비트코인 채굴하기

세명컴고 IT컨퍼런스

feat: 레전드 용돈 벌이



10202김남우

하기전에 간단한 자기소개

자기소개

보안과 10202 김남우이올시다

전공동아리

SCA소속

활동명은 광장동김치찌개장인



Security Cyber Agies

디지털 포렌식과 블록체인 암호학 공부중이다.

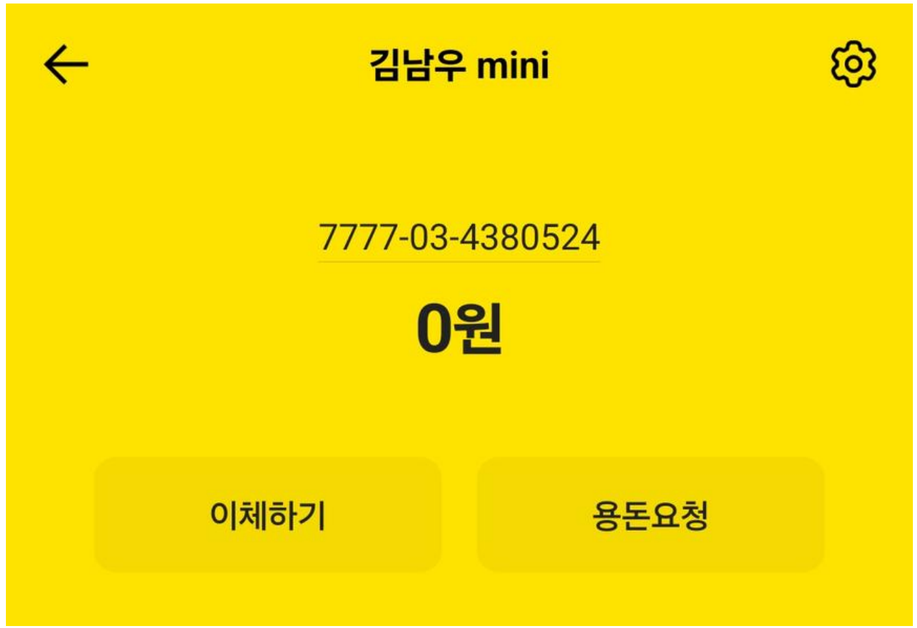
주제 선정이유

주제 선정

돈이 없어서..

뭐라도 해보려고..

학교도 못다닐뻔함





주제 선정

돈을 벌기 위해 생각한것!

주제 선정

1.버그 바운티로
용돈도 벌고 CVE도 얻기

주제 선정

버그바운티 할 실력이 안됨



CVE가지고 싶어요..

주제 선정

2번 알바하기

주제 선정

시간이 없다..



월요일 수요일 전공동아리

화요일 목요일 야자..

그래서 생각한 특단의 조치

주제 선정

비트코인 채굴!!





비트코인 채굴이란?

비트코인 채굴이란

컴퓨터로 캐는 금

- 비트코인 거래 기록을 묶어 장부(블록체인)에 새 페이지를 붙이는 일
- 조건에 맞는 숫자를 찾을 때까지 컴퓨터가 계속 계산 (= 복권 긁기)
- 가장 먼저 찾은 사람이 보상을 받음 (약 10분마다 3.125 BTC)

→ 계산이 빠른 컴퓨터가 많을수록 유리!



이런 겁내 큰 채굴기들이 점령중

ASIC 채굴기 1대

≈ 200 TH/s

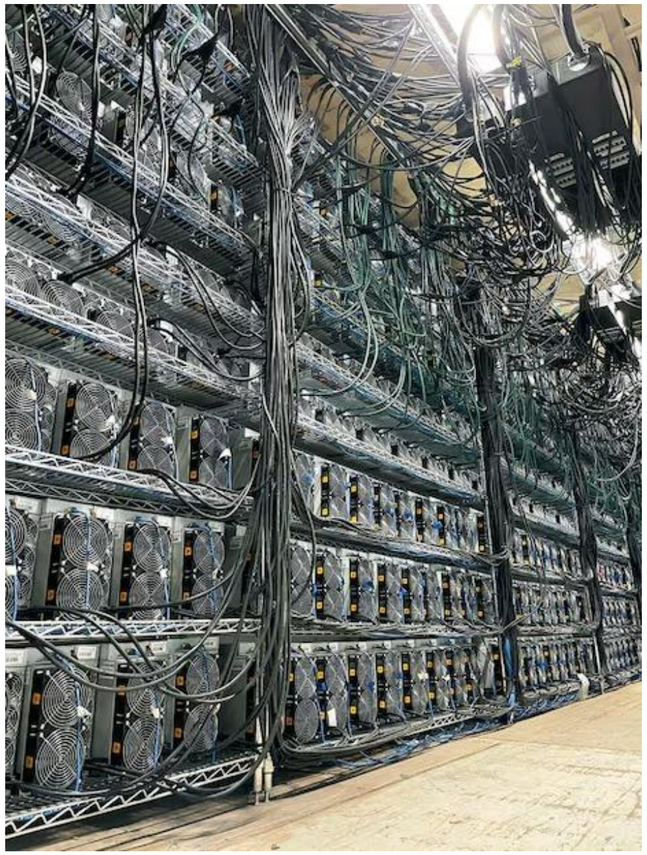
1초에 200조 번 계산 · 약 3,500W

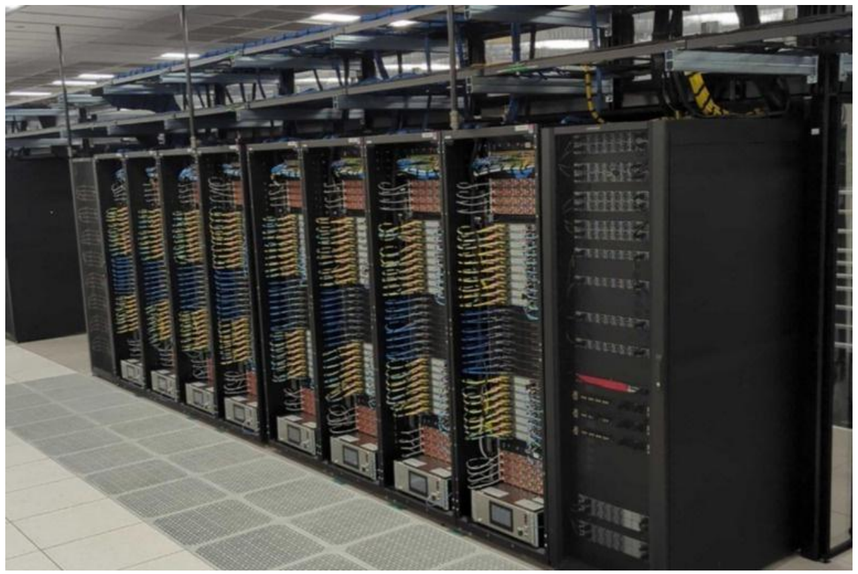
내 노트북

≈ 2,200 H/s

1초에 2,200번 계산 · 약 38W

약 900억 배 차이





그래서 내 노트북으로는 채굴이 불가능 하다 판단!

항목	사양
모델	ASUS (FA40
CPU	AMD F 16스러
GPU	NVIDI 5060 I
RAM	32GB 성)

<- 이정도도 사실 고사양이지만 한참 모자름

그래서 생각한 대체제!!

비트코인

- *SHA-256 해시 계산
- *ASIC 전용 채굴기가 판을 독점
- 노트북으로 캐면 사실상 0원

VS

모네로 (XMR)

- *RandomX 해시 계산
- ASIC이 못 끼게 일부러 설계
- CPU로도 캘 수 있다 → 노트북 OK

→그래서 비교적 가벼운 모네로를 직접 캐보기로 함

*ASIC(Application-Specific Integrated Circuit)은 한국어로 주문형 반도체

*SHA-256:어떤 데이터든 64자리의 고정된 문자열로 변환해 주는 암호화 해시 알고리즘

*RandomX는 일반용 CPU를 위해 설계된 작업증명(Proof-of-Work, PoW) 암호화폐 채굴 알고리즘



반갑소 모네로코인이여



모네로 코인을 선택한 이유

총 3가지로 나눌수 있다

첫번째

CPU로 캘 수 있다

	비트코인	모네로
해시 알고리즘	SHA-256	RandomX
계산 방식 필	같은 계산을 단순 반복	매번 다른 랜덤 프로그램 실행
요한 메모리	거의 없음	약 2GB
유리한 장비	ASIC 전용 칩 사실상 0	일반 CPU
노트북으로?	원	채굴 가능

왜 CPU가 유리할까?

RandomX는 CPU의 캐시·분기 예측·메모리를 골고루 쓰도록 설계됨 → 전용 칩 을 만들어도 결국 CPU와 비슷해져서 이득 이 작음

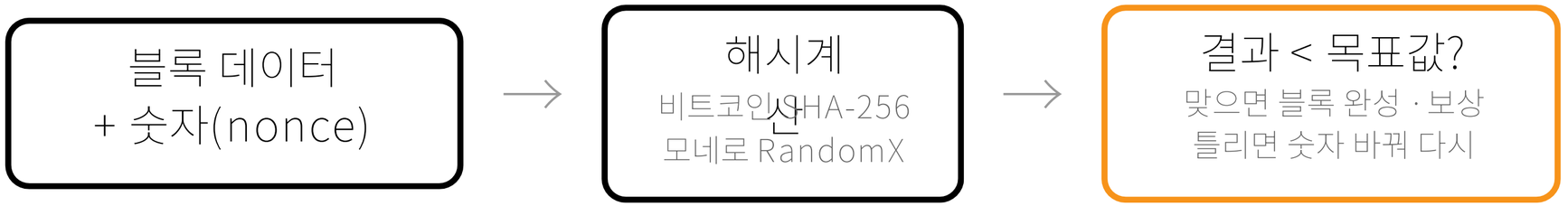
일부러 이렇게 만듦

모네로는 채굴이ASIC공장에 몰리지 않게 2019년 RandomX로 바꿈

내 노트북 실측: 약 2,200 H/s · CPU 10스레드 · 메모리 2,336MB 사용

두번째

원리가 비트코인과 똑같다



둘 다 작업증명(PoW): 조건에 맞는 숫자를 찾을 때까지 계속 계산하는 방식

	비트코인	모네로
블록 간격	약 10분	약 2분
블록 보상	3.125 BTC	0.6 XMR

→ 계산하는 함수만 다르고 채굴 과정은 그대로 비트코인 채굴 체험으로 충분!

세번째

결과를 바로 확인할 수 있다

혼자캐면? 복권

네트워크 전체6.16 GH/s 중 내 몫은 2,200 H/s

→ 블록 1개 찾는 데 평균 약 10년

마이닝 풀에 붙으면

풀이쉬운 문제(셰어)를주고, 푼 만큼 기여를 인정

→ 블록을 못 찾아도 잔고가 조금씩 쌓임

화면으로 바로 보임

터미널에accepted가뜰 때마다 셰어 인정

풀 대시보드에서 내 잔고 확인

POOL		SOLO
Hash Rate	0 H/s	Hash Rate
Average Hash Rate	0 H/s | 0 H/s | 0 H/s | 0 H/s	Average Hash Rate
Current Effort	0.01%	Current Effort
30s Share Rate	0	30s Share Rate
Total Hashes	122 480 000	Total Hashes
Total Shares	1 580 | 0 | 17	Total Shares
Last Share	3 days ago	Last Share
		Expected Block Time

XMR / XTM	XMR	BTC	USD	EUR
Pool Maturing	0	0	0	0
Solo Maturing	0	0	0	0
Confirmed Balance	0.0001008	0.00000078	0.06	0.05
Total Paid	0	0	0	0
Daily Paid	0	0	0	0
Daily Credited	0	0	0	0

HashVault 풀 대시보드 (2026-11-02)

내 결과: 셰어 1,580개 인정 · 확정 잔고 0.0001008 XMR

환경 구성

환경 구성

노트북CPU	ASUS TUF Gaming A14
RAM 채굴	AMD Ryzen 7 260 (8코어 16스레드)
에 사용 전	32GB LPDDR5X
력(실측)	CPU 10스레드
	약 38W

윈도우용 XMRig는 Defender가 트로이목마로 차단
→ 그래서 WSL(리눅스)에서 실행

소프트웨어

Windows 11

↓

WSL (Ubuntu)

↓

XMRig 6.26
채굴프로그램 · 알고리즘 rx/0 (RandomX)

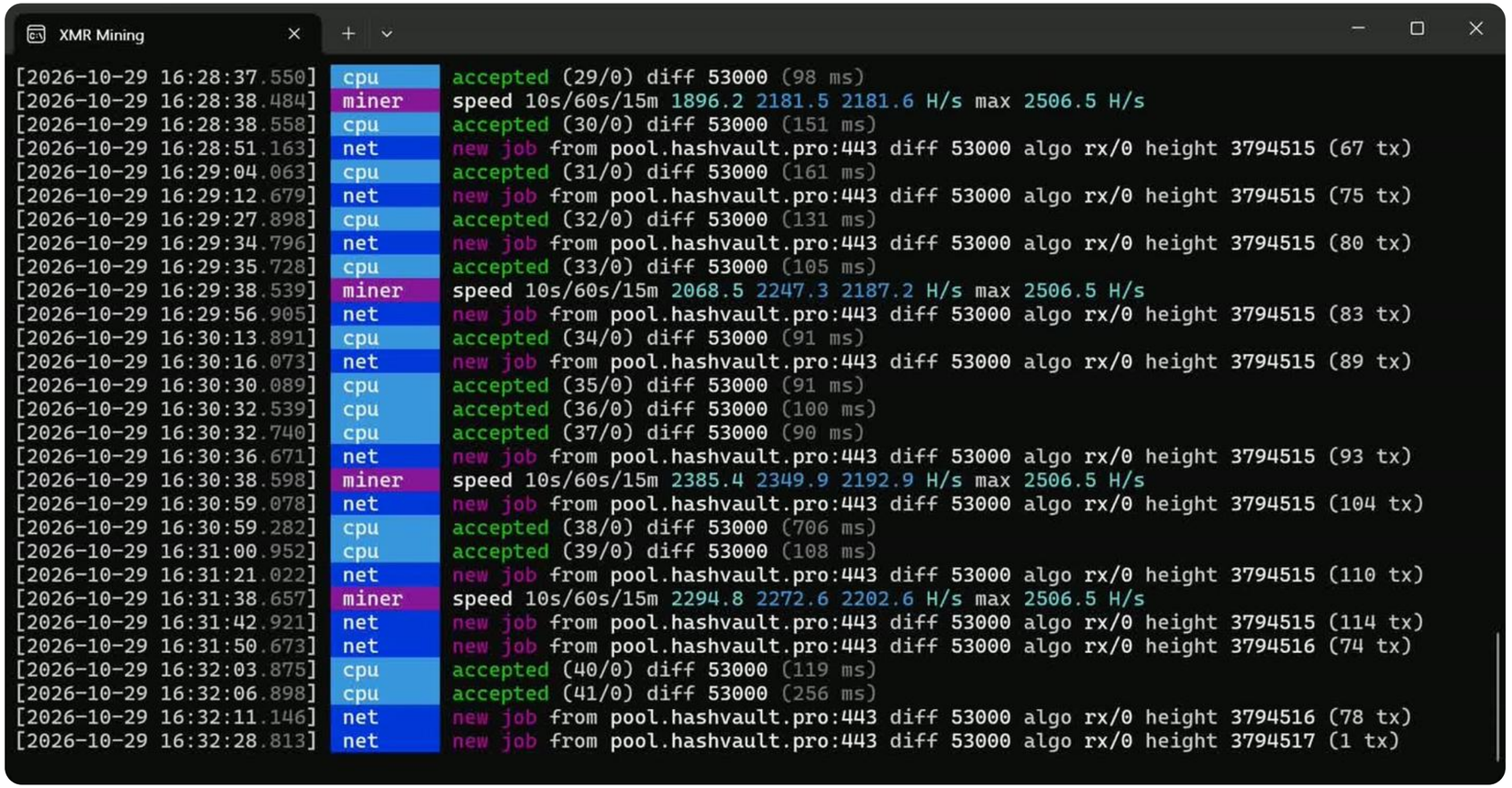
↓

HashVault 마이닝 풀
pool.hashvault.pro

↓

내 모네로 지갑

채굴한 영상



2026-10-29 노트북에서 직접 녹화한 XMRig 화면

accepted

풀이 내계산결과(셰어)를 인정했다는 뜻

≈ 2,200 H/s

1초에 해시약 2,200번
ASIC은 1초에 수백조 번

rx/0

모네로용 RandomX 알고리즘

이만큼 벌었다

POOL		SOLO
Hash Rate	0 H/s	Hash Rate
Average Hash Rate	0 H/s | 0 H/s | 0 H/s | 0 H/s	Average Hash Rate
Current Effort	0.01%	Current Effort
30s Share Rate	0	30s Share Rate
Total Hashes	122 480 000	Total Hashes
Total Shares	1 580 | 0 | 17	Total Shares
Last Share	3 days ago	Last Share
		Expected Block Time

XMR XTM

	XMR	BTC	USD	EUR
Pool Maturing	0	0	0	0
Solo Maturing	0	0	0	0
Confirmed Balance	0.0001008	0.00000078	0.06	0.05
Total Paid	0	0	0	0
Daily Paid	0	0	0	0
Daily Credited	0	0	0	0

HashVault 풀 대시보드 (2026-11-02)

확정 잔고

0.0001008 XMR

≈ $0.06 ≈ 약 90원

총 해시 1억 2,248만 번

인정받은 셰어 1,580개

실제 지갑 입금 0원

전기세 비용 계산

① 채굴 시간 1억 2,248만해시 ÷ 2,200 H/s ≈ 55,700초 ≈ 15.5시간

② 사용 전력량 38W × 15.5시간 ≈ 0.59 kWh

③ 전기세 0.59 kWh × 214.6원 ≈ 약 126원

그래서 손해봄

번 돈
약 90원

−

전기세
약 126원

=

손익
−36원

근데 그 90원도 못 뺌 (최소 출금 0.11 XMR)
→ 실제로 손에 쥔 돈 0원, 실제 손익 −126원

0.11 XMR 모으려면? 이 속도로 약 1만 7천 시간(≈ 2년) 쉬지 않고 돌려야 함
그동안 전기세 약 13.8만 원 vs 받는 돈 약 9.7만 원

돈 벌려다가 손해봤으니까 님들은 하지마세요

- 노트북 채굴 = 전기세 내고 하는 체험판
- 15시간 넘게 CPU 혹사 → 발열·소음은 덤



마무리

1. 비트코인 채굴 = 조건에 맞는 숫자 찾기 경쟁 → ASIC 아니면 못 이김 2.

그래서 CPU로 캘 수 있는 모네로를 노트북으로 약 15.5시간 채굴 3. 결과:

약 90원 벌고(출금 불가) 전기세 약 126원 → 손해

모자란 발표 들어주셔서 감사합니다!



