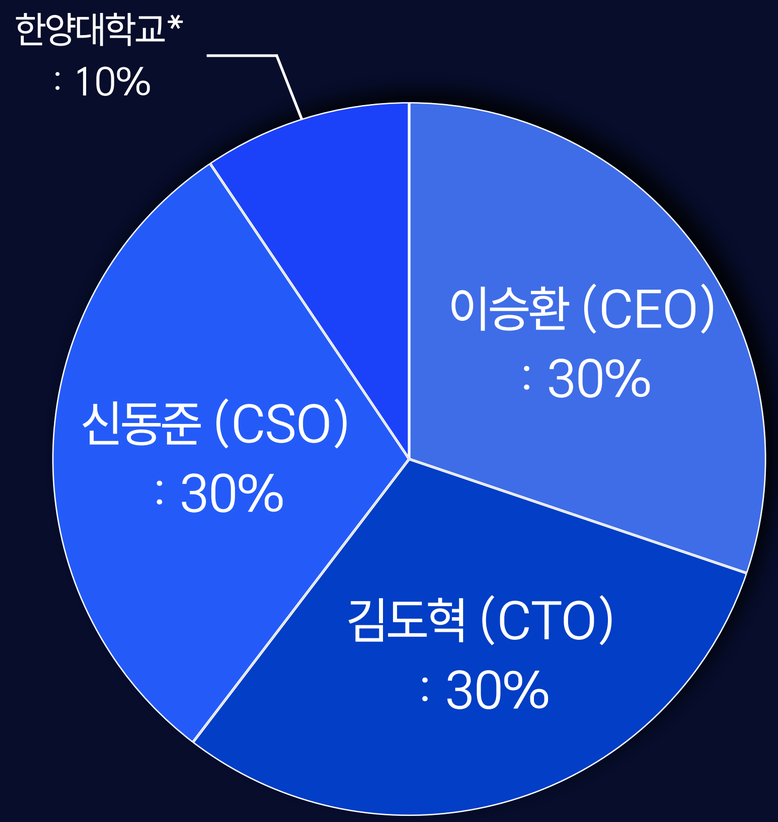
# waLLLnut

투명하고 신뢰성 있는 세상을 위해

# 회사소개

**월넛 주식회사** 양자 내성 암호 보유회사 (설립: 25.1.21)

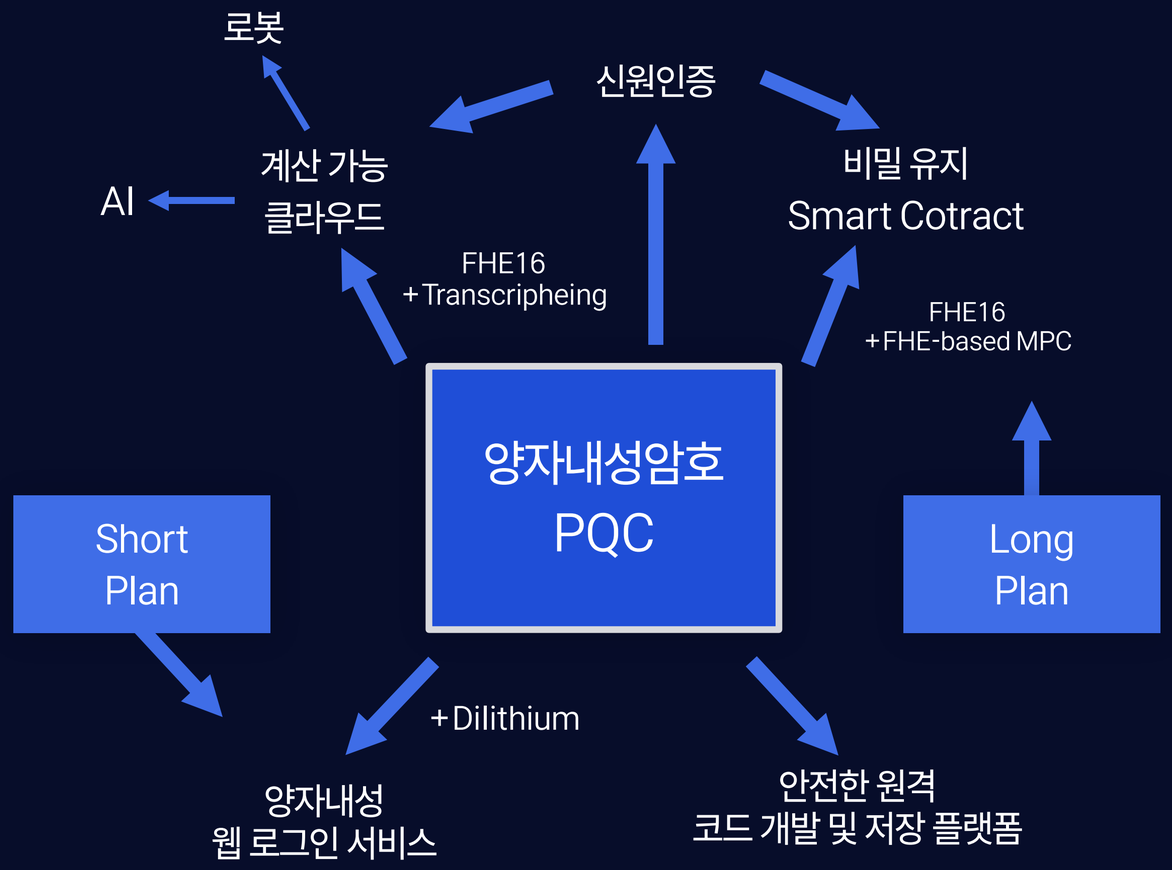
[ 지분 ]




**자본금 : 4,000만원**

*자본금 1억 넘을시, 1,000만원 고정

**회사 슬로건** 개인이 보호받는 투명하고 신뢰성 있는 세상을 위해




*Post-quantum Cryptography(PQC) : 양자내성암호

*양자 컴퓨터 공격에도 안전한 최신 암호

# Short-term plan

[암호/보안] 단기 제품 군을 통한 사업 부트스트래핑

# 01 단기 Product 제품 1

[클라우드 + FHE 사업의 발판이 될 제품]

## 보안 제품

**‘클라우드 상에서 소스코드를 보호하면서 개발할 수 있는 안전한 코딩 프레임워크’**

1. 모든 파일이 항시 암호화되어 클라우드에 저장됨
2. 복호화된 데이터는 휘발성을 지님

### Need 1

‘소규모 스타트업’의 경우,
사내 보안 리소스가 부족하고
인력 변동이 심함.
개발 속도를 높이고 싶으나,
자사의 코드가 아직 가치를
인정받기 전이므로 여러 개발자들에게
코드 흔적을 남기고 싶지 않음.

### Need 2

개발회사의 경우,
인도와 같은 개발도상국의 인력으로
개발한다면,
저렴한 비용으로 개발이 가능함.
그러나, 안전한 원격 개발 시스템이
없다면 개발 코드가 타인으로
넘어갈 수 있음.

### Need 3

많은 스타트업이 ‘Git’을
초기 개발 도구로 쓰지만,
High technology 기반 코드의 경우
작성된 코드가 ‘Git'에게
넘어가 버리는것이 아닌지에 대한
두려움이 있음.

# STEP.1 안전한 원격 소스코드 개발 서비스의 기존 시장분석

| 서비스 | 연간예상 매출 | 사용자 수 | 핵심 기능 | 보안 위험 |
|---|---|---|---|---|
| Tresorit | 약 2,500만 달러 | 11,000개<br>이상의 기관 | · 파일은 안전하게 저장되며<br>서버는 접근 할 수 없음<br>· 모든 활동은 기록됨<br>· 키는 사용자 장치에 저장됨 | · 개발 환경에 남는 소스 코드 잔재<br>· 공용/공유 디바이스에서의 취약한<br>원격 작업 |
| Proton | 약 10억 달러 | 1억명 이상의 계정<br>10,000개 이상의 기관 | · 보안 클라우드 기능<br>· VPN 및 암호화폐 지갑과 통합됨 | · 개발 환경에 남는 소스 코드 잔재<br>· 원격 근무 중 높은 보안 위험 존재 |
| Gitpod | 약 820만 달러 | 150만명의 계정 | · 브라우저 기반 협업 개발<br>· 임시 작업 공간 | · 개발 환경에 남는 소스 코드 잔재<br>· 원격 근무 중 높은 보안 위험 존재 |
| waLLLnut | [목표]<br>약 10,000만 달러 | [목표]<br>1,000만명 이상의 계정<br>1,000개 이상의 가관 | · 소스 코드 보호<br>· 모든 실행 흔적 삭제<br>· 언제 어디서나 안전한 개발환경 제공 | · 개발 환경에 코드 잔재 없음<br>· 공용/공유 디바이스와<br>공공 네트워크에서도 안전한 원격작업 |

# 01 단기 Product 제품2

## 양자 내성 로그인 서비스

1. SKT 사태와 같이, **DB가 해킹을 당해도** 비밀번호 유출이 전혀 없는 로그인 서비스
2. 사용자의 로그인 정보는 3초 후 바로 **휘발**되는  로그인 서비스
3. **양자 컴퓨터 공격**에 안전한 양자내성 로그인 서비스

## 기술 스택

(Post Quantum) SSH 통신 기법 + TEE 상에서의 로그인 검증

# 01 단기 Product 제품1

보안성 및 편의성

## 기존 해시기반 로그인 서비스

**“편의성 가장 높게, 보안성 가장 낮게”**

*보안성 낮은 이유
: 서버의 DB가 공개되면 (SKT 정보 유출 사태)
해당 사이트 비밀번호는 모두 공개되며,
로그인 시 서버가 비밀번호를 확인함

## waLLLnut 로그인 서비스

**“편의성은 기존과 유사하고,
보안성은 아주 높게”**

- 사용자가 보낸 로그인 정보는
자연스럽게 휘발됨
- DB가 해킹 되어도
유저의 비밀번호는 안전함
- 로그인 시 서버는
유저의 비밀번호를 보지 못함
- 표준 기반 시스템

*편의성이 조금 낮은 이유: TEE를 사용함

## 차세대 로그인 서비스 OPAQUE

**“편의성 가장 낮게, 보안성 가장 높게”**

- DB가 공개되어도
사용자의 비밀번호는 안전함
- 로그인시 서버는
사용자의 비밀번호를 보지 못함

*편의성이 낮은 이유
: 표준화 작업 중. 통신 round 수가 큼.
양자 내성이 있으려면 매우 느림.

# 01 단기 Product 제품 1 : 타겟 마켓

[ Market size : $202B ]

| 서비스/이름 | 특징 | 요금 모델 | 주 타겟 |
|---|---|---|---|
| Auth0/Okta | SaaS 인증 플랫폼, 다양한 OAuth/OIDC 기능,해시기반 | $23+/mo(Teams). 사용자 기반 과금 | 시리즈 A~B이상 SaaS 기업 |
| Firebase/AWS Congito | 무료 티어 있음, 자체 구현에 적합,해시기반 | 무료~호출량 기반 과금(월 $0~수십달러) | 초기 스타트업, 기술팀 있는 곳 |
| FusionAuth | 오픈 소스 기반, SaaS 옵션도 있음,해시기반 | 무료 or SaaS 유료 플랜 존재 | 기술 이해도 높은 초기~중기 스타트업 |
| Keycloak | 무료 오픈 소스, 자체 호스팅,해시기반 | 무료 (호스팅만 별도) | 엔지니어 기반 팀 |
| WorkOS/Frontegg | 엔터 프라이즈용 통합 인증/SSO,해시기반 | 사용자/호출 기반 (수백 달러/월 수준) | 중견 SaaS/엔터프라이즈 |
| Kinde/ID.me | 경량 SaaS, 인증 전문 솔루션,해시기반 | $25+/mo 기준 | 개발자용 인증 SaaS/엔터프라이즈 |
| 1Passsword Business | 비밀번호 매니저 + 인증기능,해시기반 | $7.99/user/mo | 중소기업, IT조직 |
| waLLLnut 로그인 API<br>(초기 스타트 업 대상) | REST API 기반, SSL+PW<br>극초기 스타트업용 경량 서비스<br>PQC 기반 | Free Tier (월 1,000 호출)<br>$19/mo (10K 호출)<br>$ 49/mo (50K 호출)<br>$ 99/mo (200K 호출) | 극초기 스타트업, 웹서비스/쇼핑몰 등<br>MVP급 제품 |

# Long-term plan

미래인 클라우드와 블록체인을 위한 PQC 기술

# 02 클라우드를 위한 동형암호 기술

Q

동형암호 기술은 왜 산업에서 사용하기 어려운가?

01

[일반 사용자]

각자 중요한 개인 데이터를
활용하는 데 있어 보안상의 이유로
**매우 수동적**

02

[기업]

보안 사고가 나기 전까지
보안 시스템을
**바꾸려 하지 않음**

03

[동형암호 기술의 한계]

**평문연산 대비**
**연산속도가 느림**

# 02 waLLLnut 3년 로드맵

## YEAR 1

**[ 기술 Productization ]**

- FHE API/SDK 공개 (Rust, C, WebAssembly 연동)
- Bootstrapping 성능 벤치마크 정식화 (ZAMA vs Ours)
- GitHub 오픈소스, Benchmark, Playground 제공
- Solana Grant 수주 및 26년 자금 조달&콜로세움 경험
- FHE16EVM 초기 모델 구축

## YEAR 2

**[ Confidential Layer 출시 ]**

- MPC 와 FHE16 기반 저비용 Confidential Execution Layer 출시
- GPU setting 개발
- L2 연동, FHE 비용 분산 처리 구조 설계
- Confidential wallet 및 demo dApp 제작
- 후속 Solana &Etherium 그랜트 및 CES 27 진행

## YEAR 3

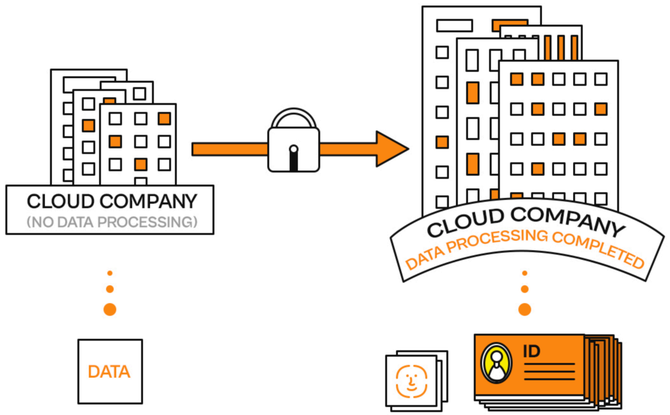
**[ Infra 확장 및 수익화 ]**

- Flip 및 블록체인 펀딩 조달
- FPGA (Alleo) 개발.
- 토큰 분배 및 IPO (Initial Public Offering) 준비

# 02 클라우드를 위한 동형암호 기술

## FHE16 기반
## AES Transciphering

데이터를 단순 저장만 하는 클라우드 회사들을
암호문 상에서 안전하게 데이터를 처리하는
데이터 가공 회사로 바꾸어 주는 B2B 서비스




**Point. 1**

일반 사용자에게 서비스 동의만
받아올 수 있으면 됨.

**Point. 2**

클라우드 서버의 인프라를 바꿀 필요 없이,
자사의 기술이 애드온 형태로 붙어서 데이터 가공 가능.

**Point. 3**

클라우드 서버가 주체적으로
사전에 계산을 진행할 수 있음.
그러므로, 실시간 처리가 필요하지 않아
상대적으로 느린 속도로도 서비스 제공 가능.

# 02 블록체인을 위한 PQC 기술

**ZAMA**

TFHE-rs를 활용한 블록체인 상에서의
private 스마트 컨트랙트 계약
-Series A : $73M
-Series B : $57M
유니콘 등극

**Fhenix**

TFHE-rs를 활용한 FHE-rollup 기술
-Series A : $15M
Helium 테스트 넷 공개

**[ waLLLnut 주식회사 ]**

**FHE16과 MPC를 활용한**
**적은 수수료로 계약 가능한 스마트 컨트랙트 기술 보유**

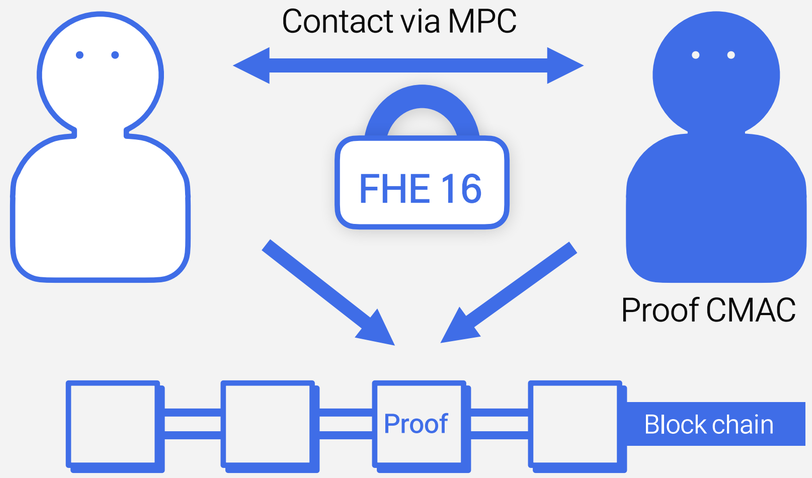
# 02 블록체인을 위한 PQC 기술

## UseCase1

통계 정보 계산 가능한 비밀 투표 시스템

## UseCase 2

블라인드 옥션 시스템




*Cloud 와 Smart contract 기술 기반으로 인해 로봇과 AI 서비스로의 확장이 쉽게 구현됨

# 보유기술

# 03 타 경쟁회사 기술과 비교 : waLLLnut의 FHE16 VS ZAMA의 TFHE-rs

- 동형암호 : 암호문상에서 연산 가능한 암호문

: 안전한 스마트 컨트랙트 구현과 안전한 데이터 처리 클라우드를 위한 핵심기술

[ 정수 덧셈 속도 ]

| | 4bit | 8bit | 16bit | 32bit | 64bit | 128bit | 256bit |
|---|---|---|---|---|---|---|---|
| TFHE-rs | 58ms | 101ms | 101ms | 132ms | 180ms | 298ms | 434ms |
| FHE16 | 40ms | 45ms | 53ms | 70ms | 111ms | 172ms | 382ms |

*Gate 연산: **5ms (자사)** VS 20ms (ZAMA)

*Key size 차이 114MiB / 20MiB (FHE16, 최적화 되었을 때) 5배 차이
투자 규모 차이: ZAMA (Series A 투자 $130M vs 자사 자본금 4000만원)
TEST CPU : Xeon 6240R

# 03 타 경쟁회사 기술과 비교 : waLLLnut의 FHE16 VS ZAMA의 TFHE-rs

**Transciphering**

연산 불가능한 기존 암호문을 동형암호로 바꾸는 기술

**Trivium/Krivium (유럽 표준 stream 암호)**

TFHE-rs : 5ms per bit / FHE16: 1.45ms per bit

**AES (전세계 표준 block 암호)**

TFD-rs : NONE/FHE16: 23ms per bit

**FHE-based MPC**

사용자들이 자신의 데이터를 숨긴채 연산결과를 얻는 기술
Ex) TFHE-rs 보다 FHE 16 이 더 월등함

**Robust MPC**

FHE16: 정직하지 않은 유저 발생 시 탐지 가능
TFHE-rs: 모든 유저는 정직히 수행해야 결과 얻을 수 있음

**Without floating point**

FHE16: 연산 합의 뿐 아니라, 저사양 chip에서도 연산 가능
TFHE-rs: 부동소수점을 사용해야 하므로,
유저간 연산 결과 합의를 이루지 못하는 문제 발생

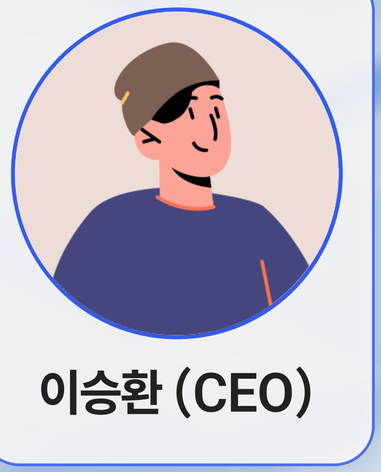
# 03 특허 보유

- 한양대학교 실험실 창업 (PQC 핵심 특허 창출 중)
- 한양대학교와 기술협약 체결 (자사의 주요 특허 관리)

| 지식재산권 종류 | 지식재산권 명 | 등록번호 |
|---|---|---|
| 특허 [출원] | 연산 속도가 향상된 동형 암호 시스템 및<br>이에 있어서 암호문 생성 방법 | PCT/KR2024/012529(24.08.22) |
| 특허 [출원] | 16bit 산술 연산으로 동형 연산을 수행하는<br>동형 암호시스템 | 10-2024-0137735 (24.09.27.) |
| 특허 [출원] | 부동소수점 숫자를 암호문 상에서 덧셈 및 뺄셈 연산을<br>하면서 오버플로우를 탐지하는 장치 | 10-2023-0017554 (23.02.09.) |
| 특허 [출원] | 확장된 NTT 연산 방법 및 장치<br>(Method and Device for Operating Extended NTT) | 10-2023-0083406 (2023.06.28.) |
| 특허 [출원] | 트리비움의 키 스트림 병렬 연산 장치 및 방법<br>(Device and Method for Parallel Computation of Key Stream in Trivium) | 10-2024-0193226 (2024.12.18.) |

⋮ 그 외 다수의 특허 보유

# 4. 팀 구성



**이승환 (CEO)**

역량 : 스타트업 멤버 활동 및 다양한 학계/산업계 활동
세계 최고 수준 FHE, MPC, 블록체인 기술 보유

경험 : 2019년 스터디룸 방 대여 플랫폼(Studyes) CTO 역임
2014년 한양대 스타트업 아카데미 8기 졸업

수상 : 2019년 한국통신학회 논문 우수상
㈜ Supergate와 협력해서 FHE 상용화 및 개발, 납품
2025년 ENRICH IT AWARD 우수 논문상 수상

⋮

# 4. 팀 구성

김도혁 (CTO)

신동준 (CSO)

역량 : 세계 최고 수준의 FHE 및 MPC, 블록체인 기술 보유
세계 최고 분산화된 병렬 동형 연산 기술 보유

경험 : ㈜ Supergate와 협력해서 FHE 상용화 및 개발 및 납품
동형암호 기반 DB 검색 연구 및 개발

⋮

역량 : 한양대학교 CCRL 연구실 PI로서 FHE 와 MPC, 블록체인
고도화 연구, 인재 육성 및 회사 전략 수립 및 진행

경험 : 다양한 주제의 연구 수립/진행. 현재 다양한 암호/보안 학계 교수 및
삼성전자등 여러 대기업과 협력하여 연구를 진행

네트워크 : 한국투자금융지주, 키움증권, 네이버 등 국내 대기업,
Cryptolab, Desilo, 지크립토 등 실험실 창업 기반의
암호 회사들과 네트워크 형성

⋮

# 4. 팀 구성

**김영준**
(수석 엔지니어)

역량 : 한양대학교 융합전자공학부/동대학원 융합전자공학과 석사 졸업
세계 최고 분산화된 병렬 동형 연산 기술 보유
경험 : 저사양 디바이스 대상 고효율 PQC 안전성 및 성능 검증 기술 개발
SK Hynix와 협력해 In DRAM ECC Worst Margin TPH Solution 개발 및 관련 회로 개선

⋮

**신기인**
(브랜드 디자이너)

역량 : 블록체인 관련 스타트업 4년차 디자이너
경험 : Solana Radar Hackathon Vietnam 1위
(캐릭터 및 그래픽 디자인 담당)
Solana Radar side track 2위 (게임 캐릭터 및 아이템 디자인 )

⋮

# Thank you

waLLLnut