



국민대학교
전자정보통신대학
컴퓨터공학부

CONFIDENTIALITY/SECURITY WARNING

이 문서에 포함되어 있는 정보는 국민대학교 전자정보통신대학 컴퓨터공학부 및 컴퓨터공학부 개설 교과목 캡스톤 디자인Ⅰ 수강 학생 중 프로젝트 “블록체인을 활용한 **QnA DAPP** 서비스 개발”을 수행하는 팀 “**K-Block**”의 팀원들의 자산입니다. 국민대학교 컴퓨터공학부 및 팀 “**K-Block**”의 팀원들의 서면 허락없이 사용되거나, 재가공 될 수 없습니다.

캡스톤 디자인 I 종합설계 프로젝트

프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발
팀 명	K-Block
문서 제목	수행계획서

Version	2.0
Date	2018-04-12

이름	김형민
----	-----

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12


문서 정보 / 수정 내역

수정날짜	대표수정 자	Revision	추가/수정 항 목	내 용
2018-03-03	김형민	0.1	최초 작성	개요 및 배경 기술 일부 작성
2018-03-07	김형민	0.9	내용 수정	개발 일정 및 자원관리 재조정
2018-03-08	김형민	1.0	내용 수정	전체 항목 최종 수정
2018-04-07	김형민	1.1	내용 수정	리뷰 반영하여 개요, 개발목표 수정
2018-04-11	김형민	1.6	내용 수정	배경 기술, 역할 분담 항목 수정
2018-04-12	김형민	2.0	내용 수정	전체 항목 수정

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

내용

1	개요	4
1.1	프로젝트 개요	4
1.2	추진 배경 및 필요성	4
2	개발 목표 및 내용	6
2.1	목표	6
2.2	연구/개발 내용	6
2.3	개발 결과	7
2.4	기대효과 및 활용방안	8
3	배경 기술	8
3.1	기술적 요구사항	8
3.2	현실적 제한 요소 및 그 해결 방안	9
4	개발 일정 및 자원 관리	10
4.1	개발 일정	10
4.2	일정별 주요 산출물	10

 <div> <p>국민대학교</p> <p>컴퓨터공학부</p> <p>캡스톤 디자인 I</p> </div>	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

1 개요

1.1 프로젝트 개요

본 프로젝트를 통해 그랩에서 운영중인 해시코드(hashcode.com)를 벤치마킹하여 QnA DAPP 서비스를 설계하고 개발한다. DAPP에서 사용되는 토큰을 발행하여 DAPP을 이용하는 이용자와 블록체인을 유지하는 노드들은 토큰 보상을 얻을 수 있게 한다.

토큰을 얻고자 하는 행동 유도를 위해 Gamification을 적용한다. 게임 디자인 요소로 동기유발 매체를 만들어 고객 서비스의 충성도와 편의성을 높이는 서비스를 개발한다.

이더리움 블록체인을 기반으로 하여 P2P 네트워킹, 사용자 소유 아이덴티티, 안전한 암호화 지불 방식 등을 활용하여 이용자 계좌 잔고 관리부터 보안 투명성까지 다양한 신뢰에 기인되는 문제들을 해결하는 탈중앙화 네트워크를 구축한다.

1.2 추진 배경 및 필요성


1. 왜 QnA인가? - QnA의 필요성

버스에서 짧은 대화를 나누거나 누군가를 가르치면서, 인터넷에서 댓글을 달거나 친구와 깊이 있는 토론을 하면서도 우리는 주변 모든 사람을 가르칠 기회가 있다. 어떤 상황에서도 효과적으로 가르칠 수 있는 방법이 있는데, 그것은 바로 질문을 하는 것이다. 좋은 질문은 좋은 배움으로 이어지며, 더 좋은 정보를 찾을 수 있도록 도와준다. 그리고 무엇보다 우리를 성장시키고, 가르치고, 자신감을 심을 수 있다. 다행스럽게도 공부하고 연습하고 배우면 누구라도 더 좋은 질문을 할 수 있다.

개발자들에게도 좋은 질문과 답변을 할 수 있는 개발자 커뮤니티 공간이 늘어나고 있는데 대표적으로 Stackoverflow, Quora, 생활코딩, 코드카데미 외 여러 국내외 커뮤니티들이 있다. 이러한 공간에서 때때로 누구도 알지 못한 놀라운 창의성과 아이디어를 찾을 수도 있다.

2. 그저 검색에 그치는 이용자들

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 개발자 노다지라 할 수 있다. 그러나 해시코드 방문자들은 주로 검색을 통해 유입되어 그저 검색에 그친다. 타서비스와 비교해 보았을 때 활발히 활동하는 이용자들은 많은 편이라 하기에는 어려운 숫자이며, 실제로 일평균 새롭게 올라오는 질문 수는 5~10개 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.

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

3. 명예의 전당

명예의 전당 ? 최근 7일 종합



Figure 1 명예의 전당

내 질문에 좋아요가 달리면: 좋아요 숫자 X 5점
 내 질문의 답변중 하나를 채택하면: 5점
 내가 올린 답변에 좋아요가 달리면: 좋아요 숫자 X 10점
 내가 올린 답변이 채택되면: 15점
 내가 편집 요청을 해서 받아들여지면: 2점
 다른 사람의 질문/답변에 싫어요를 하면 내 점수가 -1점
 단 질문이나 답변의 좋아요 점수가 0보다 작으면: 싫어요 숫자 X 2점

Figure 2 해시코드 점수 제도

현재 해시코드는 Figure 2와 같이 점수 정책에 따라 점수 제도를 운영하고 있다. 점수 제도를 바탕으로 높은 점수를 가진 이용자에게는 일종의 특권이 주어진다. 신뢰할 수 있는 사용자로 판단되어 질문 글에 대한 편집, 모든 글에 태그 수정 권한 등을 가진다. 그리고 명예의 전당에서 점수 상위 10명을 확인할 수 있다. 그러나 4월 11일 기준 2위인 이용자는 1달간 활동하지 않았음에도 순위의 변동이 일어나지 않고 있다.

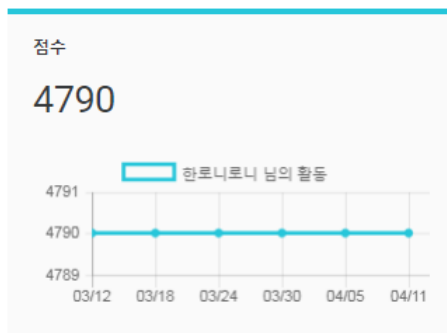


Figure 3 명예의 전당 2위 1달간 활동 내역

이는 적은 이용자 수를 원인으로 꼽을 수도 있으나, 명예의 전당에 이름을 올리려는 경쟁심과 같이 목표 달성과 관련된 심리적 기제를 불러 일으키기엔 점수만으로는 사용자의 인식이 부족한 사례로 볼 수 있다.

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

2 개발 목표 및 내용

2.1 목표.

1. 이더리움 기반의 플랫폼을 이용해 가상화폐 거래 기능을 제공한다. 중개자 없이 거래의 효율성과 투명성을 높이고 적은 수수료로 빠르고 안전한 거래가 가능하게 한다.
2. DAPP 이용자들에게 돌아가는 인센티브를 강화하기 위해 코인 이코노미 사례를 분석하여 DAPP 안의 경제 시스템을 확립한다.
3. 이용자 확보와 유지 및 커뮤니티 활성화를 위해 이용자들에게 동기부여와 몰입을 줄 수 있는 목표와 도전의식을 주는 퀘스트를 개발하여 게임적 요소들을 적용시킨다.
4. 실물 가치를 지니는 토큰(가상화폐)을 발행함으로써 생기는 신뢰성의 문제를 해결한다. 보안과 안정성, 토큰 가격 변동성에 대한 문제를 해결한다.
5. DAPP 이용자의 주 타겟인 개발자의 성향을 파악하여 웹 UI/UX를 설계한다.
6. 해시코드의 질문 답변에 대한 점수 제도를 가져오되 경험, 환금성, 기술, 카르마, 평판 점수로 구분하여 추가로 점수를 쌓을 수 있게 한다.

경험 점수	시스템 안에서 하는 모든 행동을 점수로 쌓는다.
환금성 점수	적립한 후 무언가를 바꾸거나 구입하는데 쓸 수 있다. 가상 공간 경제의 기반이 된다. Ex)쌓은 점수를 다운하여 코인으로 환급 받을 수 있다.
기술 점수	특정한 임무나 부가적인 목표를 달성했을 때 얻을 수 있는 일종의 보너스 점수 ex)퀘스트
카르마 점수	이타적인 행동에 대해 감사의 뜻으로 선물할 수 있는 점수. ex)무료 강의에 대한 감사 기부. 좋은 답변에 대한 기부.
평판 점수	신뢰를 구축함으로써 쌓는 점수. 명성도

2.2 연구/개발 내용

- 웹 UI/UX - 화면기획서
- 인센티브 정책 수립
- 게임화 적용 시나리오 설계
- 웹 아키텍처 설계
- Smart Contract 설계



계획서		
프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
팀 명	K-Block	
Confidential Restricted	Version 2.0	2018-04-12



2.3 개발 결과

기능 요구사항

1. 웹 지갑에서 출금 및 송금이 가능해야 한다.
2. 점수를 코인으로 환급 받을 수 있어야 한다.
3. 질문자는 코인을 걸어 질문 할 수 있어야 한다.
4. 원하는 질문자에 한해 질문 목록의 상위에 노출시킬 수 있어야 한다.
5. 채택된 답변자는 질문에 걸린 코인을 지급받아야 한다.
6. 가입 시 정해진 양의 코인을 지급한다.
7. 프로필에서 점수와 주간 보상 받은 코인을 확인할 수 있어야 한다.
8. 점수를 쌓는 방법은 질문, 답변, vote 외에 다른 방법으로도 쌓을 수 있어야 한다.
9. 이용자는 특정 질문에 걸린 코인양에 추가로 코인을 더할 수 있다.
10. 좋은 답변 글을 남긴 답변자에게 코인을 기부할 수 있어야 한다.
11. 스마트 거래 내역을 블록에 저장해야 한다.
12. 블록체인을 유지하는 노드들에게 매월 보상을 지급해야 한다.
13. 구인 희망자는 코인을 지불해 해당 프로필의 이력서를 열람할 수 있어야 한다.

비기능 요구사항

1. 사용자간 트랜잭션이 일어날 경우 Account, Amount, Payload, GasLimit 등의 정보를 채널로 채굴자에게 브로드캐스트 되어야 한다.
2. 브로드캐스트를 받은 채굴자는 문법, 전자서명, 넌스, 거래비용을 검증하고 트랜잭션풀을 실행한다.
3. 노드간 통신을 통해 블록생성직후 노드(지갑)에서 발생하는 거래기록을 모아 서로 공유하고 노드 각각이 가진 블록체인 데이터와 비교해 오류가 없는지 검증 후 암호화된 블록을 모든 노드들이 동시 생성해야만 한다.

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

2.4 기대효과 및 활용방안

기대효과

1. 블록체인 네트워크를 구성하여 중개자가 사라져도 높은 보안성과 수수료 절감 효과
프로필 열람 기능 혹은 구인구직 플랫폼으로 확장할 경우 블록체인을 적용함으로써 분산 원장으로 변조가 불가능하다. 투명하고 신뢰받는 사회 구현을 위한 기폭제 역할을 수행할 수 있을 것이다. 그리고 Application에서 가상화폐로 약 1%대의 수수료로 거래가 이루어 진다.

2. 게임의 부분적인 요소들만으로 게임화를 적용하여 재미와 보상을 주고, 이용자들에게 강력한 동기유발 매체로 만든다. 그리고 이 매체들을 완수하는 과정에서 보람을 얻고 프로그래밍 질문과 답변의 참여율을 높인다. 그 예시로 Codecademy는 프로그래밍 언어를 독학할 수 있는 사이트인데, Gamification을 적용한 시스템을 도입하여 프로그래밍 언어 학습을 시작할 때의 장벽을 없애기 위해 프로그램 작성이 모두 웹 브라우저상에서 가능하도록 설계하고 또한 점수와 훈련 시스템 등을 도입해 전체적인 레슨 진행 상황을 눈으로 보여주면서, 적절한 타이밍에 피드백을 제공하여 2011년 8월 서비스를 시작한지 72시간 만에 20만 명의 유저를 모집하였다.

활용방안

1. 제2의 페이스북으로 불리고 있는 스팀잇(steemit.com)을 벤치마킹하여 Pow 방식에서 Pos방식으로 전환하여 '코딩파워' 개념을 만들어본다. 구인구직 플랫폼에서 '코딩파워'를 프로그래밍 실력을 가늠하는 척도로 삼을 수 있게 한다. 그리고 구인 구직자를 다이렉트로 매칭시켜 줌으로써 무료로 가깝운 수수료로 소프트웨어의 가치 확산을 일으킬 수 있을 것이다. 또한 채굴자에게 많은 보상이 돌아가는 것이 아닌 **좋은 질문을 하고 좋은 답변을 한 이용자에게 더 많은 보상이 돌아가도록 한다.**

2. 토큰ICO를 통해 투자를 받아 서비스 공급자는 보다 나은 서비스 활성화를 추구한다.
예를 들어 프로그래밍 대회 우승 상금으로 코인을 지급하거나 알고리즘 문제 해결의 보상을 줄 수 있고, 프로그래밍 강의 시청에 대한 보상을 얻도록 확장하여 활용할 수 있다. 기존 프로그래머 플랫폼의 발전을 주도해 나가며 폭넓은 소프트웨어 시장에서 다양한 서비스와의 연계로 수익성과 비즈니스 모델을 늘릴 수 있다.

3 배경 기술

3.1 기술적 요구사항

- 웹 프론트&백엔드 개발 : **Ruby on Rails**
- 데이터 베이스 개발 : PostgreSQL

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

- 스마트 컨트랙트& 개발 프레임 워크 : 솔리디티, OpenZeplin, Truffle

3.2 현실적 제한 요소 및 그 해결 방안.

1. 이더리움 플랫폼 기반 Dapp이 지니는 제약 :

1)51% 공격

2017년 기준으로 Homestead단계에 있는 이더리움은 합의 알고리즘으로 POW(Proof of Work)인 ethash를 사용한다. 기존 비트코인의 합의 알고리즘의 경우 단순한 연산의 반복만으로 Work 가 가능하여 일반 PC가 아닌 마이닝을 위한 ASIC(주문형 반도체)를 제작하여 특정 소수가 채굴량을 독점할 위험이 존재한다. 이같이 ASIC남용을 통한 하드웨어 경쟁이 심해지면 특정 집단이 채굴량의 51% 이상을 차지 할 경우 블록체인의 조작이 가능해지는 51% 공격이 발생 할 수 있으므로 ethash알고리즘은 이같은 합의가 중앙화될 수 있는 문제점을 해결하고자 ASIC을 제작할 수 없도록 Memory 연산을 늘리되, 검증은 쉽게 할 수 있도록 하고, GPU연산에 친화적으로 설계하였다.

2)확장성(Scalability)

최근 대형 ICO들로 인하여 순간적으로 많은 트랜잭션이 몰리며 블록체인에 많은 지연이 발생하여 이더리움의 확장성(scalability) 문제가 중요한 화두로 올라왔다.

2. 법제도적 근거부족

스마트 계약은 법적 강제성이 없고 알고리즘에 의한 계약으로 계약 불이행 시 피해 보상에 대해 법적인 보호를 받기 힘들다. 현행 법제도 상 블록체인 기술의 법적 문제 발생 가능성과 사고 발생 시 책임 소재가 불명확한 현안이 존재한다. 분산 장부인 블록체인의 도입 및 활용은 다양한 법적 문제의 발생 가능성을 내재하고 있으며 원인 규명이 어려운 문제의 경우, 책임소재가 불분명 개인정보보호법 등 현행법은 중앙 집중 관리체계에 초점을 두고 있어 탈중앙화에 본질을 둔 블록체인 기술과 상충하며 법률에서 데이터 보유 기간이 규정된 경우, 거래 기록의 삭제가 사실상 불가능한 블록체인의 특성과 충돌된다.

해결방안

1. 자체 플랫폼 개발

POS 알고리즘인 Casper를 적용해, POW 방식에 비해 상대적으로 속도 향상이 있을 수 있도록 새롭게 자체 플랫폼을 개발한다. 이를 위해 하나의 커다란 블록체인을 유지하는 것이 아닌 여러 조각으로 나누어 저장하여 병렬적으로 처리될 수 있도록 한다(샤딩 기법). 그리고 블록체인을 트리 형태로 무한히 확장하여 각 하위 블록체인에 특정 목적의 트랜잭션과 데이터를 담고 Root체인에는 최소한의 검증용 데이터만 저장함 블록체인 공간 효율성과 처리 속도를 크게 높일 수 있게 한다.

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

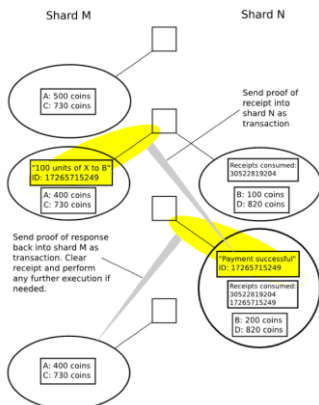


Figure 5 샤딩 기법

2. 관련 법 제도 정비

블록체인 내 거래에 대한 법적 보호 장치 마련 및 블록 체인 산업 활성화를 위한 관련 법제도 개선이 필요하다. 개인 간 직접 거래 시 계약이나 결제 불이행 등 문제 발생 시 법적인 보호 조치를 마련하고 발생 가능한 문제에 대한 기존 법제도 검토 및 개정 필요하다.

4 개발 일정 및 자원 관리

4.1 개발 일정

항목	세부내용	1 월	2 월	3 월	4 월	5 월	6 월	비고
요구사항분석	요구 분석							
	SRS 작성							
관련분야연구	주요 기술 연구							
	관련 시스템 분석							
설계	시스템 기획 및 설계							
구현 테스트	코딩 및 모듈 테스트							

4.2 일정별 주요 산출물

마일스톤	개요	시작일	종료일
계획서 발표	산출물 : 1. 프로젝트 수행 계획서 2. 프로젝트 기능 일람표	2018-02-28	2018-03-08
설계 완료	시스템 설계 완료 산출물 : 1. 시스템 설계 사양서	2018-02-01	2018-03-17

 국민대학교 컴퓨터공학부 캡스톤 디자인 I	계획서		
	프로젝트 명	블록체인을 활용한 QnA DAPP 서비스 개발	
	팀 명	K-Block	
	Confidential Restricted	Version 2.0	2018-04-12

1 차 중간 보고	스마트 컨트랙트 작성 및 배포 웹 프론트 개발 웹 UI 개선 산출물 : 1. 프로젝트 1 차 중간 보고서 2. 프로젝트 진도 점검표 3. 1 차분 구현 소스 코드 4. 보상 정책 정의서 5. 웹 화면 UI 기획서	2018-03-21	2018-04-10
2 차 중간 보고	DAPP 개발완료 산출물 : 1. 프로젝트 2 차 중간 보고서 2. 프로젝트 진도 점검표 3. 테스트 시나리오표 4. 2 차분 구현 소스 코드 5. 게임화 적용 시나리오 문서	2018-04-13	2018-05-15
구현 완료	시스템 구현 완료 산출물: 1. 완성본 소스 코드	2018-03-15	2018-05-10
테스트	시스템 통합 테스트 Application A / B 테스트 테스트넷 상 코인 송금 성능 측정 산출물: 테스트넷 성능 측정표	2018-04-30	2018-05-24
최종 보고서	전시 및 최종 보고 산출물: 프로젝트 최종 보고서	2018-05-29	2018-05-29