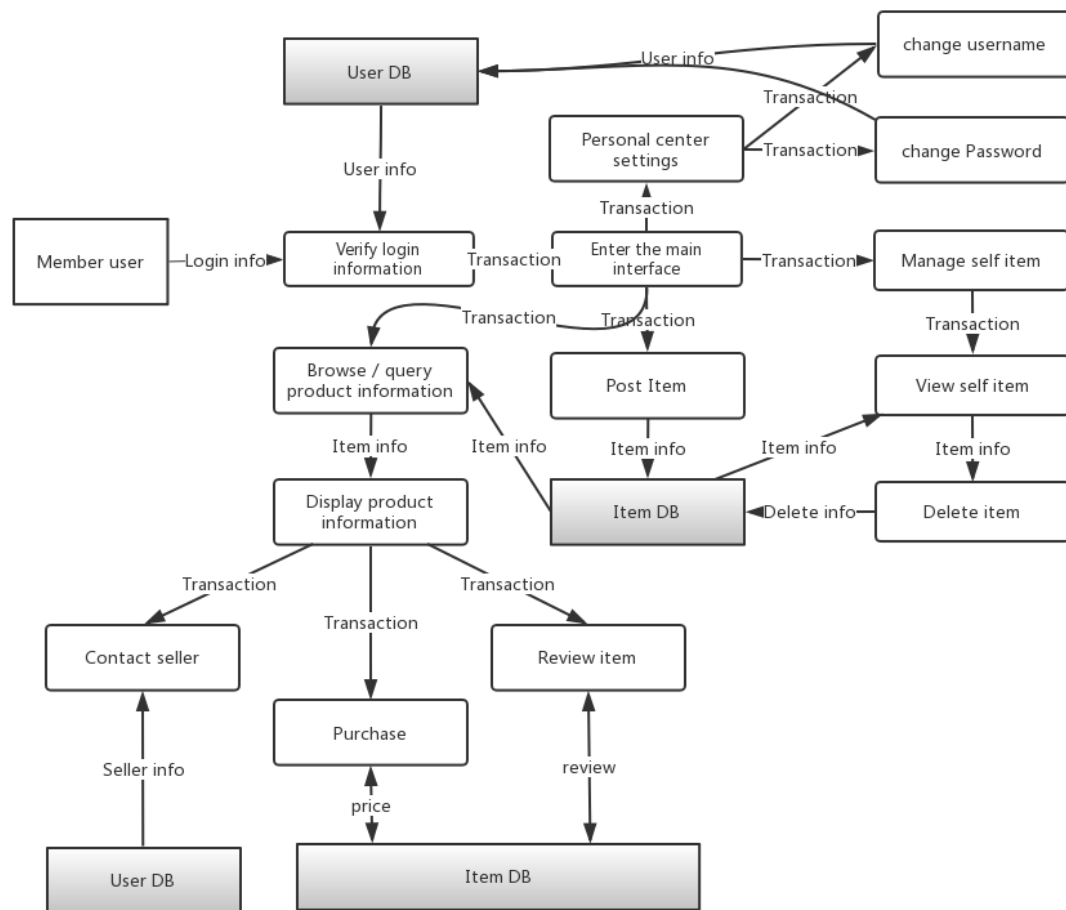


Diagram 6: Member user DFD

8. System Evolution

8.1. 경매 시스템

기본적으로 구매자는 같은 물건을 더 낮은 가격에 사기를 원하고, 판매자는 더 높은 가격에 판매하기를 원한다. 판매자 측이 기업이 아니라 일반인이기 때문에 구매자의 욕구를 충족해주는 것은 힘들 수도 있으며, 물건 가격을 협상하는 과정에서 스트레스를 받을 수도 있다.

이러한 경우에는 판매자가 물건을 올릴 때, 경매 기능을 사용할 수 있도록 해준다. 구매를 원하는 구매자들이 경매를 참가한다. 이 과정에서 경매 참가자들은 자신이 구입하고 싶은 가격을 제출하여 구매가를 갱신한다. 판매자는 자신이 희망한 판매가와 경매 최고 갱신액 중 원하는 가격으로 자신의 상품을 판매할 수 있다.

8.2. 품질 보증 시스템

구매자는 물건을 사더라도 최상의 상태인 물건을 사기를 원한다. 하지만 인터넷으로 거래되는 중고거래 특성 상 물건 상태를 직접 확인하기는 어렵다.

이러한 단점을 해소하기 위해, 구매자가 원하는 경우에 한하여

- i) 전자기기 같이 A/S 센터에서 수리를 받는 물품에 대해서는 A/S센터에서 수리 로그를 받아서 공개하도록 한다. 이러한 방안은, A/S센터에서 수리 로그를 받을 수 있을지가 미지수이다.
- ii) 판매자가 판매를 원하는 상품을 운영 측으로 배송한다. 운영 측에 있는 해당 카테고리 상품의 최소 준 전문가 수준에 해당하는 감정사가 상품에 대한 감정을 진행한다. 그리고 감정사가 적절한 감정가를 제시한다. 하지만 이 방법은 추가적인 인건비를 필요로 하며, 거래 과정의 복잡도와 시간이 증가하게 된다.

8.3. 상품 추천 시스템

구매자가 특정 물건을 사기를 원하면, 해당 카테고리에서 물건을 찾거나 검색 기능을 활용하여 물건을 찾을 것이다. 그렇게 쌓인 검색 로그를 분석하여 구매자가 원하는 물건을 추정한다. 추정한 데이터를 바탕으로, 신뢰도가 높은 방식으로 판매자와 원하는 가격대의 물건들을 나열해 추천 상품을 보여준다.

8.4. 개인정보 보호를 위한 hash 값 활용

서비스 초기에는 user 들의 거래 내역이 없는 상태이기 때문에, 제 3자인 verifier 를 통해 seller 의 번개장터, 중고나라 등의 타 플랫폼에서의 거래 기록을 확인하여 seller 의 신뢰도를 확인하는 과정을 거친다. 이 과정에서는 seller 의 개인정보가 유출될 위험이 크다.

따라서 거래 검증 과정마다 판매자에 대한 검증 여부와 개인정보에 대한 Hash값을 블록체인에 기록하여, hash값을 통해 seller의 신뢰도를 검색 및 확인하는 방식으로 변경한다.

8.5 모바일 어플리케이션 연동

Used2Block 은 웹 기반의 플랫폼이다. 일반 사용자들이 일반 PC 보다는 휴대전화나 태블릿 PC 등의 모바일 기기를 많이 사용하는 추세에 따라, Used2Block 모바일 어플리케이션을 출시하여 PC 를 통한 접근 뿐만 아니라 모바일 기기에서의 접근성을 높일 예정이다.

9. Appendices

10. Indexes

10.1. Tables

10.2. Figures

10.3. Diagrams

11. References