



| 계획서                     |                  |             |
|-------------------------|------------------|-------------|
| 프로젝트 명                  | 블록체인 기반의 알트코인 개발 |             |
| 팀 명                     | K-Block          |             |
| Confidential Restricted | Version 1.0      | 2018-MAR-09 |

**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 "XXXXXX"의 팀원들의 자산입니다. 국민대학교 컴퓨터공학부 및 팀 "XXXXXX"의 팀원들의 서면 허락없이 사용되거나, 재가공 될 수 없습니다.


# 캡스톤 디자인 I

## 종합설계 프로젝트

|        |                  |
|--------|------------------|
| 프로젝트 명 | 블록체인 기반의 알트코인 개발 |
| 팀 명    | K-Block          |
| 문서 제목  | 수행계획서            |

|         |            |
|---------|------------|
| Version | 1.0        |
| Date    | 2018-03-09 |


|    |     |
|----|-----|
| 이름 | 김명수 |
|----|-----|

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

## 문서 정보 / 수정 내역

| 수정날짜       | 대표수정<br>자 | Revision | 추가/수정 항<br>목 | 내<br>용           |
|------------|-----------|----------|--------------|------------------|
| 2018-03-03 | 김명수       | 0.1      | 최초 작성        | 개요 및 배경 기술 일부 작성 |
| 2018-03-07 | 김명수       | 0.9      | 내용 수정        | 개발 일정 및 자원관리 조정  |
| 2018-03-09 | 김명수       | 1.0      | 내용 수정        | 최종 수정            |
|            |           |          |              |                  |
|            |           |          |              |                  |
|            |           |          |              |                  |
|            |           |          |              |                  |

본 양식은 컴퓨터공학부 캡스톤 디자인 I 과목(산학분반)의 프로젝트 수행 계획서 작성을 위한 기본 양식입니다. 문서의 필수 항목을 제시하는 것이니 폰트, 문단 구조 등의 디자인 부분은 자유롭게 설정하기 바랍니다. 양식 내에 붉은 색으로 기술한 부분은 지우고 작성하기 바랍니다.

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

## 목 차

|       |                           |                        |
|-------|---------------------------|------------------------|
| 1     | 개요 .....                  | 4                      |
| 1.1   | 프로젝트 개요 .....             | 4                      |
| 1.2   | 추진 배경 및 필요성 .....         | 4                      |
| 2     | 개발 목표 및 내용 .....          | 7                      |
| 2.1   | 목표 .....                  | 7                      |
| 2.2   | 연구/개발 내용 .....            | 7                      |
| 2.3   | 개발 결과 .....               | 9                      |
| 2.3.1 | 결과물 목록 및 상세 사양 .....      | 오류! 책갈피가 정의되어 있지 않습니다. |
| 2.3.2 | 시스템 기능 및 구조 .....         | 오류! 책갈피가 정의되어 있지 않습니다. |
| 2.4   | 기대효과 및 활용방안 .....         | 9                      |
| 3     | 배경 기술 .....               | 10                     |
| 3.1   | 기술적 요구사항 .....            | 10                     |
| 3.2   | 현실적 제한 요소 및 그 해결 방안 ..... | 12                     |
| 3.2.1 | 하드웨어 .....                | 오류! 책갈피가 정의되어 있지 않습니다. |
| 3.2.2 | 소프트웨어 .....               | 오류! 책갈피가 정의되어 있지 않습니다. |
| 3.2.3 | 기타 .....                  | 오류! 책갈피가 정의되어 있지 않습니다. |
| 4     | 프로젝트 팀 구성 및 역할 분담 .....   | 오류! 책갈피가 정의되어 있지 않습니다. |
| 5     | 프로젝트 비용 .....             | 오류! 책갈피가 정의되어 있지 않습니다. |
| 6     | 개발 일정 및 자원 관리 .....       | 15                     |
| 6.1   | 개발 일정 .....               | 15                     |
| 6.2   | 일정별 주요 산출물 .....          | 15                     |
| 6.3   | 인력자원 투입계획 .....           | 오류! 책갈피가 정의되어 있지 않습니다. |
| 6.4   | 비 인적자원 투입계획 .....         | 오류! 책갈피가 정의되어 있지 않습니다. |
| 7     | 참고 문헌 .....               | 오류! 책갈피가 정의되어 있지 않습니다. |

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

# 1 개요 (최대 1 page)

## 1.1 프로젝트 개요

지금까지의 기업과 기업의 계약은 굉장히 비용이 많이 드는 일이었습니다. 어느 한쪽에서 데이터 조작을 안 할 것이라고 믿거나 서로의 서버를 제한적으로 접근 및 감시할 수 있는 소프트웨어를 만드는 것이 필수적인 일이었기 때문입니다. 또한 보통 급조된 연계 소프트웨어를 사용하기 때문에 보안상 허점도 많이 보였습니다. 하지만 블록체인이 등장하면서 분산 원장 개념과 트랜잭션들을 체인처럼 엮는 기술이 도입되면서 비잔티움 장군 문제와 보안 문제가 상당부분 개선되었습니다. 하지만 대부분의 기업에서 아직 기술적인 문제로 블록체인 도입을 고려하고 있는 상태입니다. 이에 저희 팀은 블록체인을 기반으로 한 기업간 거래를 쉽게 해주는 알트코인과 스마트 컨트랙트를 서버별 언어로 래핑하여 간단한 api로 제공함으로써 기업간의 거래에서 쉽게 사용할 수 있는 플랫폼을 개발하고자 합니다. 현재 가장 인기가 높은 블록체인 플랫폼인 이더리움을 기반으로 접근성에 초점을 맞춰 저희만의 새로운 알트코인을 개발 후 그랩에서 서비스중인 해시코드와 새로 런칭할 재능마켓에 적용할 예정입니다.

## 1.2 추진 배경 및 필요성

그랩에서 이미 서비스중인 해시코드는 개발자를 위한 커뮤니티 사이트입니다. 적절한 보상 방안을 찾던 도중 스팀잇의 예시를 보면서 가상화폐 지급 시스템을 결정하게 되었습니다. 새로 런칭할 재능마켓의 경우에는 저희가 임의로 선정한 주제입니다. 이 주제에 대한 추진 배경 및 필요성은 아래와 같습니다.

### 1.2.1 국내 아웃소싱 시장의 현황 및 문제점

### 1.2.2 기 개발된 유사 시스템 분석

### 1.2.3 개발할 시스템의 필요성

#### 1.2.1

#### <아웃소싱 하는 이유>

대부분 IT조직에게 외주 IT업체 관리는 새로운 업무가 아니다. IT 부서의 운영비용이 매년 20~30% 정도 증가하며 기술의 변화속도가 너무나 급속하게 이루어지기 때문에 일반적으로 대규모의 투자 자금이 소요되고, IT기술을 적시에 받아들이고 유지하는 데는 자체 부서로는 어려움이 많아 외부 업체에 위탁함으로써 위험을 감소시키고 있습니다.

#### <아웃소싱 확대의 배경>

국내외 IT기업의 성장과 함께 아웃소싱이 확대됐으며, 인소싱과 아웃소싱을 어떻게 결정할 것인가에 대한 고민과 논의가 활발하게 이뤄지고 있습니다. 신규 IT장비를 여러 대 관리감독해야 하고,

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

전문 기술 업체나 처음 계약을 맺는 공급업체들까지도 관리하며, 높아진 성능 기대를 충족하면서도 비용을 거의 늘리지 않거나 때에 따라 비용을 절감할 것을 요구 받기 때문입니다. 그 결과 많은 사람이 고군분투하고 있습니다.

### 1.2.2

#### <아웃소싱 문제점>

국내에서도 아웃소싱 전문업체들이 많이 생겨났으며, 프로젝트의 범위, 카테고리 등 다른 방식으로 재능마켓 플랫폼이 활성화 되고 있습니다.



[그림 1] 크몽 거래 수수료

그러나 중개플랫폼 1위인 '크몽'의 경우 아웃소싱 업체 및 프리랜서에게 거래금액 100만원 초과시 5%, 50만원 이하는 20%의 높은 중개수수료가 책정되어 있습니다.

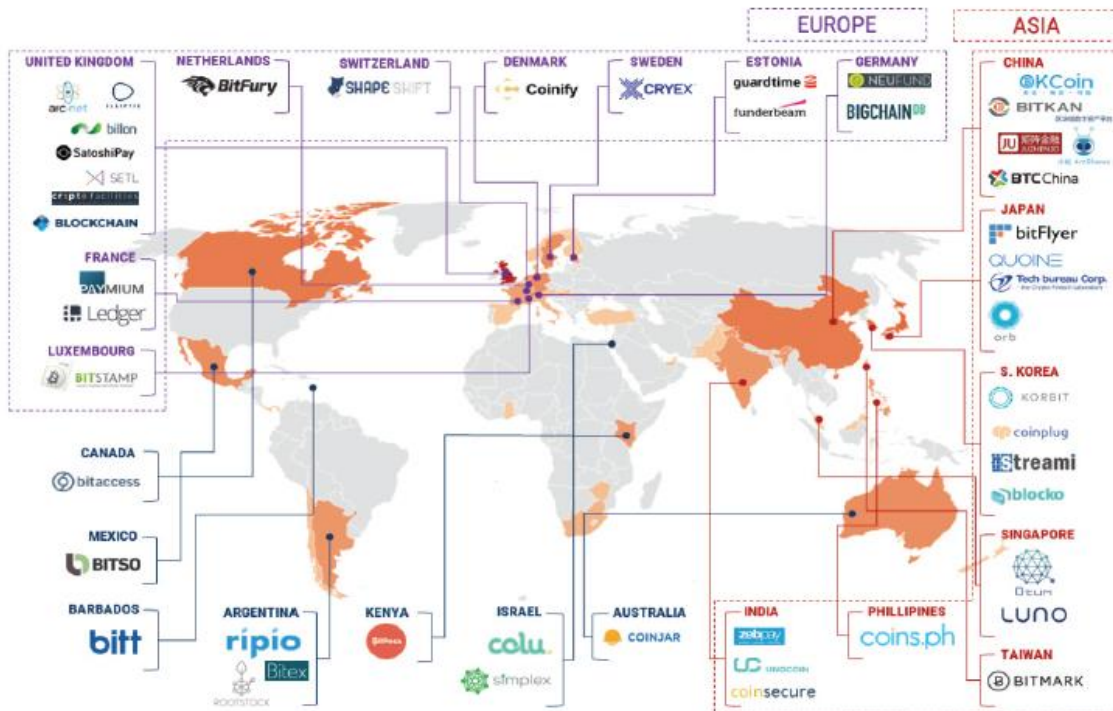
클라이언트 관점에서 보았을 때 아웃소싱 업체의 포트폴리오 및 타업체와 비교를 하였음에도 개발 지연과 낮은 완성도로 만족하기 어려운 경우가 많습니다.

타 재능마켓사이트에서도 거래를 성사 시키기 위해 메신저 답변으로 미팅 & 컨택의 시간이 오래 걸리는 경우가 많으며, 기능문의나 비용견적만 받고 의뢰를 하지않는 경우도 많습니다. 그리고 과제, 도박사이트, 티켓자동예약 등 터무니 없는 의뢰도 많으며, 하청에 하청 의뢰도 상당합니다.

3)클라이언트 관점에서 보았을 때 아웃소싱 업체의 포트폴리오 및 타업체와 비교를 하였음에도 개발 지연과 낮은 완성도로 만족하기 어려운 경우가 많습니다.

### 1.2.3 개발할 시스템의 필요성

| 계획서                     |                  |             |
|-------------------------|------------------|-------------|
| 프로젝트 명                  | 블록체인 기반의 알트코인 개발 |             |
| 팀 명                     | K-Block          |             |
| Confidential Restricted | Version 1.0      | 2018-MAR-09 |



자료: CB Insights(2017.3.6.), 「Global Ledger: Mapping Bitcoin&Blockchain Startups Around The World」

[그림 2] 글로벌 비트코인, 블록체인 서비스 기업현황

미래 신기술로 각광받고 있는 '블록체인(Blockchain)'은 금융권을 중심으로 기존의 비즈니스 프로세스를 바꿀 새로운 패러다임으로 등장하였으며, 2016년 초 세계경제포럼(World Economic Forum, WEF)에서 제4차 산업혁명 시대를 이끌 핵심 기술 중 하나로 블록체인이 선정되었습니다. 또한 2025년까지 전 세계 GDP의 10%가 블록체인 기반 기술에서 발생할 것으로 전망하였습니다.

블록체인은 퍼블릭 혹은 프라이빗 네트워크에서 일어나는 거래정보가 암호화되어 해당 네트워크 구성원 간 공유되는 디지털 원장(ledger)를 의미하며, 각 네트워크 구성원에게 분산되어 새로운 거래가 발생할 때마다 구성원들의 동의를 통해 해당 거래를 인증합니다.

-중앙 집중화된 시스템에 의존하지 않고 P2P(peer-to-peer) 네트워크 방식 기반이기 때문에 거래 중개자(intermediary)의 필요성을 없앴으로써 거래의 효율성과 투명성을 높이고 적은 비용으로 보다 빠르고 안전한 거래가 가능합니다.

-블록체인에 기반한 거래 정보는 임의로 변경이 불가능하기 때문에 거래의 신뢰성이 높아 지고 정보 추적이 용이합니다. 분산원장 기술(distributed ledger technology)을 바탕으로 동일한 거래 장부가 네트워크 참여자들 모두에게 개방되고 새로운 정보가 실시간으로 동시에 업데이트 됩니다. 하나의 거래정보를 임의로 변경하려면 수많은 컴퓨터를 동시에 해킹해야 하는데 이는 사실상 불가능합니다.

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

## 2 개발 목표 및 내용 (최대 3page)

### 2.1 목표

이더리움 기반의 플랫폼과 가상화폐를 이용해 스마트 계약 기능을 제공함으로써, 기존의 높은 수수료를 절감하고 보안성, 안정성을 보장받고 신뢰할 수 있는 플랫폼을 개발하려 합니다.

아래와 같은 블록체인의 특징들을 반영하여 분산원장 및 보안 개념을 살려 개발합니다.

| 특징               | 설명  |
|------------------|---|
| <b>원장 무결성 확보</b> | 분산 장부의 무결성을 확보하기 위해 모든 참여자가 같은 원장을 저장하고 변경이 있을 때마다 수정하며 새로운 블록의 추가가 확정 되면 되돌릴 수 없는 비가역성을 가짐                 |
| <b>참여자간 합의</b>   | 참여자들 간 거래 내역에 대한 정당성을 검증하여 증명하는 합의 과정이 필요, 공개 블록체인과 개인 블록체인은 서로 다른 합의 알고리즘으로 수행될 수 있음                       |
| <b>화폐 발행 정책</b>  | 화폐 발행 기능을 가진 블록체인에서 필요한 과정(ex, 비트코인)으로 다수의 참여자가 합의된 문제를 풀고 이를 증명하면 새로운 화폐를 발행하여 소유할 수 있도록 허가                |
| <b>거래 장부 동기화</b> | 공개 블록체인에서 필요한 과정으로 참여자들이 서로 다른 원장을 가지고 있는 경우(Fork), 블록이 많이 형성된 것을 진본으로 간주 하고 이를 기준으로 거래를 다시 조정하는 동기화 과정이 필요 |

### 2.2 연구/개발 내용


본 프로젝트의 수행의 내용을 구체적으로 기술한다.

목표를 세분화하여 세부 목표를 정하고 그에 따른 결과물을 제시한다.

연구/개발 방법을 기술한다. 연구/개발 방법은 단계별 수행 방법을 기술한다.

#### - 사이트맵 작성

현재 재능마켓의 경우 사이트맵이 확정 되었지만 해시코드의 경우 기업과 논의가 끝나지 않아 재능마켓의 사이트맵만 작성하겠습니다.

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

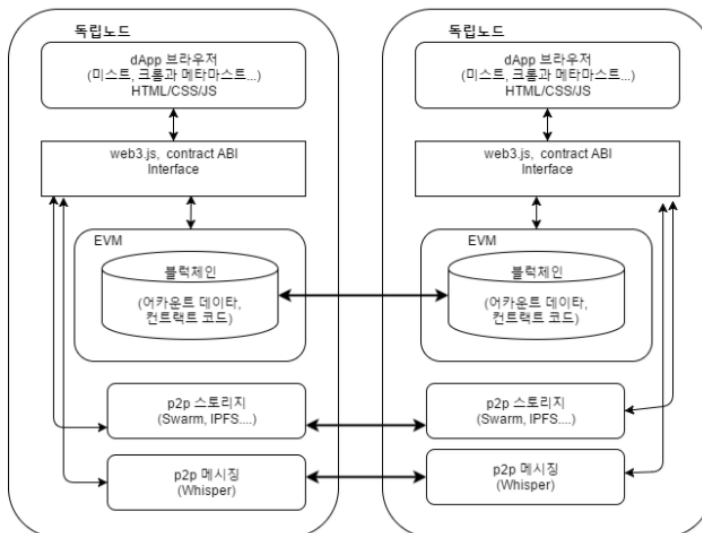
## BLOCKCHAIN-KOREA 메뉴 구조도

### \* 카테고리

| 재능구매(클라이언트) | 재능판매(외주업체) | 고객센터      | 마이페이지                                 |
|-------------|------------|-----------|---------------------------------------|
| 재능 구매 등록    | 재능 판매 등록   | Q&A       | 개인정보<br>-회원정보수정<br>-회원탈퇴<br>-포트폴리오 수정 |
| 진행 중인 재능    | 진행 중인 재능   | <u>알림</u> | 거래내역<br>-판매정보<br>-구매정보                |
| 종료된 재능      | 종료된 재능     | 이용방법      | 나의 지갑<br>-토큰 환전                       |
|             |            |           |                                       |
|             |            |           |                                       |
|             |            |           |                                       |

- 사이트 기능정의서(테스트 시나리오)
- 웹프론트
- 웹백엔드
- 웹 아키텍처 설계

dApp 웹 아키텍처



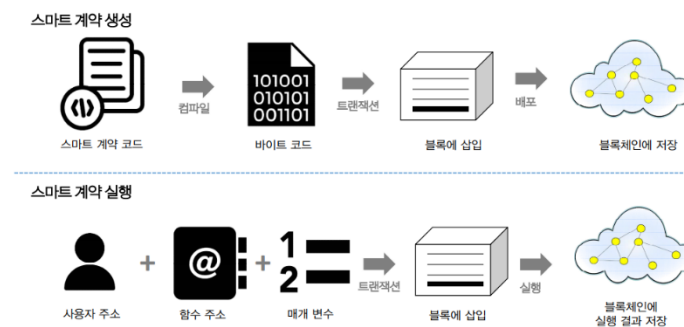
- 서버&DB개발
- 스마트 계약 규칙 작성



|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |



이더리움 DApp의 생성, 실행 과정



## 2.3 개발 결과

저희는 스택오버플로우와 스팀잇이 합해진 것 같은 결과를 해시코드에 반영할 것입니다. 또한 수수료를 극도로 낮춘 크몽 같은 사이트를 재능마켓으로 런칭할 계획입니다.



아직 시스템 설계 합의가 끝나지 않았기 때문에 자세한 내용은 기술할 수 없습니다.


## 2.4 기대효과 및 활용방안

저희는 재능마켓 Dapp을 먼저 만들어 실험한 후 해시코드에 보완된 내용으로 코드를 작성하여 한국 최고의 개발자 QnA 커뮤니티를 만들고자합니다.

<기대효과>

-중개자가 사라짐 : Application에서 가상화폐로 약 1%대의 수수료로 거래가 가능하다. 기존의 높은 중개 수수료비용을 절감한다.

-중개자가 사라져도 높은 보안성 제공 : 블록체인을 적용함으로써 분산 원장으로 변조가 불가능하

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

다.

-Win-Win 전략 실현 : 계약 참여자 간의 후기 평가로 높은 신뢰성을 제공하며, 클라이언트에겐 낮은 비용의 비해 높은 요구 사항에 제약을 걸고 실력 있는 아웃소싱 업체에게 의뢰를 맡길 수 있다.

#### <활용방안>

-제2의 페이스북으로 불리고 있는 스팀잇을 벤치마킹하여 Pow 방식에서 Pos방식으로 전환하여 '재능파워' 개념을 만들어본다. **재능파워 개념 추가 설명**

-토큰ICO를 통해 투자를 받아 서비스 공급자는 보다 나은 서비스 활성화를 추구한다.

그랩도 프로그래머 채용에 관심이 많으며, 본 프로젝트의 프로토 타입을 이용하여 개발한다면 무료인 **그랩의 사이트에 수익성과 비즈니스 모델을 확장** 시킬 수 있다.

-사이트 지적재산권을 활용한 M&A : 2015년 사람인HR에서 재능마켓 Big3 업체인 '오투잡'을 인수하였다. 사람인은 국내 대표 취업포털로 성장한 사람인의 운영 노하우를 접목, 다각도로 영역을 확장하며 재능마켓 플랫폼의 발전을 주도해 나가며 정규 취업 시장뿐만 아니라 폭넓은 영역에서 매칭 기술을 활용한 고도화된 서비스를 제공해 전 연령, 전 계층에 걸쳐 모든 취업 서비스를 제공하는 생계 플랫폼을 계획할 수 있을 것이다.

## 3 배경 기술 (최대 1page)

### 3.1 기술적 요구사항

**프로젝트의 결과물의 기술적인 요구 사항을 모두 나열한다.**

**프로젝트를 개발하는 데 필요한 개발 환경과, 프로젝트 결과물을 확인할 수 있는 환경을 나누어 기술한다.**

**개발 환경은 개발에 필요한 운영체제 환경, 컴파일 환경, 개발 언어, 언어의 문법적 요구사항을 기술한다.**

**프로젝트 결과물 확인 환경은 동작시킬 수 있는 운영체제 환경, 미리 설치되어 있어야 하는 소프트웨어 및 라이브러리를 기술한다. 서버 환경의 경우 서버의 구성 방법에 대해서 기술해야 한다.**

-웹사이트 프론트 : vue.js, bootstrap

-웹사이트 백엔드 : node.js

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

- 서버 및 DB설계
- 스마트 컨트랙트& 사용자 인터페이스 개발 : 솔리디티
- 이외의 툴 : Zeplin, Truffle



[블록의 개념] 이 사진은 어디다 쓸까나

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

## 3.2 현실적 제한 요소 및 그 해결 방안

프로젝트를 수행하기 이전에 시스템 개발시 발생할 가능성이 있는 제한 요소를 미리 예측하여 나열한다. 또한 그 제한 요소를 피해갈 수 있는 해결 방안에 대해서도 나열한다. 예를 들어, GNU 라이선스가 있는 소프트웨어 라이브러리를 사용하는 경우에 이를 사용하는 소프트웨어의 소스를 공개하여야 한다. 만약 개발할 시스템이 상용화 제품일 경우에는 문제가 발생할 수 있다. 이를 어떻게 해결할 것인가? 하는 점 등이다. 또한 시스템의 성능(속도, 처리할 수 있는 데이터의 양 등등)이 어느 정도 이상이 되어야 한다든지 혹은 안정성을 어느 정도 확보를 하여야 하는 점도 현실적 제한 요소가 될 수 있다. 이를 하드웨어 측면 혹은 소프트웨어적인 측면에 대하여 기술한다.

이러한 현실적 제한요소를 팀원들과 토의한 내용과 지도 교수님과 토의한 내용은 반드시 회의록에 남기도록 한다.

### 3.2.1 이더리움 플랫폼 기반 DAPP의 한계

=이더리움 플랫폼의 한계 :

1)51% 공격

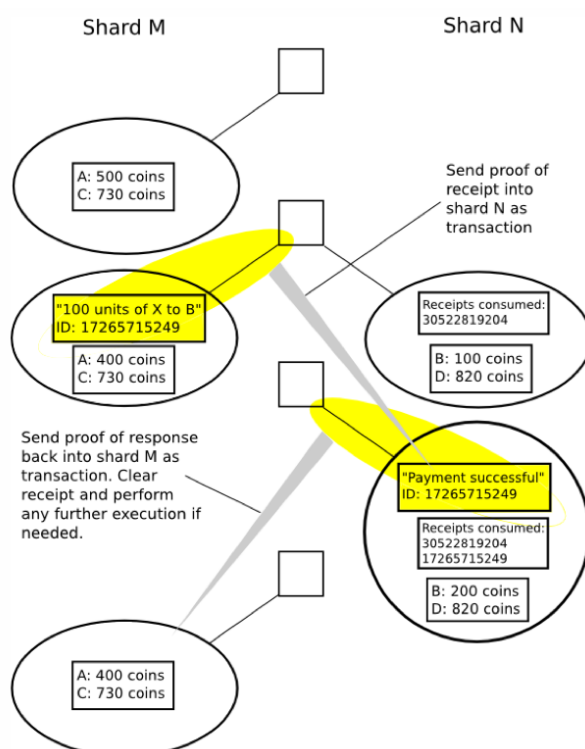
현재 2017년 기준으로 Homestead단계에 있는 이더리움은 합의 알고리즘으로 POW(Proof of Work)인 ethash를 사용한다. 기존 비트코인의 합의 알고리즘의 경우 단순한 연산의 반복만으로 Work 가 가능하여 일반 PC가 아닌 마이닝을 위한 ASIC(주문형 반도체)를 제작하여 특정 소수가 채굴량을 독점할 위험이 존재한다. 이같이 ASIC남용을 통한 하드웨어 경쟁이 심해지면 특정 집단이 채굴량의 51% 이상을 차지 할 경우 블록체인의 조작이 가능해지는 51% 공격이 발생 할 수 있으므로 ethash알고리즘은 이같은 합의가 중앙화될 수 있는 문제점을 해결하고자 ASIC을 제작할 수 없도록 Memory 연산을 늘리되, 검증은 쉽게 할 수 있도록 하고, GPU연산에 친화적으로 설계 하였다. 구체적인 방식으로는 매 30,000 블록마다 DAG라는 완전 다른값의 1GB 의 데이터를 생성 하여 Work에 사용하도록 하여 많은 Memory 용량과 IO가 요구된다. 하지만 이같은 POW 형식의 합의 알고리즘은 전기 등 많은 에너지와 컴퓨팅 자원을 사용하게 됨으로써 이더리움은 최종 세레니티(Serenity)단계에서는 Casper라 불리는 POS(Proof of Stake) 방식으로 전향하게 된다. 하지만 합의 알고리즘의 변경은 기존 마이닝 풀 생태계에 혼란을 줄 수 있으므로, 기존 POW 방식에 일정 주기로 한 번씩 POS 를 섞는 hybrid 방식을 거쳐 점진적으로 POS로 넘어갈 계획을 가지고 있다.

2)확장성(Scalability)

최근 대형 ICO들로 인하여 순간적으로 많은 트랜잭션이 몰리며 블록체인에 많은 지연이 발생하여 이더리움의 확장성(scalability) 문제가 중요한 화두로 올라왔다. 앞서 다른 POS 알고리즘인 Casper 가 적용되더라도, POW에 비해 상대적으로 속도 향상이 있을 수 있지만, 확장성을 초점으로 이더리움 팀 내에서 공식적으로 연구되고 있는 방안으로는 [샤딩\(Sharding\)](#)과 [플라즈마\(Plasma\)](#) 가 있다. 샤딩이란 하나의 커다란 블록체인을 유지하는 것이 아닌 여러 조각(Shard)으로




나누어 저장하여 병렬적으로 처리될 수 있도록 하는 방안이다. 간단하게 예를 들었을 때 0x1 로 시작하는 지갑 주소에 대한 Shard, 0x2 로 시작하는 주소에 대한 Shard와 같은 방식으로 나뉘었을 때 같은 Shard내에 있는 지갑끼리의 트랜잭션은 해당 Shard안에서만 처리될 수 있어서 병렬처리로 인해 속도 향상을 가져올 수 있다. 하지만 다른 Shard에 존재하는 지갑끼리의 트랜잭션을 처리하는 Cross shard communication 문제와 하나의 Shard의 대다수를 특정인이 차지해 버리는 Single shard takeover attacks 등 안정적으로 적용하기에는 해결할 문제가 많아 지속적으로 연구, 개발이 진행 중에 있다.



플라즈마(Plasma) 는 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 된다. 또한 Map-Reduce[3] 방식으로 각 서브 체인들에 대해 분산 병렬 연산을 통해 목적에 따라 빠른 결과를 얻을 수 있게 한다. 아직 Paper 만 나와 있는 상황에서, 실질적인 코드가 공개되진 않았지만 추후 개발 및 공개가 된다면 플라즈마를 이용하여 빠르고 확장성이 중요한 블록체인 시스템 시스템을 구현할 수 있게 될 예정이며 최근 omisego 또한 플라즈마를 통해 VISA를 뛰어넘는 TPS(Transaction per sec) 를 구현할 계획을 밝혀 주목을 받은 바 있다.

(기술적 제약) 블록체인 기술에 대한 잠재적인 위험 요소나 검증 미흡으로 인한 우려로 각 분야의 블록체인 도입 및 활용에 제약이 존재 - 블록체인의 논의가 활발한 금융 분야도 블록체인의 기술적 한계와 문제점\*에 따른 블록체인 도입에 대한 거부감과 불신 존재 \* 처리 속도, 확장성, 기

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

존 시스템의 대체 비용, 기술의 미성숙성, 잘못 인식된 보안성, 안전성 보장 등 - 실제 산업 전반에 활용하기 위해서는 기술적 한계와 문제점을 극복하여 기술의 안정성을 확보해야 하는 현안이 남아 있다.

(법제도적 근거부족) 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.

### 3.2.2 해결방안

-이더리움을 따르지 않고 자체적으로 플랫폼을 개발한다. EVM 환경에서 돌아가기 때문에 이더리움을 완전히 거스르긴 어렵다.

-분야별 컨소시엄 구축에 기여 :


-관련 법 제도 정비 : 블록체인 내 거래에 대한 법적 보호 장치 마련 및 블록 체인 산업 활성화를 위한 관련 법제도 개선 필요

- 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.

\* 중앙 집중 관리체계 중심의 개인정보보호법, 전자금융거래법, 전자문서 및 전자 거래 기본법, 거래 기록 삭제가 필요한 신용정보법 등 기존 법제도의 개선

- 블록체인 활용 및 활성화를 위한 법률을 추가할 필요성이 대두된다.

데이터 관리에 보안성이 강화되어야 하거나 투명성과 신뢰성이 요구되는 영역에 적용이 필요

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

## 4 개발 일정 및 자원 관리

### 4.1 개발 일정

개발 일정을 계획한다.

| 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 설계      |     |     |     |     |     |     |    |
| 구현     | 코딩 및 모듈 테스트 |     |     |     |     |     |     |    |
| 테스트    | 시스템 테스트     |     |     |     |     |     |     |    |

### 4.2 일정별 주요 산출물

일정별로 어떤 결과물을 도출할 지 상세하게 작성한다. 그래프의 형태로 작성하여도 좋다.

| 마일스톤      | 개요   | 시작일        | 종료일        |
|-----------|--|------------|------------|
| 계획서 발표    | 개발 환경 완성 (GCC 설치, 기본 응용 작성 및 테스트 완료)<br><b>산출물 :</b><br>1. 프로젝트 수행 계획서<br>2. 프로젝트 기능 일람표       | 2018-02-28 | 2018-03-08 |
| 설계 완료     | 시스템 설계 완료<br><b>산출물 :</b><br>1. 시스템 설계 사양서   | 2018-03-09 | 2018-03-14 |
| 1 차 중간 보고 | 기능 xxx ~ yyy 구현 완료<br><b>산출물 :</b><br>1. 프로젝트 1 차 중간 보고서<br>2. 프로젝트 진도 점검표<br>3. 1 차분 구현 소스 코드 | 2012-03-21 |            |
| 구현 완료     | 시스템 구현 완료<br><b>산출물:</b>   |            |            |
| 테스트       | 시스템 통합 테스트<br><b>산출물:</b>  |            |            |
| 최종 보고서    | 최종 보고<br><b>산출물:</b>   |            |            |

|   |                         |                  |             |
|---|-------------------------|------------------|-------------|
|  <b>국민대학교</b><br><b>컴퓨터공학부</b><br><b>캡스톤 디자인 I</b> | <b>계획서</b>              |                  |             |
|   | <b>프로젝트 명</b>           | 블록체인 기반의 알트코인 개발 |             |
|   | <b>팀 명</b>              | K-Block          |             |
|   | Confidential Restricted | Version 1.0      | 2018-MAR-09 |

## 5. 참고문헌

- 금융위원회, 블록체인기술 금융분야 도입방안을 위한 연구, 2016
- 박현제(IITP), 블록체인 TechBiz 컨퍼런 '17 블록체인R&D 추진현황, 2017
- 임명환, 블록체인 기술의 활용과 전망, 2016
- 소프트웨어정책연구소, 블록체인 기술의 산업적 사회적 활용전망, 2017