

**원금 손실 없는 로또 게임
(Dapp)**



INDEX

1

디파이란?

- 디파이(DeFi)란 무엇인가?
- 디파이 예치 시장 규모
- 디파이를 활용한 로또 게임

2

프로젝트 설명

- 스마트 컨트랙트
- 원금 손실 없는 로또 게임이란?

3

블록체인 시스템 구성

- 시스템 구성도
- 트랜잭션 데이터 흐름도
- 솔리디티 소스

4

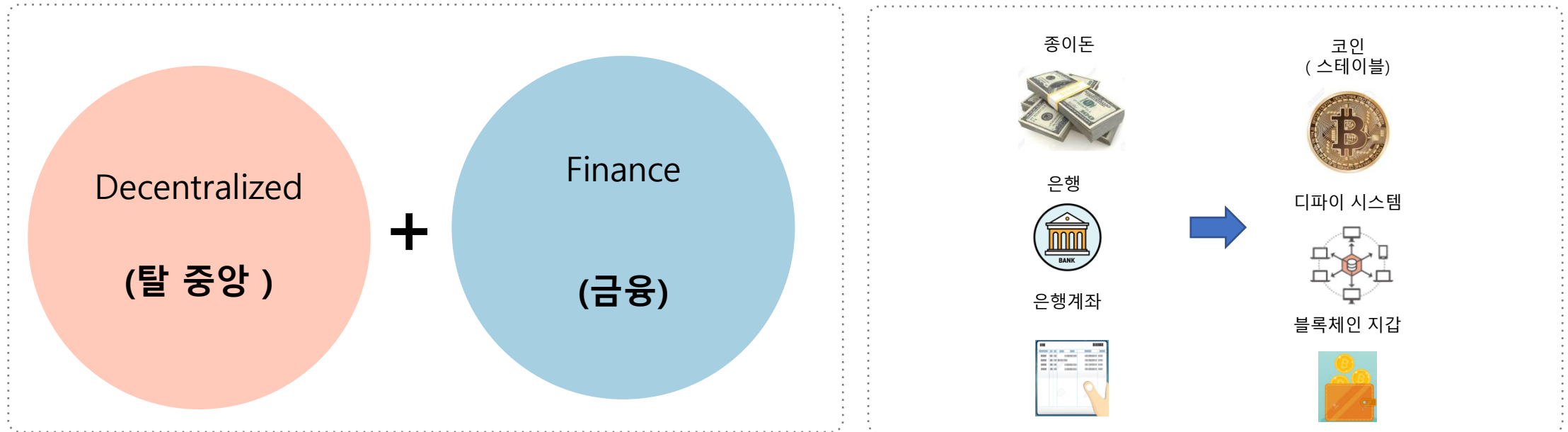
결과 화면



디파이(DeFi)란 무엇인가?

디파이(DeFi)란 탈중앙화 금융(Decentralized Finance)의 약자로서 즉 탈중앙화된 분산금융을 의미합니다.

- ① 전통금융 시스템에 의존하지 않고 중개자를 제거하여
- ② 이더리움과 같은 활성화된 퍼블릭 블록체인상에서
- ③ 완전히 탈중앙화된 독립적인 금융시스템을 말한다.

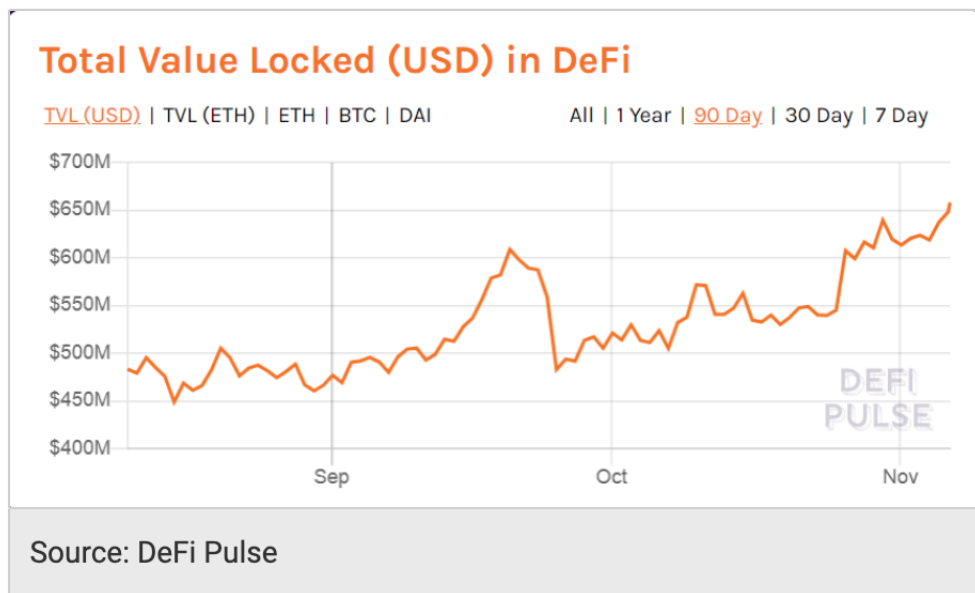




디파이 예치 시장 규모

DeFi 제품에 고정된 총 USD 가치(TVL)는 작성 시점에서 현재 6억 6,300만 달러로 8월 이후 37%의 인상적인 성장을 보이고 있다.

암호화 데이터 분석 회사인 [Defipulse](https://defipulse.com/) 에 따르면 DeFi 제품에 고정된 USD의 총 가치는 11월 6일에 6억 6,600만 달러에 달해 4개월 최고치를 기록했습니다. DeFi 시스템은 대출, 레버리지 및 파생 상품 거래와 디지털 플랫폼에서 전통적인 금융 자산의 이전을 제공하는 모두가 접근할 수 있고 분산된 안전한 플랫폼을 제공합니다.



DEFI PULSE	Name	Locked (USD) ▼	1 Day %
1.	Aave	\$16.12B	10.17%
2.	Maker	\$15.50B	4.62%
3.	Curve Finance	\$14.47B	-1.13%
4.	InstaDApp	\$12.20B	1.91%
5.	Compound	\$11.29B	4.15%
6.	Convex Finance	\$7.32B	-1.98%
7.	Uniswap	\$7.07B	3.26%
8.	yearn.finance	\$4.60B	1.63%
9.	SushiSwap	\$4.52B	1.79%
10.	Liquity	\$2.14B	-16.78%

<https://defipulse.com/>

<https://coingape.com/total-value-locked-ether-in-defi-products-reaches-an-all-time-high-at-3-5-million-eth/>



디파이를 활용한 로또 게임

탈 중앙화된 금융 + 로또

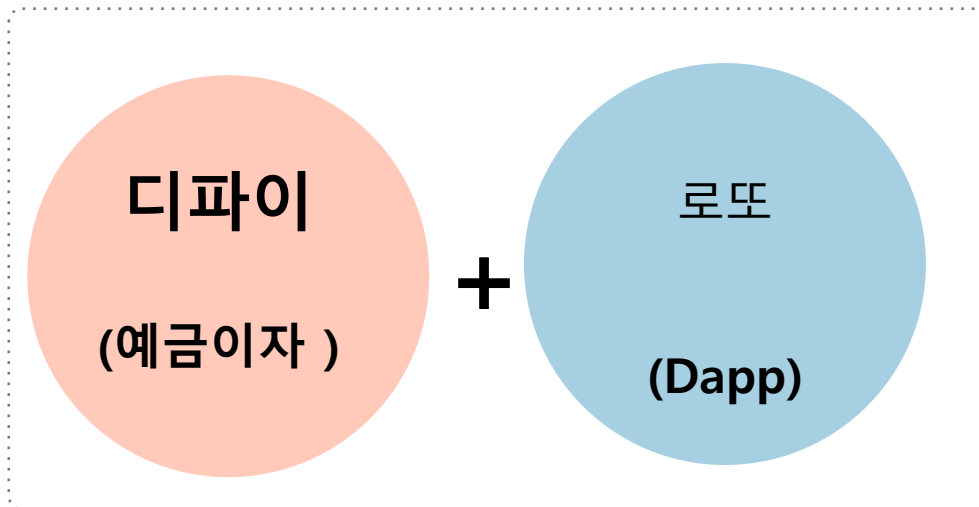
디파이를 활용한 복권

최근 거래소또는 메이커다오, 컴파운드와 같은 서비스에서 암호화폐를 예치하고 이자를 받는 서비스가 발전하고 있습니다.

이러한 디파이 서비스와 결합하여 서비스를 구현하고자 합니다.

* 1등 당첨자를 선별하는 과정도 이더리움 네트워크에서 제공하는 당첨자 선정 알고리즘을 씬으로써 공정성을 확보하려고 했습니다.

- 메이커다오 or 컴파운드 시스템에 블록체인 예치를 통한 이자 발생금액을 당첨금으로 지급합니다.
- 디파이 서비스를 활용하여 원금은 보장하는 무손실 로또 게임을 구성합니다.



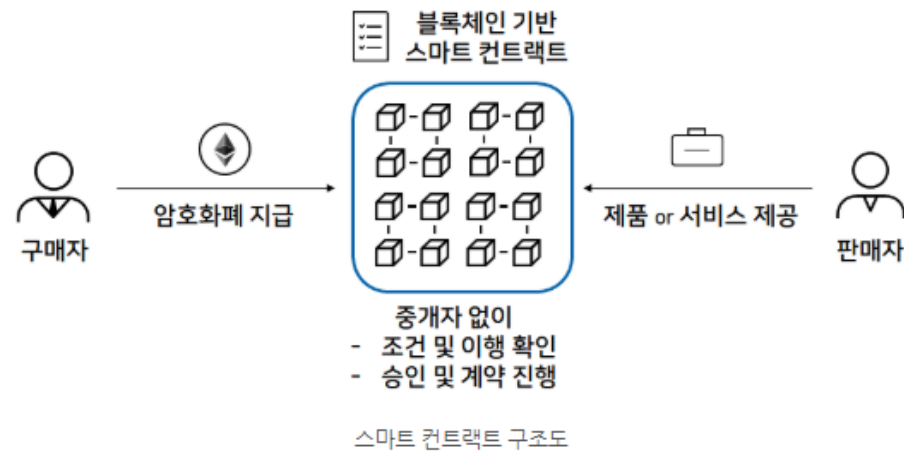
특징
스테이블 코인을 활용하여 원금 손실이 없는 총 참여금의 이자를 1등 당첨자에게 지급하는 복권
퍼블릭 블록체인으로 서비스
예치기간 : 참여 기간
잠금 기간 : 예치 코인을 디파이 프로젝트에 15일 예치 컴파운드, 메이커다오
당첨금 선정 : 스마트 컨트랙을 통해 당첨자 선정 투명성 제고
지급 : 1등으로 선정된 당첨자에게 원금 + 당첨금 지급



스마트 컨트랙트

조건에 부합하면 사람의 개입 없이 계약이 이행되는 일종의 디지털 자동화 계약 방식

현재 블록체인에서 사용되고 있는 스마트 컨트랙트는, 서면으로 이루어지던 계약을 코드로 구현하고 특정 조건이 충족되었을 때 해당 계약이 이행되도록 하는 script에 가깝습니다. 스마트 컨트랙트를 활용하면 두 당사자가 서로를 모르거나 신뢰하지 않더라도 계약을 체결할 수 있습니다





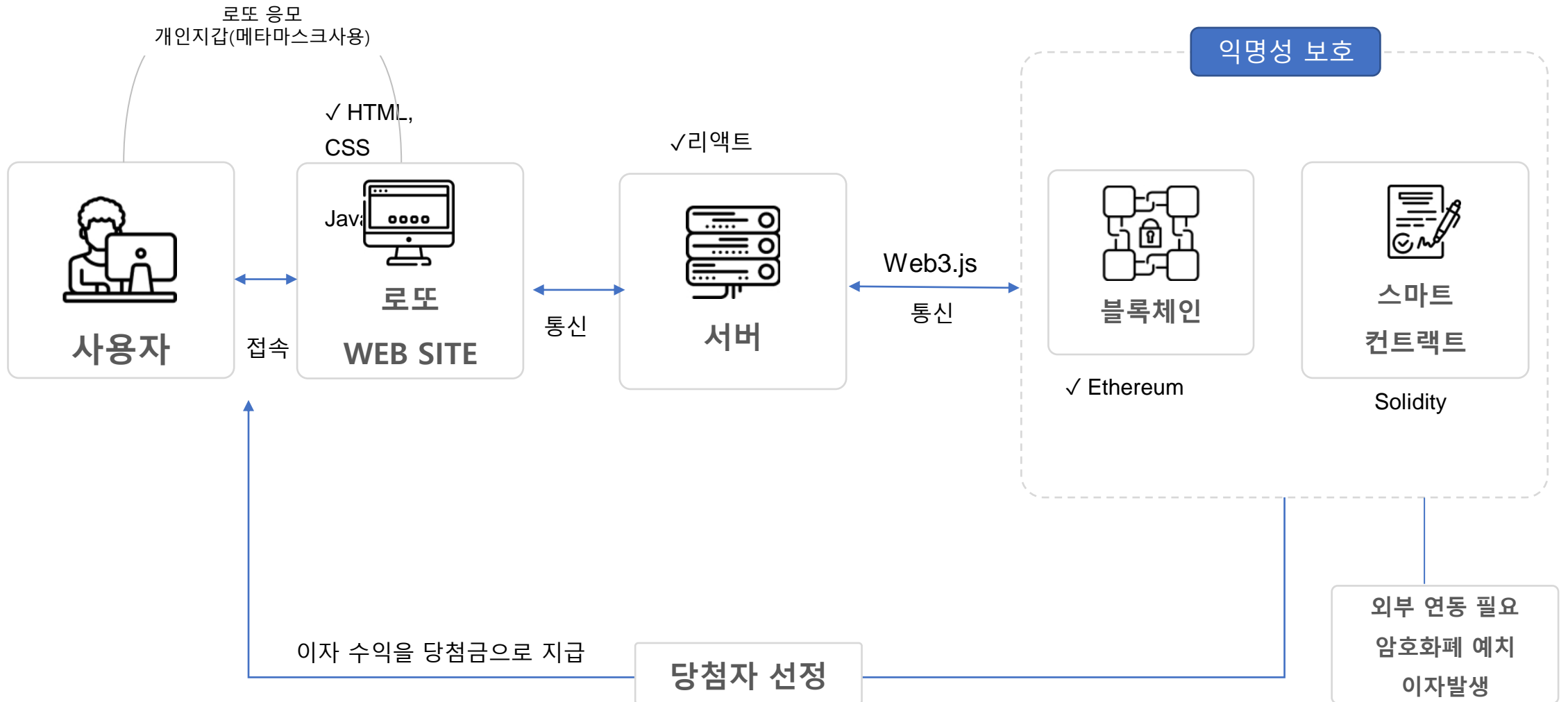
원금 손실 없는 로또 게임이란?

로또 구매 사이트에서 사용자들의 이더리움을 스테이블 코인 (DAI, 컴파운드, 테라)를 스마트 컨트랙트에 묶어서 이자를 발생하게 합니다.
그리고 여기서 발생하는 이자를 추첨을 통해 행운의 주인공에게 이자수익을 몰아주게 됩니다.
그리고 아쉽게 당첨이 되지 않는 사용자에게는 예치한 이더리움(DAI, 컴파운드, 테라)를 그대로 돌려줍니다.





시스템 구성도



외부 API

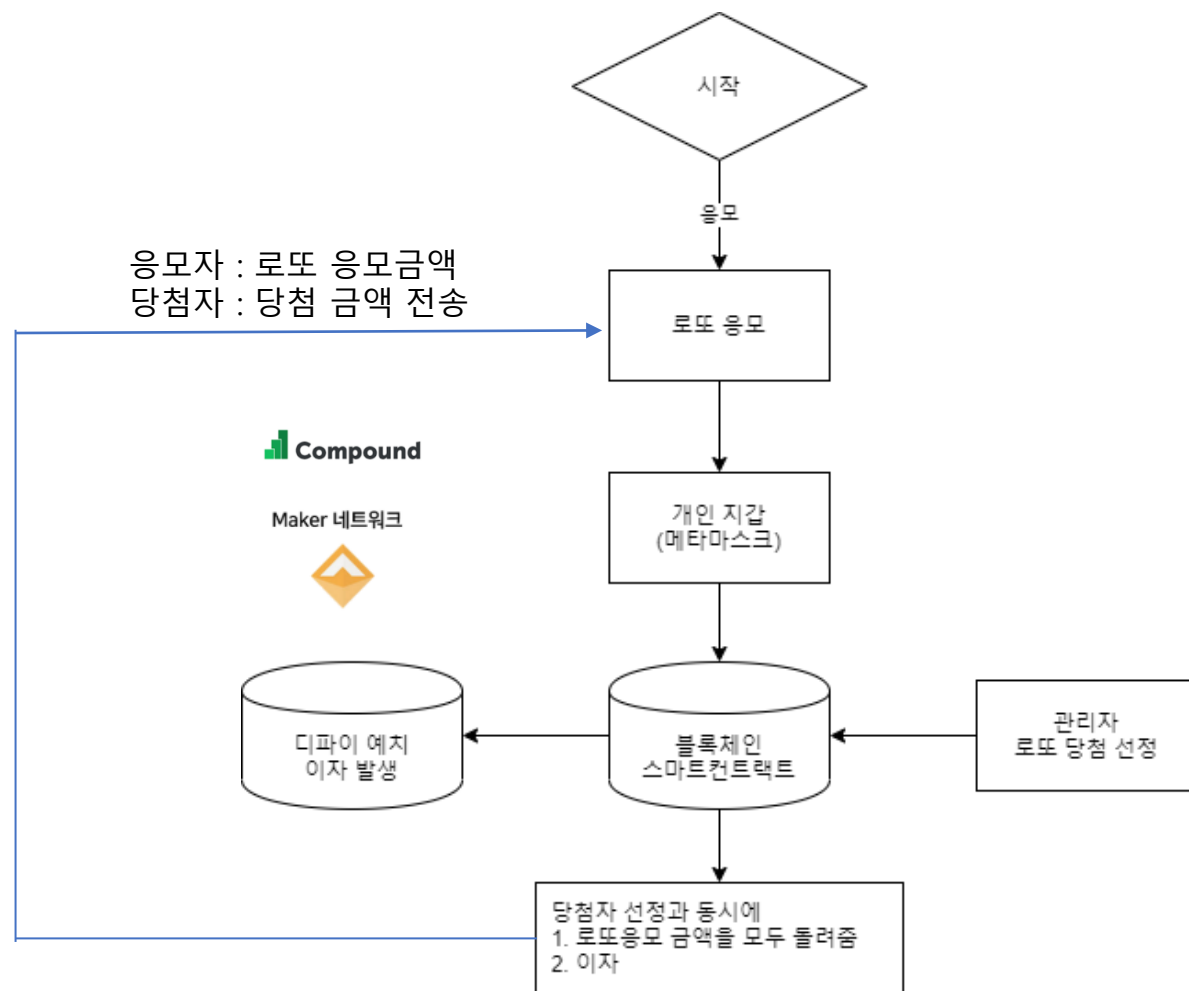
<https://developer.makerdao.com/>

<https://compound.finance/developers>





트랜잭션 데이터 흐름도





프로젝트 디렉토리 및 화면 구성

```
buntu 4096 Oct 17 02:38 ./
buntu 4096 Oct 17 02:36 ../
buntu 5139 Oct 17 02:40 DefiLottery.html
buntu 4096 Oct 17 02:35 css/
buntu 4096 Oct 17 02:35 images/
buntu 4096 Oct 17 02:34 js/
buntu 1227 Oct 17 02:34 lottery.sol
buntu 12288 Oct 17 02:37 node_modules/
buntu 119460 Oct 17 02:37 package-lock.json
buntu 648 Oct 17 02:42 server.js
~/homework$
~/homework$
~/homework$
~/homework$ node server.js
```

← → ↺ 주의 요함 | 54.255.237.145:8080/DefiLottery.html ☆ 🦊 🌐 🛠️ 👤 영민 ⋮

🌐 앱 📄 전자문서블록체인... 📁 카이스트발전재단 📄 머신러닝 📄 인공지능 📄 알고리즘 📄 블록체인 🌐 Remix - Ethereum I... 📄 이미지에 OCR 결과... » 📄 읽기 목록

Modern dapp browsers

무손실 로또 게임

Account 0xe9bb502a7150d5326be9a16baa9aada75a644c4b

로또 구매하기: 참여 하기 입력

0.1

Result value

무손실 로또 참여하기

관리자 기능

참가자 수 0

참가자-응모금액 0 ether

디파이 이자 금액 입력

0.03

이자 확정

응모현황

순서	응모자	참여금액
----	-----	------



실행 화면 - 로또 응모 & 응모자 현황

무손실 로또 게임

Account 0xfb889358301ec05a1612722cce777c1ec190962a

로또 구매하기: 참여 하기 입력

0.1

Result value

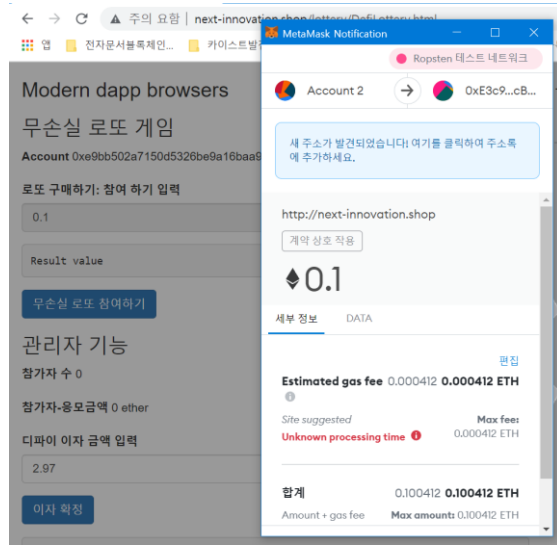
무손실 로또 참여하기

응모현황

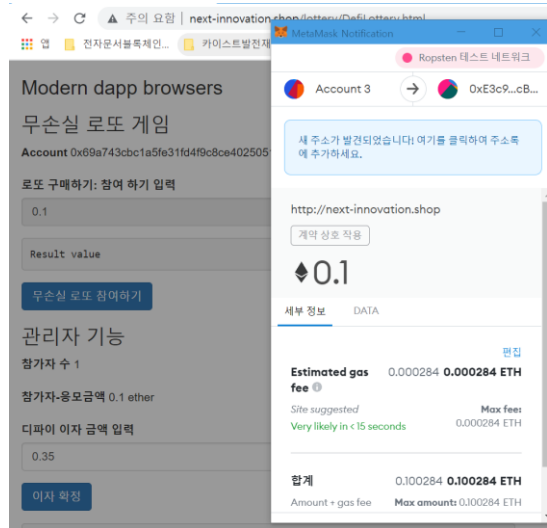
순서	응모자	참여금액
0	0x69a743cbc1A5FE31FD4f9C8ce4025051AA36415B	0.1eth
1	0x98d830A6b3254c8cF7e49E22166D53172Dcb5183	0.1eth
2	0xeeE72F2D87900f7702C84cFa29f2aA2dDE04dFa9	0.1eth
3	0xfb889358301eC05a1612722CCe777c1eC190962a	0.1eth



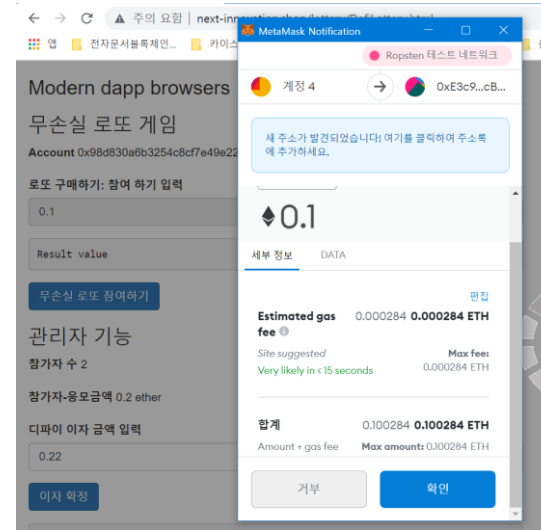
실행 화면 - 로또 응모



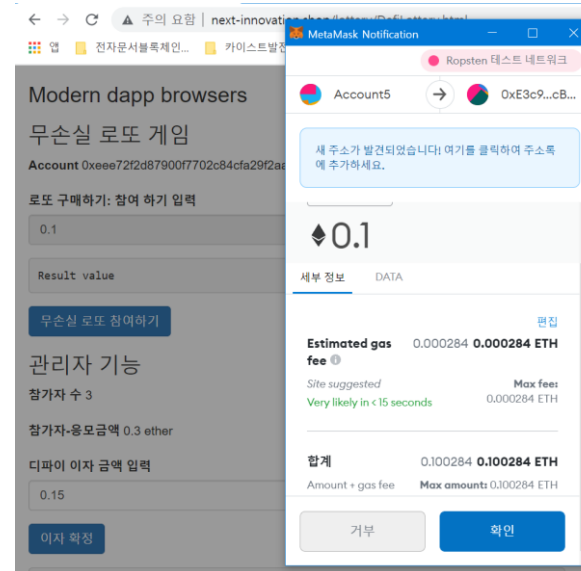
사용자1



사용자2



사용자3



사용자4



실행 화면 - 관리자

관리자 기능

참가자 수 4

참가자-응모금액 0.4 ether

디파이 이자 금액 입력

6.40

이자 확정

Result value

당첨자 선정하기

로또 당첨자 선정

앱 전자문서불록체인... 카이스트발전재단

두손길 로또 게임

Account 0xfb889358301ec05a1612722cce777c1ec1

로또 구매하기: 참여 하기 입력

0.1

Result value

무손실 로또 참여하기

관리자 기능

참가자 수 4

참가자-응모금액 0.4 ether

디파이 이자 금액 입력

0.05

이자 확정

error occured

당첨자 선정하기

MetaMask Notification

Ropsten 테스트 네트워크

Account 1 → 0xE3c9...cB...

새 주소가 발견되었습니다! 여기를 클릭하여 주소록에 추가하세요.

0.05

세부 정보 DATA

Estimated gas fee 0.000472 0.000472 ETH

Site suggested Very likely in < 15 seconds

Max fee: 0.000472 ETH

합계 0.050472 0.050472 ETH

Amount + gas fee Max amount: 0.050472 ETH

거부 확인



실행화면 - 응모자에게 배팅금액을 돌려줌

Block:	11242962 5 Block Confirmations
Timestamp:	1 min ago (Oct-17-2021 02:21:12 AM +UTC)
From:	0xe9bb502a7150d5326be9a16baa9aada75a644c4b
To:	<div>Contract 0xe3c9e5b8e1116cc4c253c9e52f219cfab74fcb0d</div> <div><div>TRANSFER 0.1 Ether From 0xe3c9e5b8e1116cc4c253c9e5... To → 0x69a743cbc1a5fe31fd4f9c8ce...</div><div>TRANSFER 0.1 Ether From 0xe3c9e5b8e1116cc4c253c9e5... To → 0x98d830a6b3254c8cf7e49e22...</div><div>TRANSFER 0.1 Ether From 0xe3c9e5b8e1116cc4c253c9e5... To → 0xee72f2d87900f7702c84cfa2...</div><div>TRANSFER 0.1 Ether From 0xe3c9e5b8e1116cc4c253c9e5... To → 0xfb889358301ec05a1612722c...</div><div>TRANSFER 0.05 Ether From 0xe3c9e5b8e1116cc4c253c9e5... To → 0xfb889358301ec05a1612722c...</div></div>
Value:	0.05 Ether (\$0.00)
Transaction Fee:	0.000251640000805248 Ether (\$0.00)
Gas Price:	0.000000002500000008 Ether (2.500000008 Gwei)
Txn Type:	2 (EIP-1559)

응모자

당첨자

<https://ropsten.etherscan.io/tx/0x7364b5eb808f9edfe5fcfd89f85729350ba301b6bdb20b96ee03fa9fb735d54b>