

2016/11/01

캡스톤 설계 최종 발표

P2P 기반 보안 메신저

컴퓨터소프트웨어공학과

201321283 고현서

201321286 김미옥

201321300 명소희

201321319 이민영

지도교수 : 이종혁 교수님

목차

1. 개요
2. 관련 기술 소개
3. 기존 서비스와 비교
4. 특징
5. Network Topology
6. Software Architecture
7. 프로젝트 구현 방식
8. 프로젝트 기능
9. 시연영상
10. 기대효과
11. Q&A

개요

• 배경

- 중앙 집중 형 서버를 이용한 메신저나 거래시스템에서 발생하는 문제
 - 데이터 해킹, 위조 문제
 - 서버 과부하에 따르는 트래픽 발생

카톡보다 안전하다는 메신저 '텔레그램'도 해킹 당했다

강동철 기자

입력 : 2016.08.03 23:07

한때 한국에서 '메신저 망명(亡命)'이란 신조어를 만들어냈던 독일의 모바일 메신저인 '텔레그램(telegram)'이 이란에서 해킹 공격을 받아 대규모 피해를 입었다고 로이터가 3일(현지 시각) 보도했다.

로이터에 따르면 이번 해킹 사건은 이란 해커들이 저질렀고, 텔레그램 가입자 1500만명의 전화번호와 일부 이용자의 대화 내용이 유출됐다. 이란에선 2000만명이 텔레그램을 사용하는데 그중 75%에 달하는 이용자의 정보가 유출된 것이다.

애플 텔레그램은 메신저 대화 내용을 자사의 서버(대형컴퓨터)에 저장하지 않고 전달만 하는 방식이기 때문에 감청이나 해킹으로부터 안전하다고 알려졌다. 이에 2014년 국내 수사기관이 카카오톡 대화 내용을 감청한다는 소식이 전해지자 100만명이 넘는 카카오톡 이용자가 텔레그램으로 이동하는 '메신저 망명' 사태가 벌어지기도 했다. 그런데 텔레그램이 더 이상 해킹의 안전지대가 아니라는 사실이 드러난 것이다.



카카오톡 장애, 메시지 '폭주' 추정

송수신량 폭주로 서버 다운 추정...국민안전처 홈페이지도 먹통

2016년 09월 12일 오후 22:16

🗨️ 의견달기

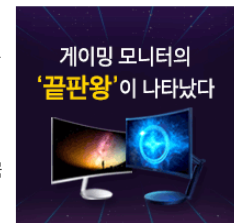
[성상훈기자] '국민 메신저' 카카오톡이 대규모 서비스 장애가 발생한 가운데 지진여파로 인한 메시지 송수신 폭주로 서버가 다운된 것이 직접적인 원인으로 추정되고 있다.

카카오톡은 12일 오후 8시께부터 대규모 서비스 장애가 발생했으며 오후 9시 22분부터 메시지 송수신 일부 기능이 복구됐다.

IT 전문가들은 지진 여파로 인해 메시지 송수신량이 순간적으로 폭주하면서 서버가 다운된 것이 직접적인 원인으로 추정하고 있다.

이날 오후 7시 44분 경북 경주에서 진도 5.1의 지진이 발생하자 경북 지역 위주로 메시지 송수신량이 폭주했다는 것.

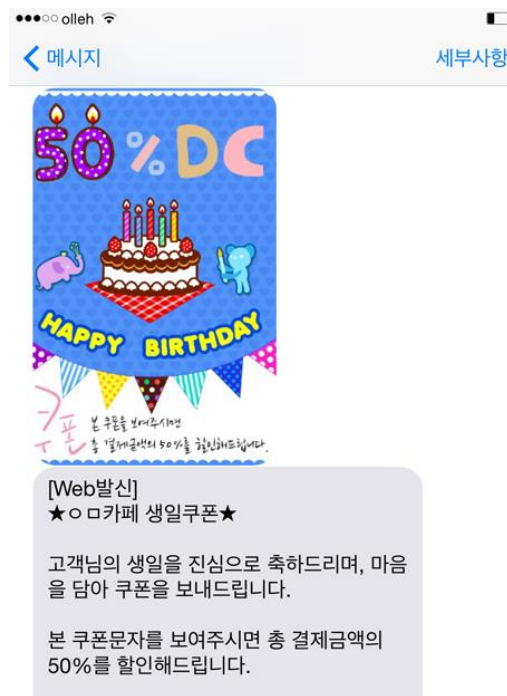
이때문에 부산 LG CNS 데이터센터안에 있는 카카오톡 서버가 다운됐고 이후 전국의 카카오톡 메시지 전송이 타 지역의 서버로 몰리면서 전국 서버 전체가 다운됐다는 것이 전문가들의 분석이다.



개요

• 배경

- 기프트티콘과 같은 쿠폰을 한번에 모아서 관리하기 어려움
- 예시



개요

• 개발 목표

- 데이터 해킹, 위조 문제 / 서버 과부하에 따르는 트래픽 발생
 - 중앙서버 없이 사용자끼리 안전하게 메시지를 주고 받을 수 있는 커뮤니티 서비스 구현
- 기프티콘과 같은 쿠폰을 한번에 모아서 관리하기 어려움
 - 쿠폰내역 서비스 구현
 - 발급한 쿠폰을 한번에 관리가능
 - 거래를 마친 쿠폰을 선물할 때, 쿠폰에 대한 정보를 암호화하여 전송

관련 기술 소개

- **Ethereum**

- 블록체인을 기반으로 거래 기록 뿐만 아니라 계약서, SNS, email, 전자투표 등 다양한 금융 어플리케이션을 투명하게 운영할 수 있도록 확장성 제공
- C++, 자바, Python, GO 등 대부분의 주요 프로그래밍 언어를 지원하여 모든 형태의 거래를 프로그래밍 가능하게끔 설계



ethereum

관련 기술 소개

- **Whisper**

- Ethereum이 지원하는 기술 중 하나인 P2P 네트워크를 기반한 messaging 프로토콜
- topic-based : 해시 된 topic을 기반으로 하여 메시지를 송수신
- 메시지는 특정키(공개키)를 통해 디지털 서명과 암호화 할 수 있음



기존 서비스와 비교

• 기존 서비스와 비교표

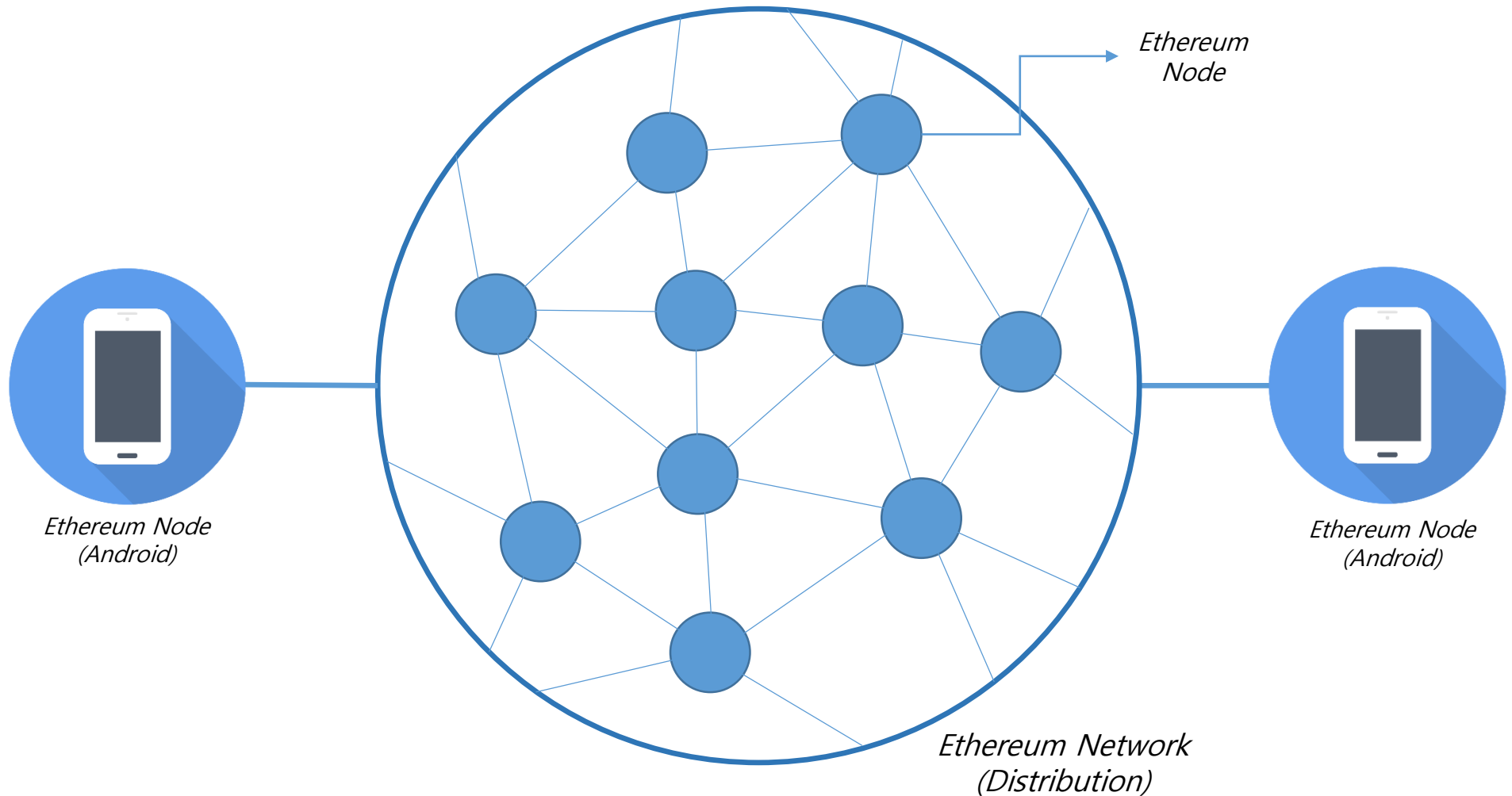
특징 \ 종류	Telegram	KakaoTalk	Bleep	Sock-Dark
P2P방식	X	X	O	O
종단간 암호화	O	수동(비밀채팅) 선택	O	O
모바일 쿠폰함	X	카카오 서비스만 가능	X	다양한 모바일 쿠폰 서비스 가능
단점	사용량 증가로 인한 서버 과부하로 실행 속도 느려짐	<ul style="list-style-type: none">- 서버에 저장된 대화 내용이 노출될 수 있음- 사용량 증가로 인한 서버 과부하로 실행속도 느려짐	알파버전이기 때문에 기능 부실	기술 발전단계라 보완 작업이 필요

특징

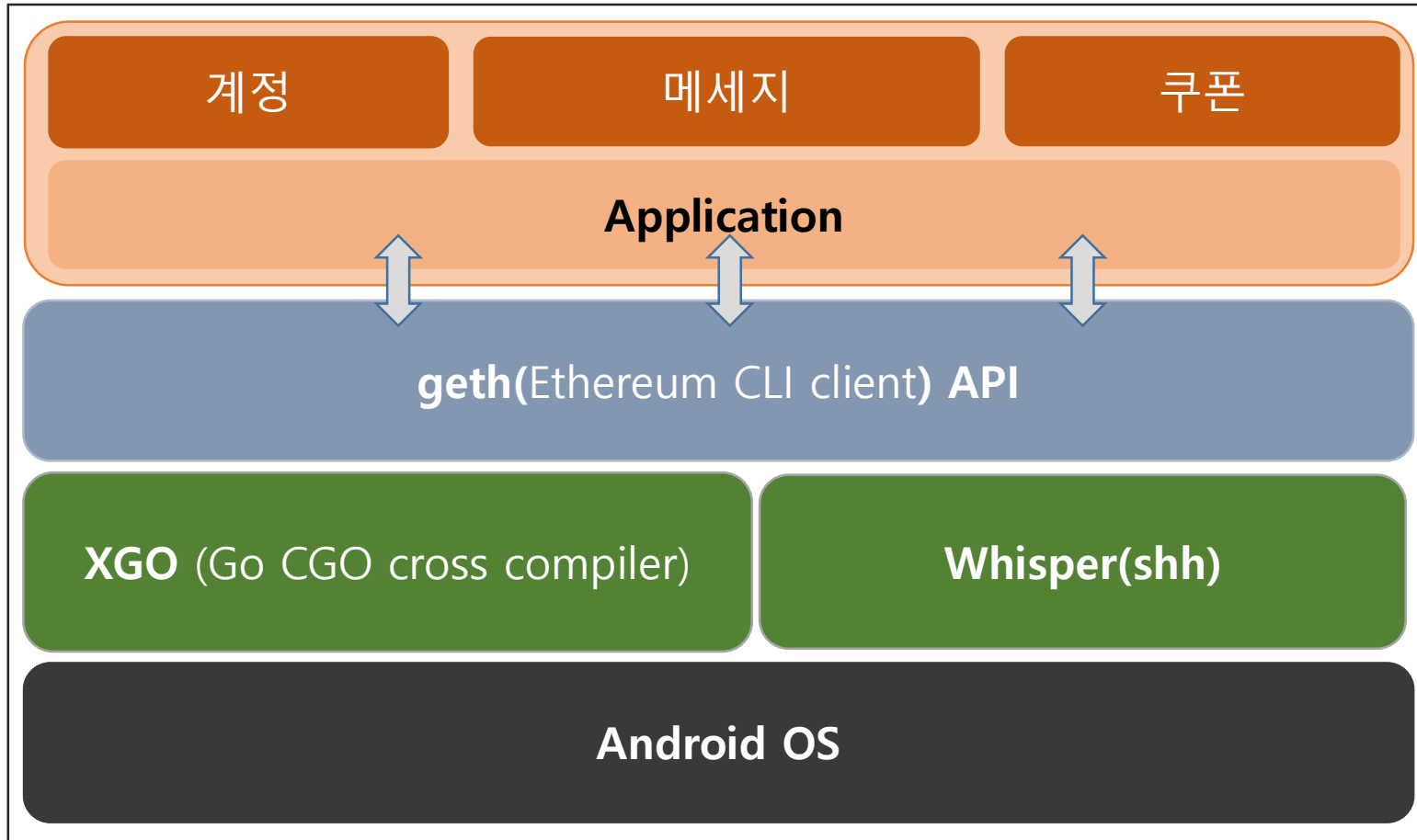
• Sock-Dark 장점과 단점

구분	특징
장점	모바일에서 발행된 쿠폰을 관리하기가 용이
	중앙 서버 없이 P2P네트워크를 이용하여 해킹에 대한 위험성을 최소화
	디지털 서명과 암호화를 통해 메시지를 보호
	서버에 의존적이지 않으므로 서버 과부하가 일어나지 않음
단점	국내에 본격적으로 도입되기 위해서는 기술적 보완이 필요함

Network Topology

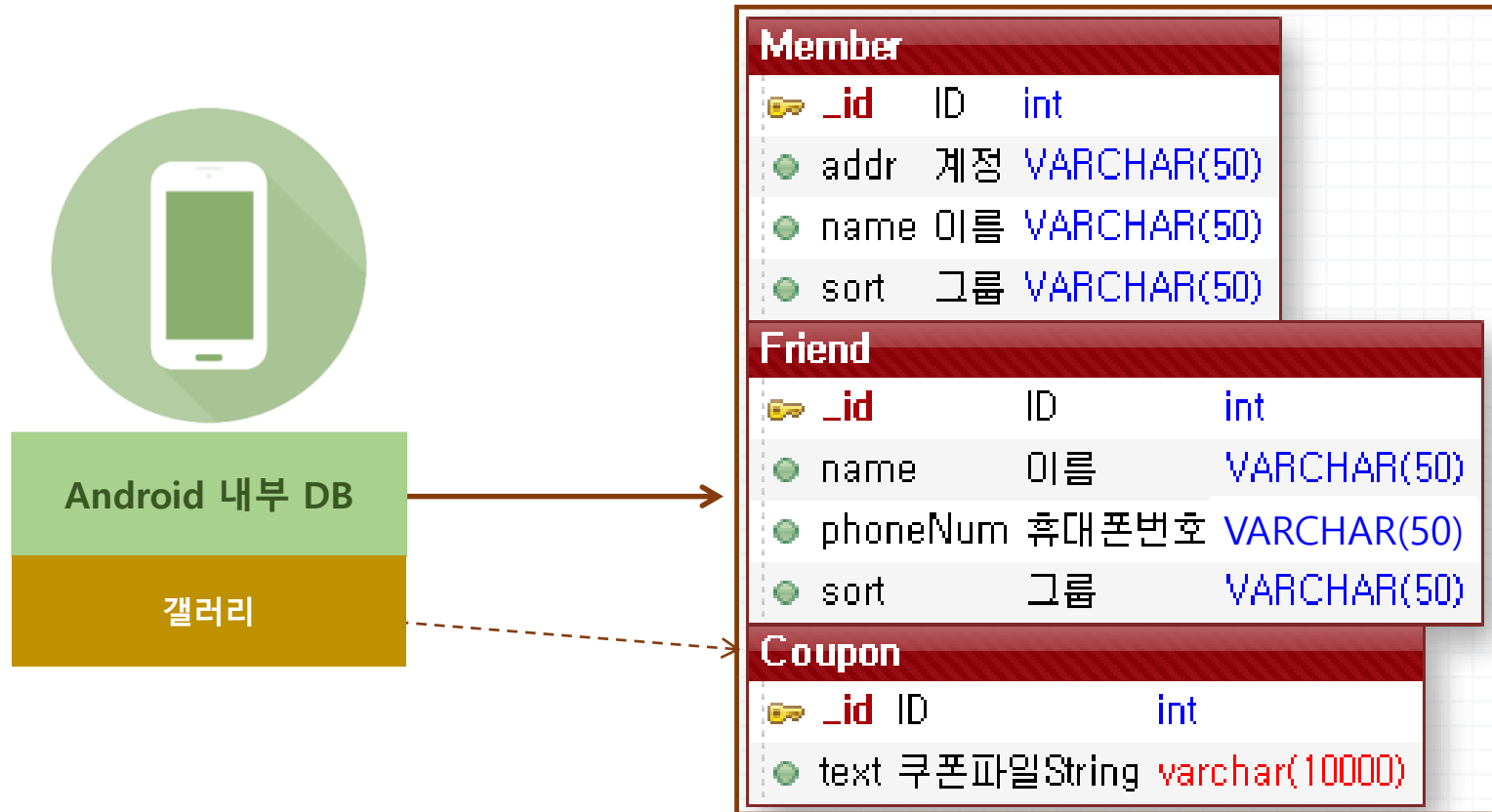


Software Architecture



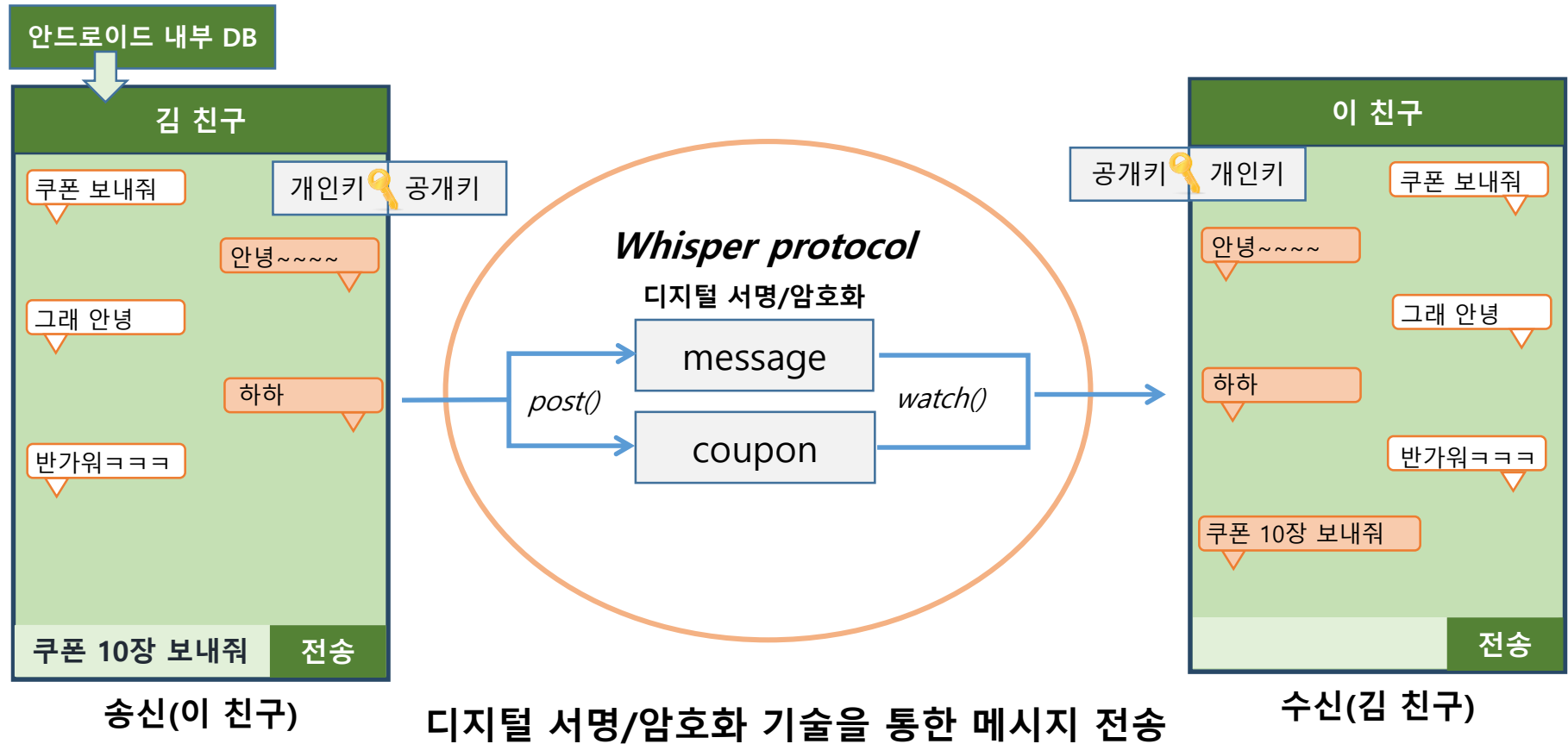
프로젝트 구현 방식

- 스마트 폰 Peer 구성(DB 중심)



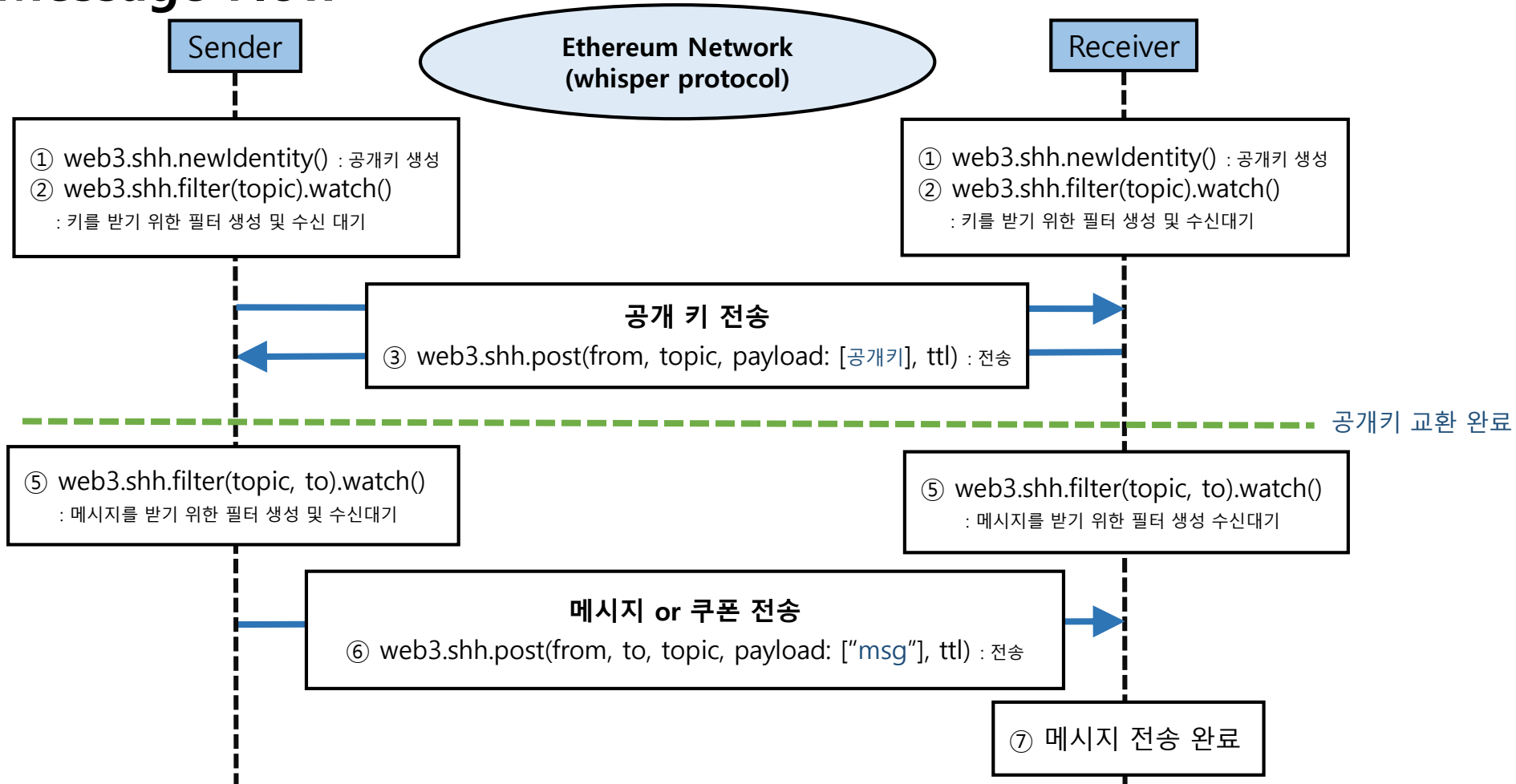
프로젝트 구현 방식

• 전송 방식



프로젝트 구현 방식

• Message Flow



프로젝트 구현 방식

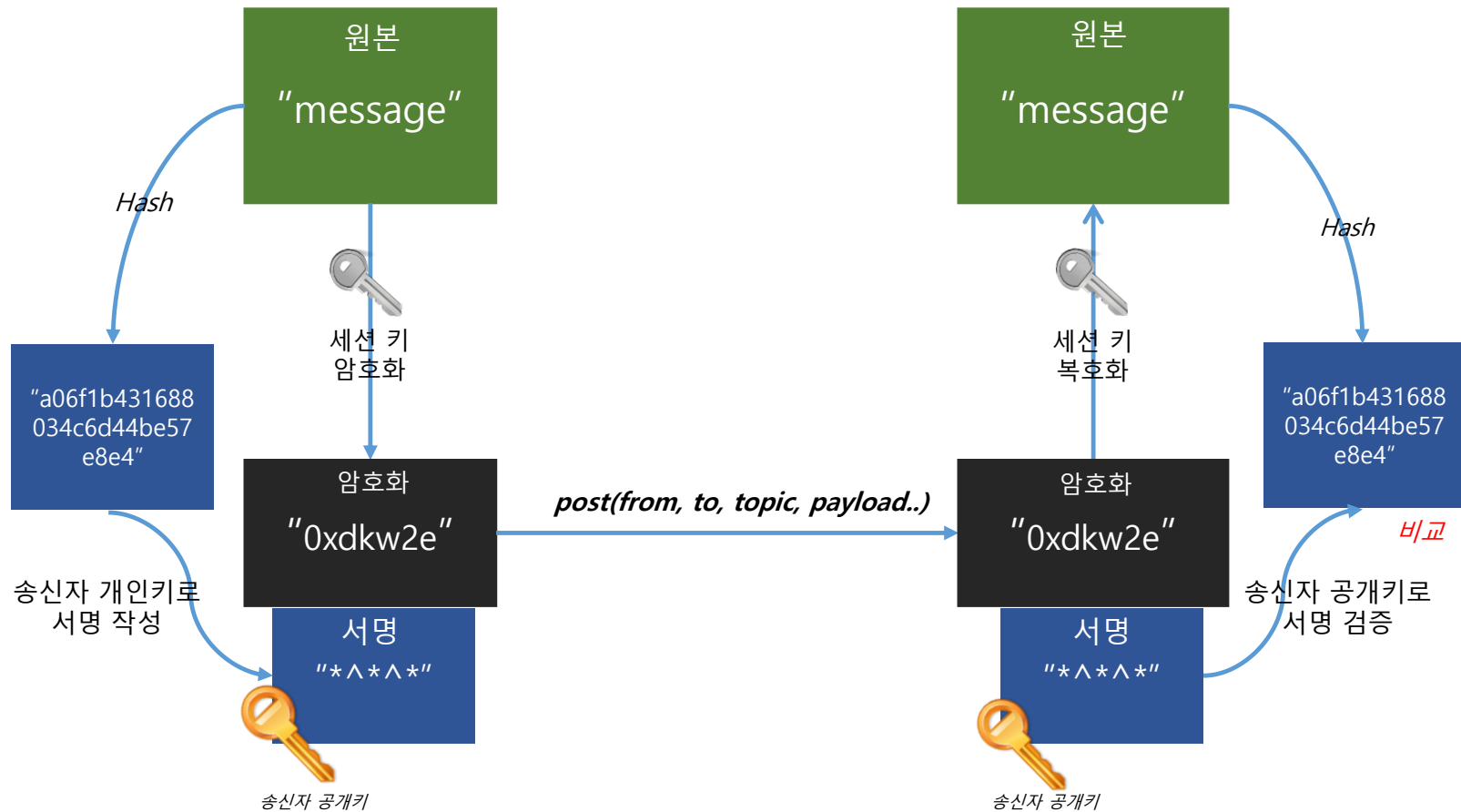
• 암호화 방식

- 메시지 / 쿠폰 송·수신 : 디지털 서명 + 암호화

기능	데이터 타입	암호화 방식 (디지털 서명)	암호화 방식 (암호화)
메시지 송·수신	text	<ul style="list-style-type: none">• 공개 키 암호화 방식<ol style="list-style-type: none">1. 개인 키로 암호화 한 후 공개키로 복호화2. 송신자가 개인키로 암호화된 서명과 송신자의 공개 키를 함께 전송• 데이터 무결성• 송·수신자 인증• 부인 방지	<ul style="list-style-type: none">• 대칭 키(세션 키) 암호화 방식<ol style="list-style-type: none">1. 메시지 전송 시 일부 정보를 공유하고 세션 키 생성2. 송신자와 수신자가 세션 키로 메시지를 송·수신• 메시지·쿠폰 데이터 보안(기밀성)
쿠폰 송·수신	file ↓ text		

프로젝트 구현 방식

• 암호화 방식



프로젝트 기능(개요)

• 상세 기능 설명

기능	상세기능		상세설명
계정	계정생성		시스템 사용을 위한 계정을 생성
	친구관리	그룹화	그룹을 지정하여 그룹별로 친구 관리
		등록	친구의 이름과 휴대폰 번호로 친구등록
		삭제	친구목록 삭제
메시지	메시지 송·수신		디지털서명과 암호화 기술을 이용한 메시지 송·수신
쿠폰	쿠폰관리	쿠폰등록	갤러리 내 제공된 쿠폰을 등록
		쿠폰삭제	등록된 쿠폰을 삭제
	쿠폰 송·수신		디지털서명과 암호화 기술을 이용한 쿠폰 송·수신

시연영상



기대 효과

- **편리성 향상** 발행된 쿠폰을 찾을 필요 없이 한 곳에 모아 확인 가능
- **보안강화** 서버에 따로 데이터가 저장되지 않아 데이터 유출을
방지를 할 수 있으며 디지털 서명과 암호화 과정을 통해
보안이 강화됨
- **비용 절감** 중앙 서버가 없으므로 관리비용이 줄어듦

Q & A

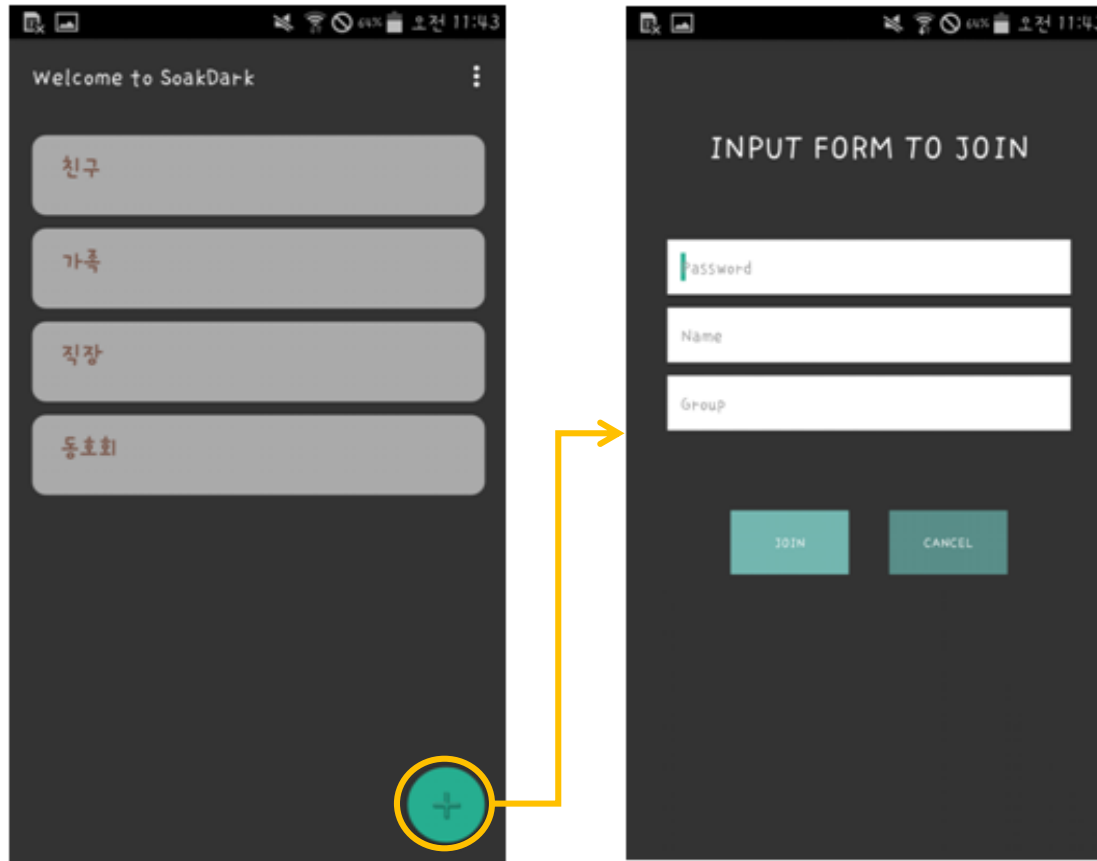
감사합니다

고현서 김미옥

명소희 이민영

프로젝트 기능(상세)

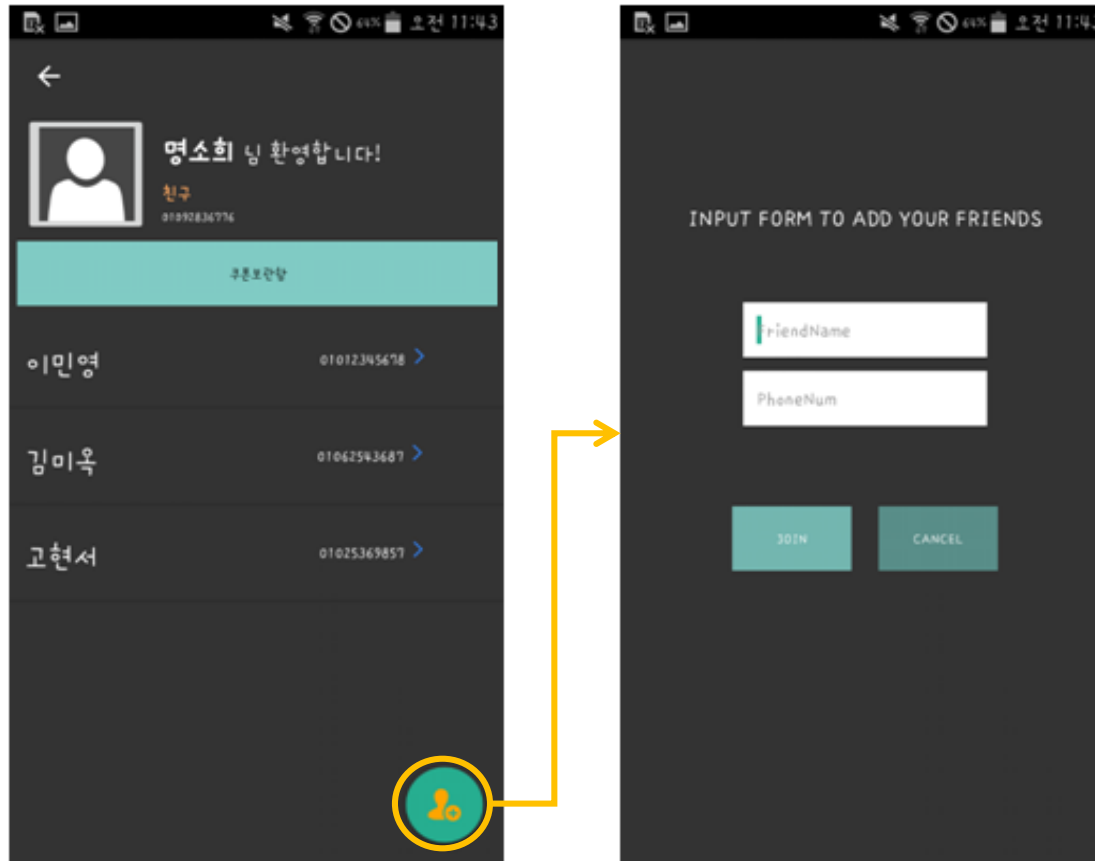
- 계정 관리 ① 계정 생성 (친구 그룹화)



- ① 추가 버튼 클릭
- ② geth 서비스에 연결
- ③ 정보 입력
- ④ 계정, 그룹 생성

프로젝트 기능(상세)

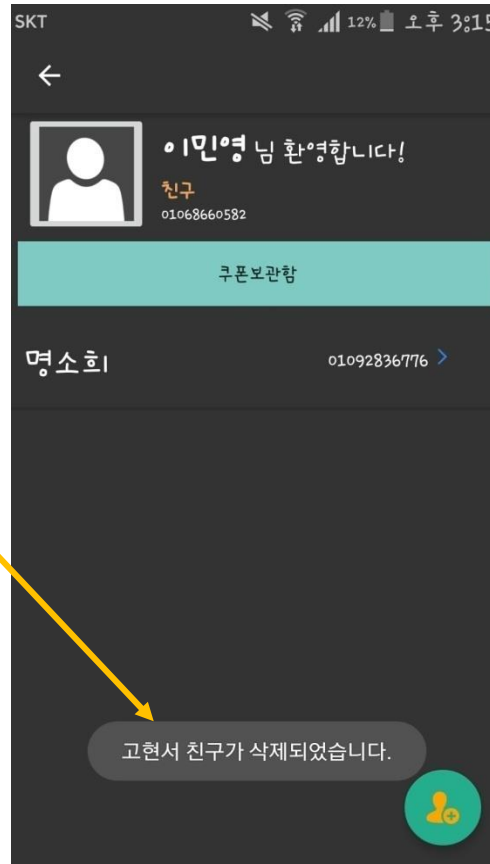
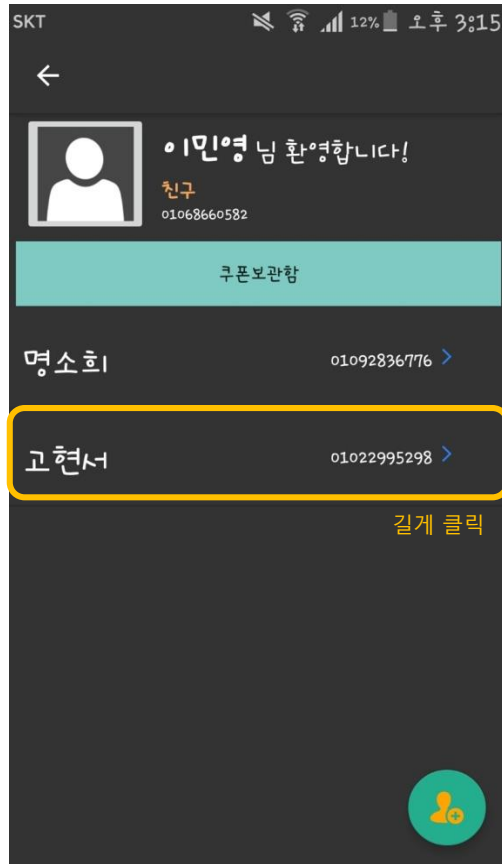
• 계정 관리 ② 친구 추가



- ① 친구 추가 클릭
- ② 친구의 정보 입력
- ③ JOIN 버튼 클릭
- ④ 추가완료

프로젝트 기능(상세)

• 계정 관리 ③ 친구 삭제



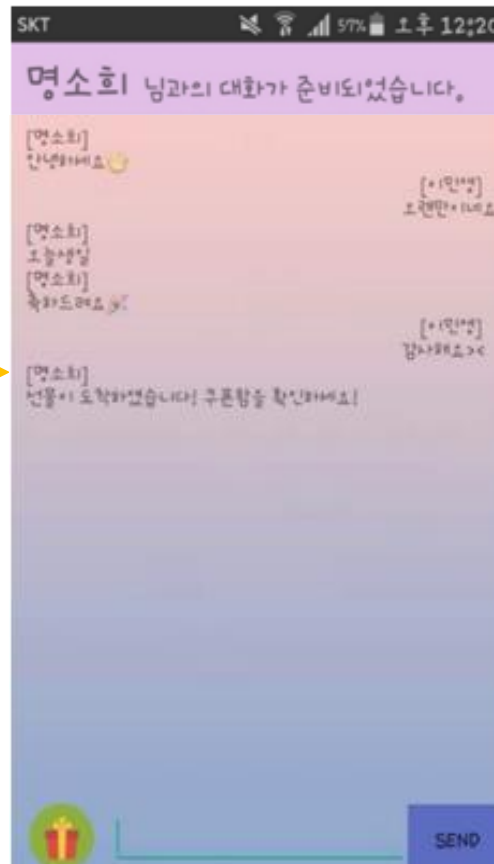
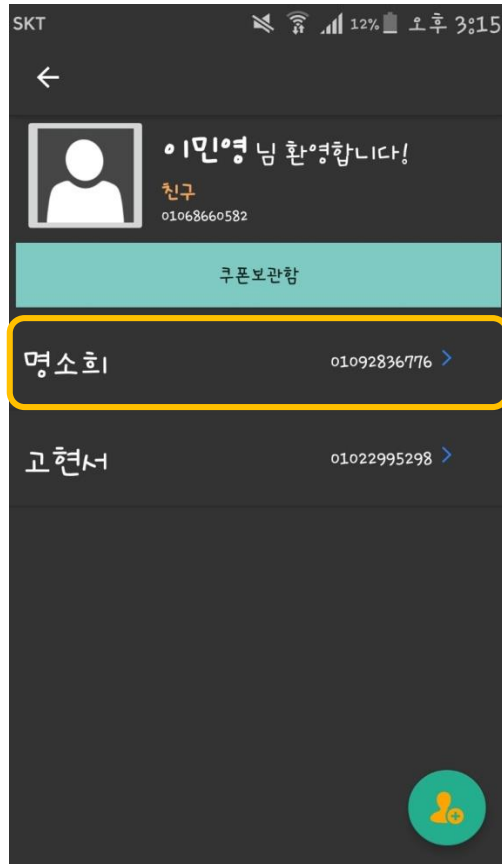
① 삭제할 친구를 선택

② 길게 클릭

③ 친구 삭제 완료

프로젝트 기능(상세)

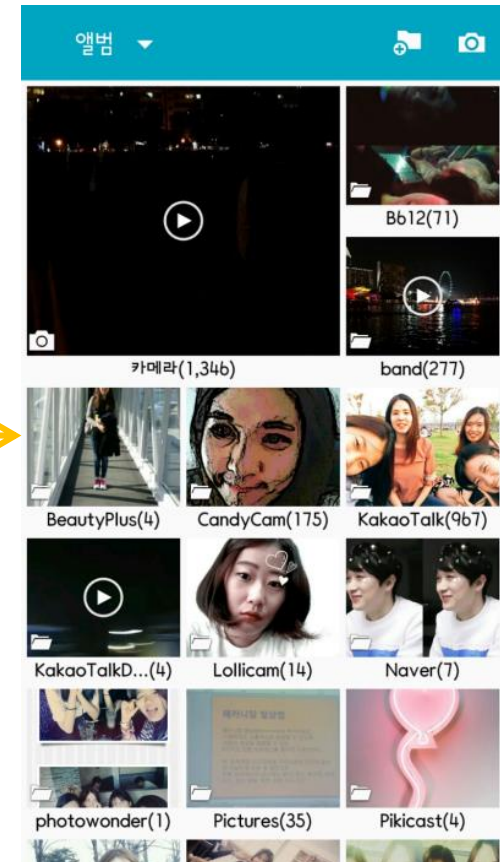
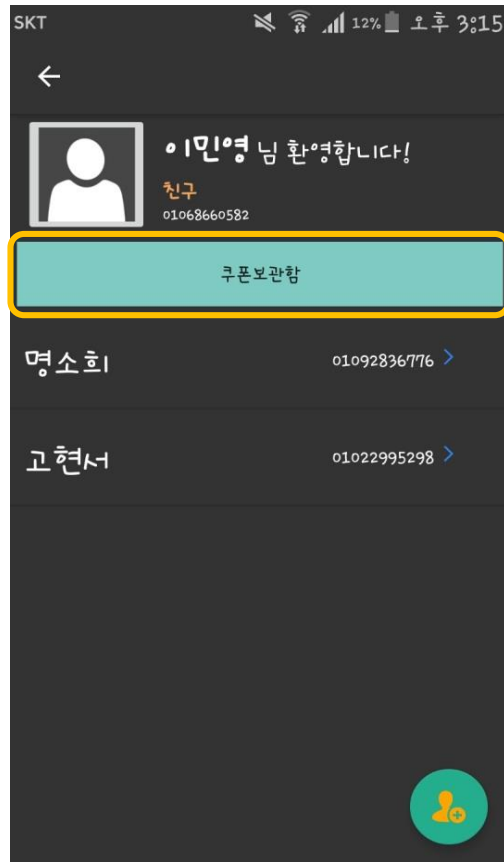
• 메시지 ① 메시지 송·수신



- ① 메시지를 받을 친구를 클릭
`web3.shh.newIdentity();` → 공개키 생성
- ② 입력된 메시지와 함께 생성된 세션 키로 암호화 한 뒤 서명과 함께 친구에게 전송됨
`web3.shh.post();` → 메시지 전송
- ③ 메시지를 받은 친구는 세션 키로 메시지를 확인
`web3.shh.filter.watch();` → 메시지 수신
- ④ 전송된 메시지는 디지털 서명의 과정(나의 공개키)을 통해 유효함을 입증

프로젝트 기능(상세)

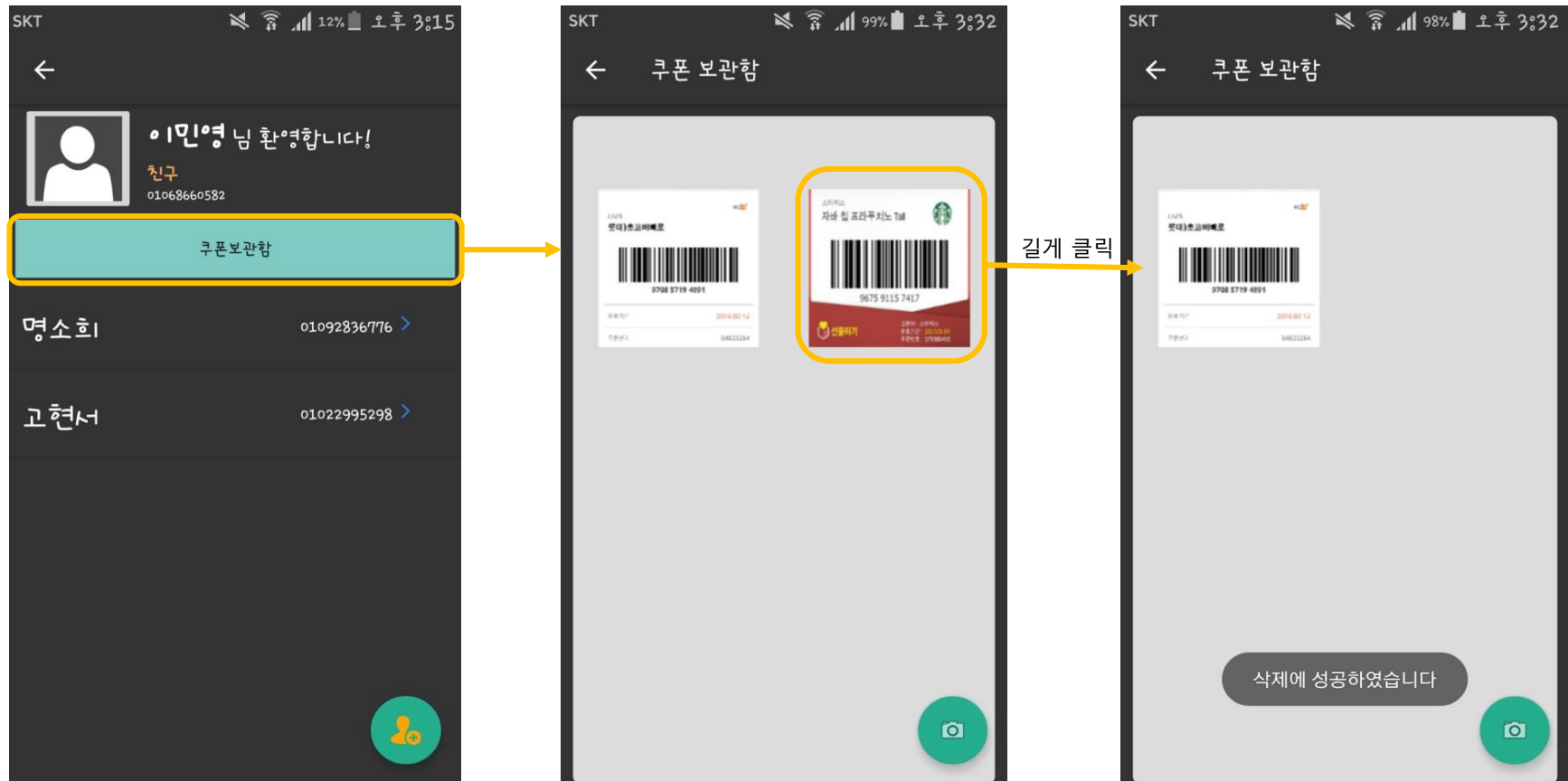
• 쿠폰 관리 ① 쿠폰 등록



갤러리에서
쿠폰 선택

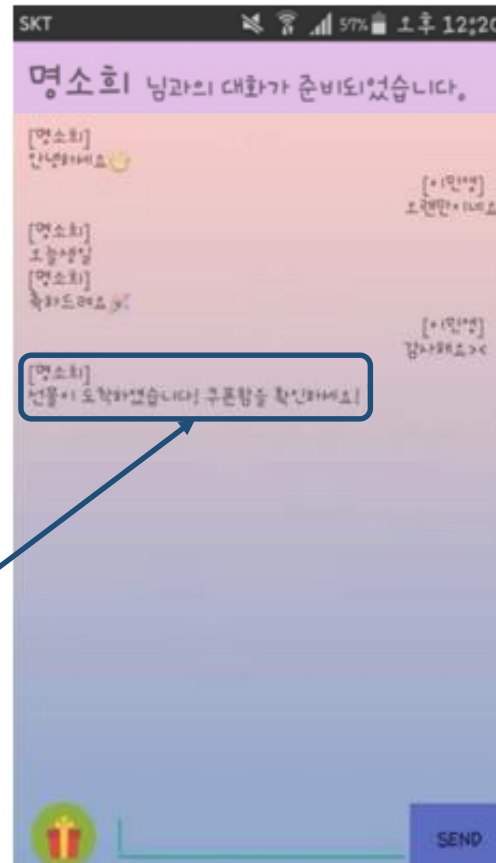
프로젝트 기능(상세)

• 쿠폰 관리 ② 쿠폰 삭제



시스템 기능(상세)

• 쿠폰 전송 ③ 쿠폰 송 · 수신



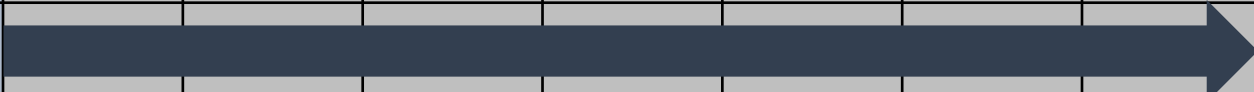


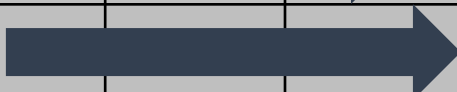



- ① 메시지를 받을 친구를 클릭하여 쿠폰 선택
- ② 선택된 쿠폰과 함께 생성된 세션 키로 암호화 한 뒤 서명과 함께 친구에게 전송됨
`web3.shh.post();` → 메시지 전송
- ③ 쿠폰을 받은 친구는 세션 키로 메시지를 확인
`web3.shh.filter.watch();` → 메시지 수신
- ④ 전송된 쿠폰은 디지털 서명의 과정 (나의 공개키)을 통해 유효함을 입증

개발 환경

- 개발환경
 - OS: Ubuntu 14.04
- 개발도구
 - Android Studio, Android SDK Platform(android 4.4)
- 개발언어
 - JAVA
- 시뮬레이터
 - 삼성 갤럭시S3(android 4.4.4), 갤럭시 S4(android 5.0.1)

개발 일정 및 역할 분담

		3월	4월	5월	6월	7월	8월	9월	10월
아이디어 선정									
기능 설정 및 API선정									
관련 연구 및 자료 수집									
개발 환경 구축 (명소희)									
프로젝트 구현	API 연동 (이민영)								
	DB 설계 (고현서)								
	쿠폰 기능 (김미옥)								
최종보완 및 테스트								