「goBlock: 디지털 자산 선제적 보호를 위한 실사구시형 합의 알고리즘 제시」

2021.6.12

goBlock 실무 프로젝트 과정 A반 [2]팀

팀 Kosk 소개

김규리 ***(K)***

컴퓨터 공학 전공 (전)
이빛컴퍼니 카페이
mvp *모델 개발 인턴*
관심분야: ***3D*** *컴퓨팅*

탈중앙화*, 송/수신 설계*

오준석 ***(o)***

관광일본어 전공
(전) 현대호텔 프론트 인턴
관심분야: 정보보안

탈중앙화*, 송/수신 설계*

성종현 ***(s)***

경영학과 전공
(전)푸르덴셜 세일즈 인턴
관심분야: 인터체인, ***NFT***

프로젝트 ***리딩****,*
알고리즘 *총괄*

김태웅 ***(k)***

임학 전공
(전)반지엔지니어링
산림경영선임기술자
관심분야: ***AI****,블록체인*
응용 영상 분석

보안성 *설계*

Proof of Safe Number(PoSN)

탈중앙화, 고 보안성, 고성능 합의기술, **금고번호 증명**

해결하고자 하는 실생활 문제

- 전세계적으로 디지털 자산의 가치가 높아지는 상황(ex 비플 785억, 크립토키티)
- 고부가가치를 가지는 디지털 자산에 대한 탈취/해킹 문제 빈번하게 발생.
- 디지털 자산(NFT, 전자화폐, 게임 아이템 등)을 안전하게 예탁/인출하는 보안성 문제 대두.
- 1차적으로는 게이밍 유저들의 디지털 경제 권익 보호를 목표.

수혜자(알고리즘 타겟)

- 1차 목표 : 고사양 3D 게임 유저(팀 Kosk 파트너쉽 맺은 협약사)
  - 일반 게임유저
- 2차 목표 : 게임, 예술품, 부동산 블록체인 플랫폼 사용자
  - 고가치 digital asset 보관자
- 3차 목표 : 모든 블록체인 dapp 사용자
- 기대효과 : 넷상 블랙박스 효과

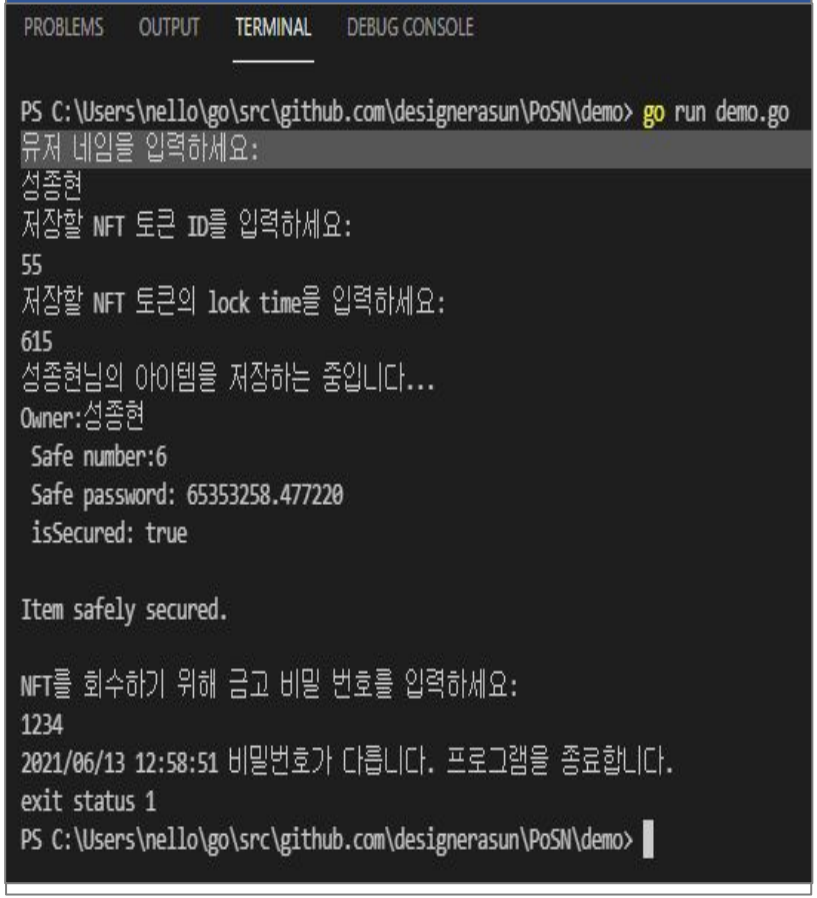
문제 해결을 위한 알고리즘! PoSN

1. 비대칭키 암호화 방식 채택
   (공개키1, 개인키1)
2. 공개키: 금고 번호 생성
3. 개인키:
   1)랜덤시드 OTP 1차 확인(A) -
   1차 보안성 ↑ [일반 사용자]

   2) 금고번호 입력 시 생체인식-지정맥(B) -
   2차 보안성 ↑ [고가 자산 보호자]
4. if A == A && B == B { fetch NFT to user inventory } else { ask user to re-enter one of those }

[참고 1] 프로토 타입 개발 방향 제시

데모 프로그램 시연



데모 프로그램 설명

1. NFT token ID, NFT lock time을 입력 받고, Knot(손잡이) 값을 계산한다.
2. 세 개의 값을 연산, **금고 비밀 번호**를 생성한다 **(공개키 암호화)**
3. NFT를 저장한다(1 레이어)
4. 유저에게 금고 비밀 번호를 입력 받는다
5. **랜덤시드 + OTP 모듈을 이용하여 작업 성공 시** 금고 lock을 해제한다 - 주요 개발 사항
6. 고가의 Digital asset의 보관자의 경우 생체인증 검증 과정을 한 번 더 거쳐 해제한다.
7. 5번과 6번에서 동일하지 않은 경우 금고 lock을 유지하고, 프로그램을 종료한다.

[참고 2] 소스 코드 발췌

```
// Create a safe and safeNumber.
mySafe := safe{}
mySafeNumber := safePassword{}

// Enter a user name, NFT token ID, and locktime to store.
// Exmaple - owner: jonghyun, lock_time: 20210615, token_id: goBlock
fmt.Println("유저 네임을 입력하세요: ")
fmt.Scanln(&mySafeNumber.owner)
fmt.Println("저장할 NFT 토큰 ID를 입력하세요: ")
fmt.Scanln(&mySafeNumber.token_id)
fmt.Println("저장할 NFT 토큰의 lock time을 입력하세요: ")
fmt.Scanln(&mySafeNumber.lock_time)
fmt.Printf("%v님의 아이템을 저장하는 중입니다...\n", mySafeNumber.owner)

// Creat a random safe number and assign it to mySafe.
rand.Seed(time.Now().UnixNano())
temp_safeNum := rand.Int63n(10)
mySafe.safeNum = int(temp_safeNum)

// Calculate knot first.
radius := mySafeNumber.lock_time
height := mySafeNumber.token_id
mySafe.knot = math.Pi * math.Pow(radius, 2) * height

// Add a lock_time, token_id, and safe.knot to create a safePw.
mySafeNumber.safePw = radius + height + mySafe.knot

// Declare a boolean variable to state if item is well secured.
isSecured := true

// Print a message: safeNum: xxx, owner: jonghyun item well secured.
fmt.Printf("Owner:%s\n Safe number:%d\n Safe password: %f\n isSecured: %v\n ", mySafeNumber.owner, mySafe.safeNum, mySafeNumber.safePw, isSecured)
fmt.Println()
fmt.Println("Item safely secured.")
fmt.Println()

// Check item storage state.
var user_safe_pw float64
fmt.Println("NFT를 회수하기 위해 금고 비밀 번호를 입력하세요: ")
fmt.Scanln(&user_safe_pw)
stateCheck := mySafeNumber.stateCheck(user_safe_pw)

if stateCheck == true {
    fmt.Println("NFT가 회수되었습니다.")
} else {
    log.Fatal("비밀번호가 다릅니다. 프로그램을 종료합니다.")
}
```

기존 알고리즘과의 차별성 및 핵심 개발 목표

문제·이슈

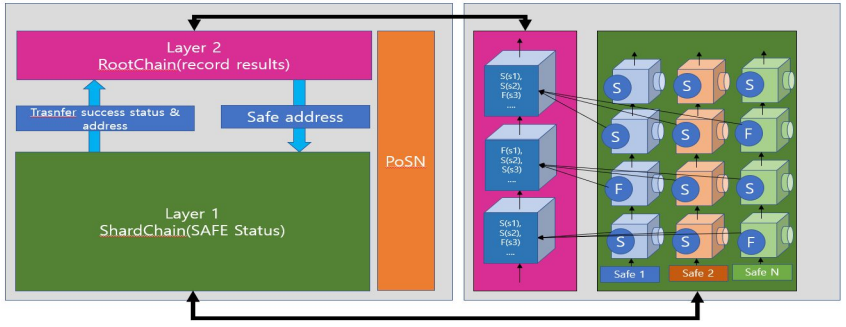
- 디지털 자산의 수요가 급증, '소유권' 분쟁의 문제 - 디지털 경제 권익 보호
- 보안성 문제 : 고부가 가치를 가지는 디지털 자산에 대한 탈취 해킹 문제가 빈번하게 발생
- 탈중앙화 문제 : DPoS 합의 알고리즘 (정해진 노드 수), PoW합의 알고리즘 (생태계독점)

기존 알고리즘 분석 (Quarkchain)

- 샤딩기술을 통한 블록체인의 확장성 문제 해결 (TPS)
- Boson 합의 알고리즘 - 루트체인 우선합의 (교차검증을 통한 탈중앙화, 보안성 실현)
- PoSW (PoW + PoS) 채택, 주요합의 - PoW의 문제점인 독점을 막고자 Staking까지 해야만 해시파워 인정 (독점 탈중앙화)

기술 정의 및 개념도

KOSK chain – PoSN



개선 제시안 (PoSN)

- 알고랜드 장점 차용 - 랜덤 노드 생성, 금고 랜덤 배정(탈중앙화)
- 쿼크체인 장점 차용 - 샤딩기술로 수평적 데이터 저장기술로 수 많은 노드들의 트랜잭션들을 분배해서 빠르게 처리함으로 TPS를 올림 (확장성), NFT 토큰활용 이종 플랫폼 인터체인 연결 (확장성)
- 암. 복호화 시 랜덤시드 + OTP, 생체인식를 통해 보안성을 강화하여 샤드 자체의 안전성 강화.

연구목표 및 내용

연구 목표

2팀 합의 알고리즘 목표
NFT 기반 공개키 + 타이핑 DNA 기반 개인키를 활용한 10,000tps이상 합의기술 개발

연구 내용 - 개발 모듈 5가지

- 랜덤시드 + OTP, 생체인식[지정맥 인증] 기반 복호화 모듈 - 자체 개발
- 2 layer sharding system - 쿼크체인 이더리움 오픈소스
- 유동적 랜덤 노드 선정 기술 개발 - Algorand 오픈소스
- ERC-721 토큰활용 이종 플랫폼 인터체인 연결 - 오픈 소스
- 유저 친화적 최적의 UI/UX 디자인 - 오픈소스

개발 제안 목적 및 필요성과 개발 일정

정부지원의 필요성

- **(게이머의 보호)** 게임 시장 규모에 비해 유저들의 경제적 권익 보호를 위한 정책의 미비
- **(거대 플랫폼의 독점 방지)** 거대 플랫폼의 수수료 인상 및 독점으로 인한 생태계의 붕괴
- **(사용자들의 참여 독려)** 인터체인 플랫폼 구축을 통한 사용자들의 순수한 경쟁 및 컨텐츠의 확장

추진 시급성

- **아이디의 해킹을 통한 디지털 자산의 분실에 대한 보상정책의 미비를 극복하기 위해 게임 자산을 금고에 보관하여 분실을 방지**
- **거대 플랫폼에 대한 의존성과 독점을 극복하기 위한 인터체인 플랫폼 개발**
- **사용자들의 참여기회 확대 및 순수한 경쟁을 통한 컨텐츠의 확장**

과제의 구성	목표 성능
• **독창적 기술 확보**	• 기존 알고리즘 대비 저전력, 고속도의 알고리즘 개발 • 접근성이 좋은 UI/UX 개발을 통한 사용자 편의성 확보
• PoSN(Proof of Safe Number)	• NFT, 2계층 샤딩 기술 기반의 아이템 금고 구현 • 랜덤시드+OTP, 생체인식 분석을 통한 복호화 기술 개발
• NFT-Smart Contract	• NFT 이용 DAP(Digital Asset Protection) 특화 합의 개발
• Multi – Test Net 구축	• 성능 평가 및 시뮬레이션을 위한 테스트넷 구축
• **타 체인 플랫폼 지원 가능 메인넷 구축**	• 거대 플랫폼의 독점 방지 • 오픈소스를 통한 공유 및 사용자 참여 생태계 구축

1차 – 192h	2차 – 192h	3차 – 192h	4차 – 192h	5차 – 192h	추정 소요예산(%)
취약점 분석 및 구조설계	랜덤시드 OTP + 생체 인식 분석 모듈 1		랜덤시드 OTP + 생체 인식 분석 모듈 2	유저 친화 UI/UX 구축	50%
	2 layer sharding system		랜덤 노드 배정 기술		40%
	ERC-721 이종 플랫폼 인터체인 연결		각 모듈 별 보조 모듈		10%

[참고 3] PoSN White Paper

문제 인식 ~ 피해 대상

https://docs.google.com/document/d/1UJgPtJqh9DRFu9pnyua1XPf_bkUEeaMEJJY7fZ_C_r4/edit?usp=sharing