


# 캡스톤 디자인 I

## 종합설계 프로젝트

프로젝트 명	An incentivied, blockchain-based, Q&A service
팀 명	K-Block
문서 제목	결과보고서

Version	1.2
Date	2018-05-25

이름	박고은
----	-----

 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05


#### CONFIDENTIALITY/SECURITY WARNING

이 문서에 포함되어 있는 정보는 국민대학교 전자정보통신대학 컴퓨터공학부 및 컴퓨터공학부 개설 교과목 캡스톤 디자인I 수강 학생 중 프로젝트 "xxxx xxxx"를 수행하는 팀 "xxxxx"의 팀원들의 자산입니다. 국민대학교 컴퓨터공학부 및 팀 "xxxxxx"의 팀원들의 서면 허락없이 사용되거나, 재가공 될 수 없습니다.

## 문서 정보 / 수정 내역


<b>Filename</b>	결과보고서.doc
<b>원안작성자</b>	박고은
<b>수정작업자</b>	박고은

수정날짜	대표수정자	Revision	추가/수정 항목	내 용
2018-05-23	박고은	1.0		전체 작성

 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

## 목 차

1	개요 .....	4
1.1	프로젝트 개요 .....	4
1.2	추진 배경 및 필요성 .....	4
2	개발 내용 및 결과물 .....	6
2.1	목표 .....	6
2.2	연구/개발 내용 및 결과물 .....	7
2.2.1	연구/개발 내용 .....	7
2.2.2	활용/개발된 기술 .....	8
2.2.3	현실적 제한 요소 및 그 해결 방안 .....	8
2.2.4	결과물 목록 .....	9
2.3	기대효과 및 활용방안 .....	9
3	자기평가 .....	10

 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

# 1 개요

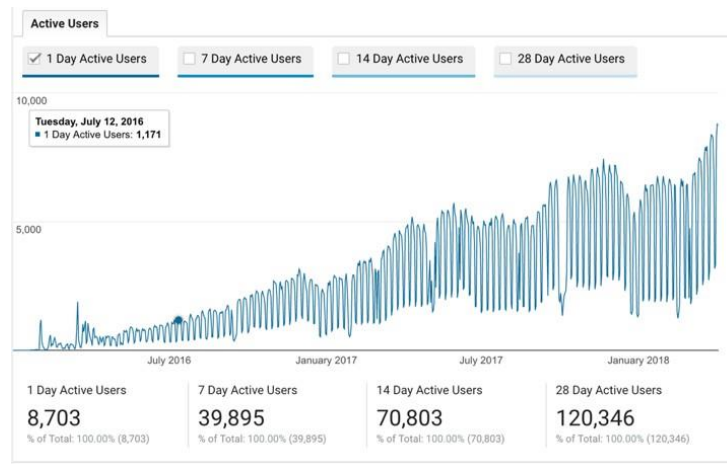
## 1.1 프로젝트 개요

본 프로젝트는 그렙(<http://grepp.co>)과 산학프로젝트로 이더리움 및 이오스 플랫폼 기반 응용 QnA DAPP 서비스를 개발한다. 진행된 프로젝트는 블록체인기반의 가상화폐를 발행해 기존의 Q&A 서비스에 보상시스템으로 활용하고자 하는데 목적이 있다. 대상은 현재 그렙에서 운영하는 Q&A 서비스인 해시코드이며, 개발자를 위한 Q&A 서비스로 해외의 스택오버플로와 유사한 형태로 운영되고 있다. 프로그래머들에게는 퀄리티 높은 질문과 좋은 답변을 하여 프로그래머로서 성장해 갈 수 있는 서비스를 제공하도록 개발한다.

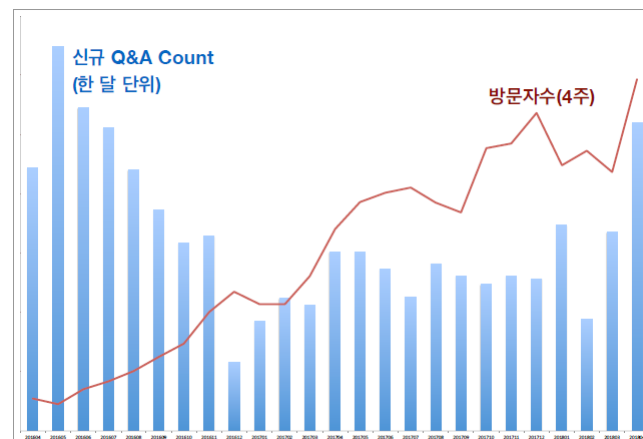
블록체인 기반의 가상화폐를 이용자 및 예비 이용자들에게 지급하여 커뮤니티 활동에 동기 의식을 부여하고 구성원들의 기여도를 투명성 있게 반영해 정확하게 보상하고자 한다. 이를 위한 블록체인 플랫폼으로 이더리움과 EOS를 채택했으면 본인이 맡은 역할을 이더리움이다.

이더리움 기반의 플랫폼과 가상화폐를 이용해 스마트 계약 기능을 제공함으로써, 기존의 높은 수수료를 절감하고 보안성, 안정성을 보장받고 신뢰할 수 있는 DAPP(Decentralized Application)을 개발한다. 해시코드 기존의 질문 답변에 대한 점수 제도를 가져오되 구분하여 점수를 쌓을 수 있게 한다. 자연스럽게 질문을 등록하는 사용자를 증가하도록 유도하여 해시코인 서비스를 성장시키고자 한다. 지식인과 스팀잇이 합해진 결과를 해시코드에 반영한다.

## 1.2 추진 배경 및 필요성



▲ 해시코드 DAU 증가 현황




▲ 방문자 수는 증가하고 있지만 콘텐츠 공급량은 답보상태

그래프에서 운영 중인 해시코드는 하루 평균 방문자 수(DAU)가 서비스 시작 이후 계속 증가하여 현재는 하루에 1만 명 내외의 방문자가 접속하는 서비스가 되었다. 하지만 이에 비례해서 증가해야 할 콘텐츠(질문 및 답변)가 등록되는 양은 답보상태에 있는데 이를 개선해 증가하는 방문자만큼 콘텐츠가 등록되는 양도 증가한다면 그만큼 방문자는 기하급수적으로 증가할 수 있다.

시간 흐름에 따른 관심도 변화 ?



 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

▲ 구글 트렌드라는 도구를 활용한 스팀잇의 검색량 변화

이러한 문제점에 블록체인 기술을 활용한 q&a 시스템이 방안이 될 수 있다. 개발자들에게도 좋은 질문과 답변을 할 수 있는 개발자 커뮤니티 공간이 늘어나고 있는데 SNS라는 서비스를 명확하게 눈앞에 보여주니, 오히려 신뢰가 더 강하게 생기는 것이다. 그리고 눈 앞에 보이는 보상체계가 필요하다. 기존의 시스템들은 중앙에서 설정된 기준에 의하여 아주 소액으로만 이루어지지만 스팀잇은 사용자가 콘텐츠 이용대가를 지불하고 그에 대한 액수 또한 적지 않다는 점이 장점이다. 이 보상이 어디로부터 나온 것인지 블록체인을 활용하여 Audit이 가능하기 때문에 더 신뢰성을 높일 수 있다. 삭제 및 위/변조가 불가능한 블록체인의 특성상 운영자의 관리와 제재가 투명하게 저장되므로 효과적인 해결책이 될 수 있다.


현재 그랩은 개발자들의 성장과 구인구직, 소프트웨어 가치의 사회적 확산을 목표로 서비스를 제공하고 있으며 더불어 많은 사용자를 모으는 것을 목표로 하고 있다. 그 중 해시코드는 많은 사람이 자신에게 놓인 문제를 공유하고 그와 비슷한 문제를 겪은 사람들이 경험을 공유할 수 있는 장이 될 수 있다. 그러나 해시코드 방문자들은 주로 검색을 통해 유입되어 그저 검색에 그친다. 방문자수는 지속해서 성장하고 있으나, 방문자 수 증가에 비해 Q&A 글은 한달전과 비슷하다. 실제로 일평균 새롭게 올라오는 질문 수는 5~10 개 이내에 불과하다. 따라서 서비스 마케팅 관점에서 유저에게 상호작용과 피드백을 제공하는 서비스 시스템과 핵심 서비스 개발로 많은 사용자들이 서비스에 상주하는 시간을 늘리고, 사용자의 성취감을 주는 요소를 추가로 넣어 커뮤니티 활성화가 필요하다.

## 2 개발 내용 및 결과물

### 2.1 목표

블록체인 기반의 가상화폐를 발행해 콘텐츠 제공의 지급함으로써, 이용자 및 예비 이용자들로 하여금 동기 의식을 부여해 커뮤니티를 참여를 독려하고 각 커뮤니티 구성원의 기여도를 일관되게 반영할 수 있는 공정한 회계 제도로 블록체인을 서비스에 적용하고자 한다.

이더리움 기반의 가상화폐를 발행하고 질문과 답변 등의 커뮤니티 활동에 이 가상화폐를 보상으로 지급하는 탈중앙화 어플리케이션(dApp)을 개발한다.

 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

1. DAPP 이용자들에게 돌아가는 인센티브를 강화하기 위해 코인 이코노미 사례를 분석하여 DAPP 안의 경제 시스템을 확립한다. 이용자들에게 자율성을 보장함과 동시에 악용하는 사례를 막을 수 있는 체계를 만든다.
2. 이용자 확보와 유지 및 커뮤니티 활성화를 위해 이용자들에게 동기부여와 몰입을 줄 수 있는 목표와 도전의식을 주는 요소를 찾아 적용시킨다.
3. DAPP 이용자의 주 타겟인 개발자 성향을 파악하여 웹 UI/UX를 설계한다.
4. solidity로 개발되는 블록체인의 코인을 이해하고, Truffle framework와 ganache-cli를 이용하여 solidity와 javascript, json으로 저자와 보팅한 사람들에게 보상을 나누어 주는 코드를 구현한다.

## 2.2 연구/개발 내용 및 결과물

### 2.2.1 연구/개발 내용

#### 1) 가상화폐 발행

ETHEREUM 기반의 가상화폐를 발행하기 위해 스마트 컨트랙트를 개발했다. 컨트랙트에는 송금기능 / 질문 등록 / 답변 등록 / 가입 / upvote / 답변 채택 / 채택답변자보상 / 기부 / 등급 측정 하는 액션이 포함되어 있다.

이 컨트랙트를 deploy하여 action 권한을 가진 계정이 사용할 수 있도록 하였다.

#### 2) test case 구현 및 실행

```


Contract: gasToken
  ✓ should sign in (182ms)
  ✓ should regist question (148ms)
  ✓ should regist answer (171ms)
  ✓ should choose answer (1383ms)
  ✓ should upvote (68ms)
  ✓ should reward answer (61ms)
  ✓ should donate token (76ms)

? passing (2s)

```

질문을 등록하는 액션, 답변을 채택하는 액션 등 이용자들이 취할 수 있는 행동에 대응하는 스마트 컨트랙트를 테스트하는 코드를 개발했다. 이를 활용해 가상화폐를 분배할 수 있으며 기여도에 따라 운영자의 개입 없이 토큰을 발행해서 지급할 수 있다.

#### 3) 스마트 컨트랙트 보안 취약성 분석

 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

## 스마트 컨트랙트 보안 취약성과 분류체계

classification of vulnerability checks in Ethereum using security tools

### 요 약

이더리움은 암호화폐 교환 및 스마트 컨트랙트의 자체적 검증 애플리케이션 개발을 가능하게 하는 개방형 플랫폼을 제공하고 블록 체인 영역 내에서 디지털 자산 및 다양한 분산 응용 프로그램을 보유할 수 있는 토대를 제공한다. 이더리움과 스마트 컨트랙트는 공개적이고 분산되어 있으며 불변하기 때문에 개발자의 단순한 코딩 실수로 인한 취약점에 약하다.

이더리움과 스마트 컨트랙트는 공개적이고 분산되어 있으며 불변하기 때문에 개발자의 단순한 코딩 실수로 인한 취약점에 약하다. 스마트 컨트랙트의 보안 침해 및 반복적인 재정적 손실을 예방하기 위해 스마트 컨트랙트의 보안 분야를 분석하여 KCC정보과학회에 논문을 제출하였다.

### 2.2.2 활용/개발된 기술

콘텐츠 제공자에게 가상화폐를 보상하는 시스템을 구현하기 위해 블록체인 기술이 활용되었다. 구체적으로는 전자서명과 암호화 해시 기법이 가상화폐에 활용되었고 이를 거래하는 트랜잭션들을 가치교환거래가 순차적인 블록단위로 분류된 형태의 분산 장부 형태로 저장되었다.

각 블록은 기존 블록과 연결되며 암호 메커니즘을 기반으로 Peer-to-peer 네트워크를 통해 지속적으로 기록되며, 특정 조건이 달성되면 자동적으로 프로그램이 실행되어 계약이 이행되는 탈중앙화된 어플리케이션(dApp)의 기술이 프로젝트에 사용되었다.

### 2.2.3 현실적 제한 요소 및 그 해결 방안

- 스마트 컨트랙트는 상당수의 가상 화폐를 처리 할 수 있기 때문에 악용하고 싶을 만큼 쉽게 재정적으로 높은 인센티브를 취할 수 있다. 이더리움과 같은 스마트 계약 플랫폼은 임의의 참가자가 참여할 수 있는 공개 네트워크에서 작동하기 때문에 이들의 실행은 공격자의 조작 시도에 취약하다.

→ 보안 침해 및 반복적인 재정적 손실을 예방하기 위해 스마트 컨트랙트의 보안 분야를 보안 코드 분석 도구로 검사한다.

- 현재 EOS는 버전4.1 플랫폼이며 새롭게 업데이트 되고 있다. 최근 메인넷 런칭을 앞두고 api가 자주 바 꾸고 있어 변경사항을 계속 팔로우하면서 이를 적용해야 한다.



 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

→ EOS 1.0이 6월에 정식으로 런칭된다면 안정화 될 것으로 보인다.

- 스마트 계약은 법적 강제성이 없고 알고리즘에 의한 계약으로 계약 불이행 시 피해 보상에 대해 법적인 보호를 받기 힘들다. 분산 장부인 블록체인의 도입 및 활용은 다양한 법적 문제의 발생 가능성을 내재하고 있지만 현행법은 중앙 집중 관리체계에 초점을 두고 있어 탈중앙화 블록체인 기술과는 맞지 않다.

- 초기 토큰 분배

초반에 많은 사용자들이 어느정도 토큰을 가지고 있어야 토큰 이코노미를 설계가 가능하다. 따라서 초기 토큰 분배가 필요하다.

→ 토큰을 받은 모든 사람에게는 이 토큰의 가치를 올릴 초기 인센티브가 발생하며 참여함으로써 자발적으로 토큰을 획득할 수 있다.

- 콘텐츠의 가치 판단

질문 및 답변의 퀄리티를 사람이 주관적으로 가치를 판단하기 어렵다.

→ 큐레이션을 도입해 시장 경제 시스템을 통해 많은 이용자들에게 보팅을 받은 질문과 답변에 더 큰 가치를 보상해 줄 수 있을 것이다.

## 2.2.4 결과물 목록

### 1) EOS 스마트 컨트랙트

EOS 기반 token 컨트랙트.

질문 및 답변 등록과 채택에 따라 계약을 이행하는 dApp.


### 2) 블록체인 네트워크와 통신하는 웹 클라이언트

## 2.3 기대효과 및 활용방안

<기대 효과>

### 1. 해시코드의 이용자들에게 커뮤니티 활동에 강력한 동기 의식을 부여 + 투명성 보상

토큰을 받은 모든 사람에게는 이 토큰의 가치를 올릴 인센티브가 생기며, 개발자라면 해시코드 커뮤니티 참여를 통해 가치를 올릴 수 있다. 이를 통해 정리된 소프트웨어 개발 Q&A 콘텐츠에 대한 수요는 계속 늘어나는데, 공급의 정체 상태를 극복하고 해시코드 서비스를 성장시킨다. .

 <b>국민대학교</b> <b>컴퓨터공학부</b> <b>캡스톤 디자인 I</b>	<b>결과보고서</b>		
	<b>프로젝트 명</b>		
	<b>팀 명</b>		
	Confidential Restricted	Version 1.2	20xx-JUN-05

## 2. 중개자가 사라져서 수수료 0 의 서비스 이용

이더리움 플랫폼 기반 DAPP 은 중개자 비용을 지불하지 않아도 된다. 이로써 많은 사용자를 끌어들이 수 있다. 특히 해외유저의 경우 수수료 절감에 큰 효과를 볼 수 있다.

### <활용방안>

#### 1. 구인 구직 사이트

구인구직 플랫폼으로 확장할 경우 보상 개념으로 프로그래밍 실력을 가늠하는 척도로 삼을 수 있게 한다. 그리고 구인 구직자를 중개자 없이 무료로 가까운 수수료로 매칭 가능하다. 좋은 질문을 하고 좋은 답변을 한 이용자에게 더 많은 보상이 돌아가도록 설계한 것처럼 뛰어난 프로그래머 이용자들에게 더 많은 보상이 돌아가도록 한다

2. 게임화를 적용하여 재미와 보상을 주고, 이용자들에게 보다 나은 서비스 활성화를 추구  
프로그래밍 언어 학습을 시작할 때의 장벽을 없애기 위해 대회의 우승 상금으로 코인을 지급하거나 알고리즘 문제 해결의 보상을 줄 수 있고, 프로그래밍 강의 시청에 대한 보상을 얻도록 확장하여 활용할 수 있다. 폭넓은 소프트웨어 시장에서 다양한 서비스와의 연계가 가능하다.

## 3 자기평가

본 프로젝트는 기존의 운영하고 있는 서비스에 가상화폐를 적용하는 프로젝트로 기존의 웹사이트 위에서 dApp 형태로 토큰을 발행 했다. 프로젝트 내에서 이더리움 solidity 개발자 역할로 서비스를 구현하였다. 각 구현한 함수 기능에 대해 테스트 코드를 작성하며 올바르게 작동하는지 즉각 확인하고자 하였다. 이더리움 보안 취약성을 분석하기 위해 최대한 공부하여 관련 논문을 작성하기도 하였다. 그러나 다양한 보안 툴을 익히고 실행하는데 어려움을 겪었다. 프로젝트를 더 진행하면서 보완해나갈 예정이다.