# 0917 블록체인밸리

## 마이닝 풀로 자금 세탁을..

보안팀 8기 육은서

# 시나리오 개요

## 아래 상황에서 어떻게 깨끗한 돈으로 탈바꿈 할 것인가..

- 스캐밍으로 100BTC 탈취
- Flagged 지갑 및 자금 세탁 필요성
- 목표 : 실물자산 통합 -> 강남 건물..

# Mixer

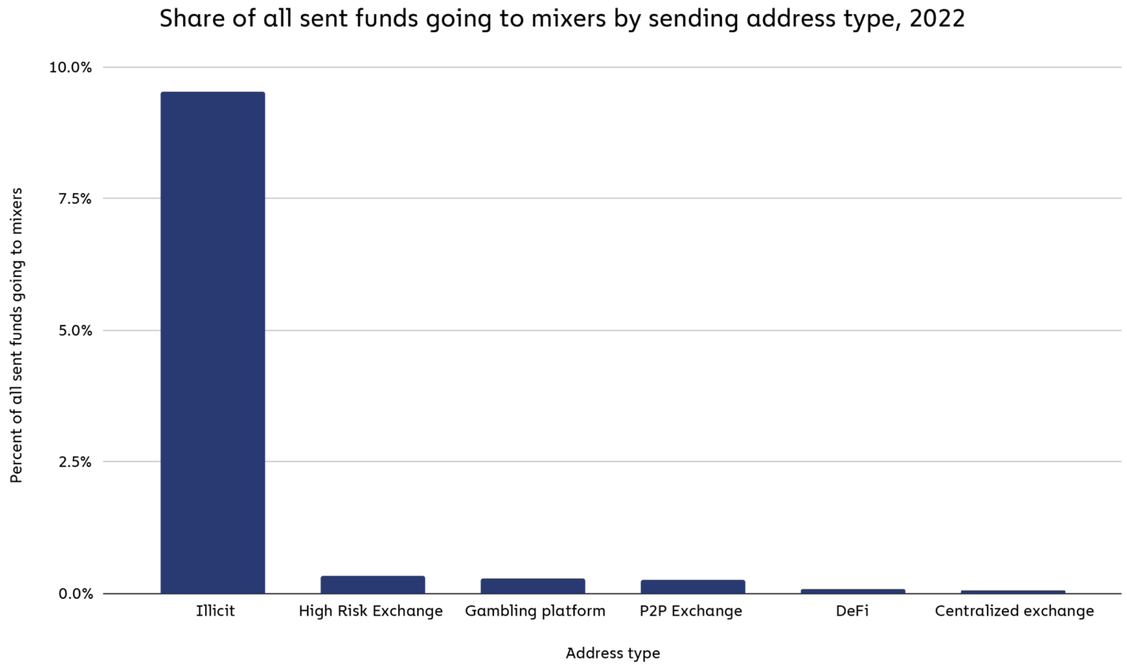
거래 기록을 복잡하게 만드는 서비스,
암호화폐를 하나의 풀에 모아 섞고 분산

1. 목적이 확실한 단순 서비스
2. 온체인 소프트웨어

AML, CFT 관점에서 중요하게 감시

Ex.. 미국은 FinCEN 등록을 의무화한다거나.. 형사 처벌이 있다거나.. 서버 압수가 있다거나..

아무튼 선례가 많다 -> 비약적이긴 하지만 디팩토 다수 존재한다는 건 표준화가 쉽다



AML, CFT 관점에서 중요하게 감시

AML 우회하기 좋은 거..

Ex.. 미국은 FinCEN 등록을 의무화한다거나.. 형사 처벌이 있다거나.. 서버 압수가 있다거나..

아무튼 선례가 많다 -> 비약적이긴 하지만 디팩토 다수 존재한다는 건 표준화가 쉽다 표준 만들기 어려운 거..

사실 믹서는 누가 발표를 할 거 같았음

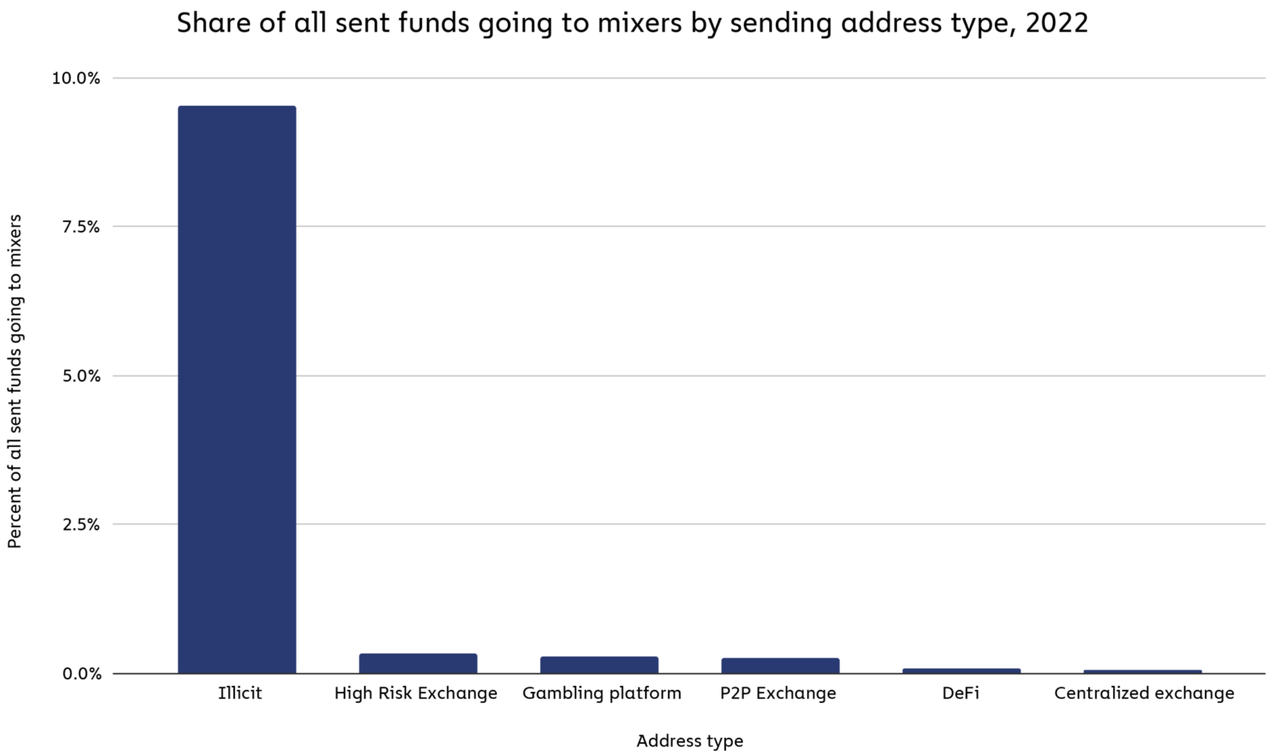
# Mixer

거래 기록을 복잡하게 만드는 서비스,
암호화폐를 하나의 풀에 모아 섞고 분산

여러가지 목적이 혼용되어 있다면

1. 목적이 확실한 단순 서비스
2. 온체인 소프트웨어

인프라나 여러가지 따져야 할 게 많은 거..



# Mining?

...

# Mining pool 세탁 구조

## Placement

Intermediary wallet 여러 개 거쳐서 mining pool로

## Layering

채굴이 되면 보상을 해야 하니까

Coinbase tx 생성 -> pool에 있는 자금 혼합 -> Payout을 여러 새로운 주소로 분배

## Integration

Coinbase tx -> 자금 출처가 새로 채굴된 코인인 것처럼(합법인 것처럼) 위장

# Mining pool 세탁 구조

## Placement

Intermediary wallet 여러 개 거쳐서 mining pool로

Pool 자체의 특징으로 추적 어려워질 수도.. ZKP나 P2P
직접 pool 참여하는 게 아니고 클라우드 마이닝 서비스 활용도 가능

어렵긴 한데 마이닝 풀 운영자가 조력자라면
멤풀에서 트랜잭션 조작해서 채굴

## Layering

채굴이 되면 보상을 해야 하니까

채굴 조건 맞추기 위한 가짜 신원으로 계정 생성하여 위장

Coinbase tx 생성 -> pool에 있는 자금 혼합 -> Payout을 여러 새로운 주소로 분배

## Integration

Coinbase tx -> 자금 출처가 새로 채굴된 코인인 것처럼(합법인 것처럼) 위장

이후 디파이로 빼버리고 swap해서 flashloan등으로 탈바꿈하는 방법도

Shell company 만들어서 빼기

# Mining pool 세탁 구조

## Placement

Intermediary wallet 여러 개 거쳐서 mining pool로

## Layering

채굴이 되면 보상을 해야 하니까

Coinbase tx 생성 -> pool에 있는 자금 혼합 -> Payout을 여러 새로운 주소로 분배

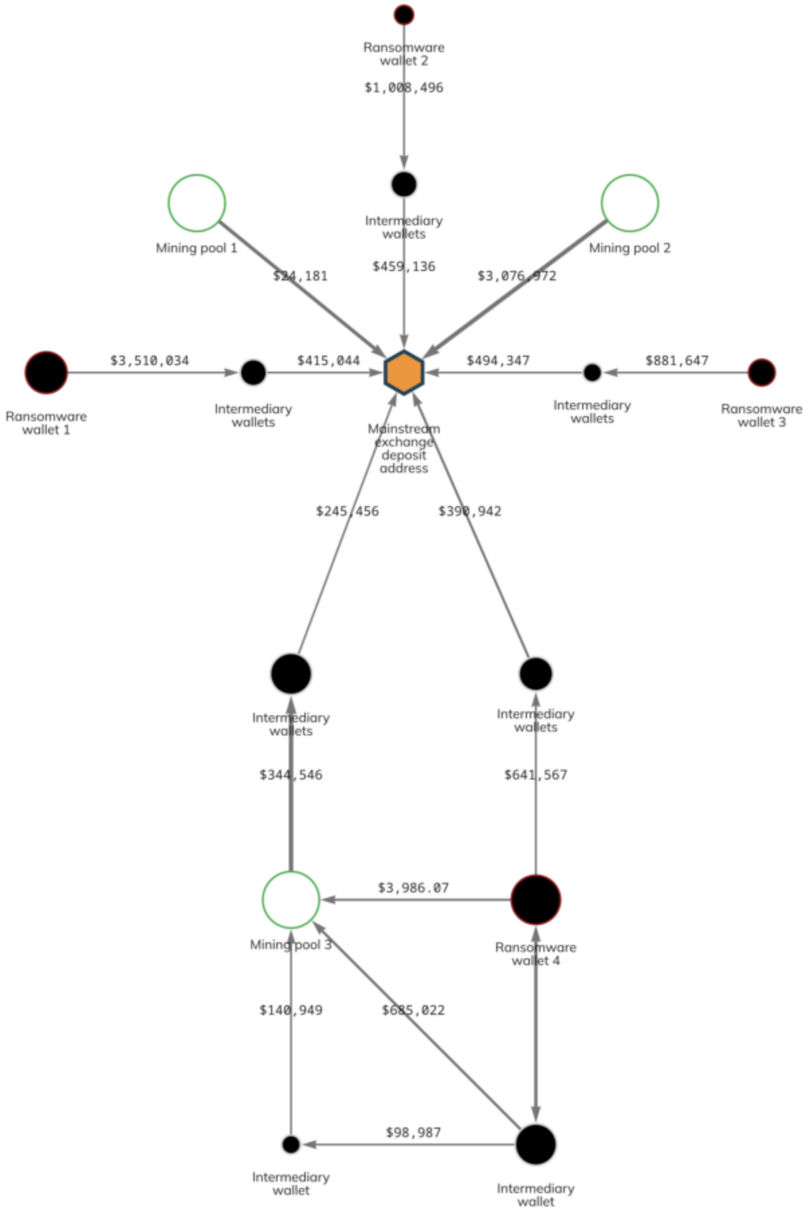
## Integration

Coinbase tx -> 자금 출처가 새로 채굴된 코인인 것처럼(합법인 것처럼) 위장

랜섬웨어 수익을 이렇게 자금 세탁한다는 chainalysis 보고서 (물론 mixer보다 까다로움)

예를 들어, 비공개 주류 거래소의 "매우 활동적인" 암호화폐 지갑은 일상적으로 "랜섬웨어와 관련된 채굴 풀과 지갑 모두에서 상당한 자금을 받는다"고 보고서는 말한다. 이 주소에 예치된 9,420만 달러 중 1,910만 달러는 랜섬웨어 행위자와 관련된 주소에서, 1,410만 달러는 채굴 풀에서 입금되었습니다.

랜섬웨어 행위자들은 또한 중개 지갑이라고 불리는 별도의 주소를 사용하여 자금 흐름을 더욱 난독화하기 위해 채굴 풀로 돈을 보냅니다. "이 시나리오에서 채굴 풀은 자금의 출처를 난독하게 하고 자금이 랜섬웨어가 아닌 채굴 수익금이라는 환상을 만들어낸다는 점에서 믹서와 유사하게 작용한다"고 보고서는 말했다

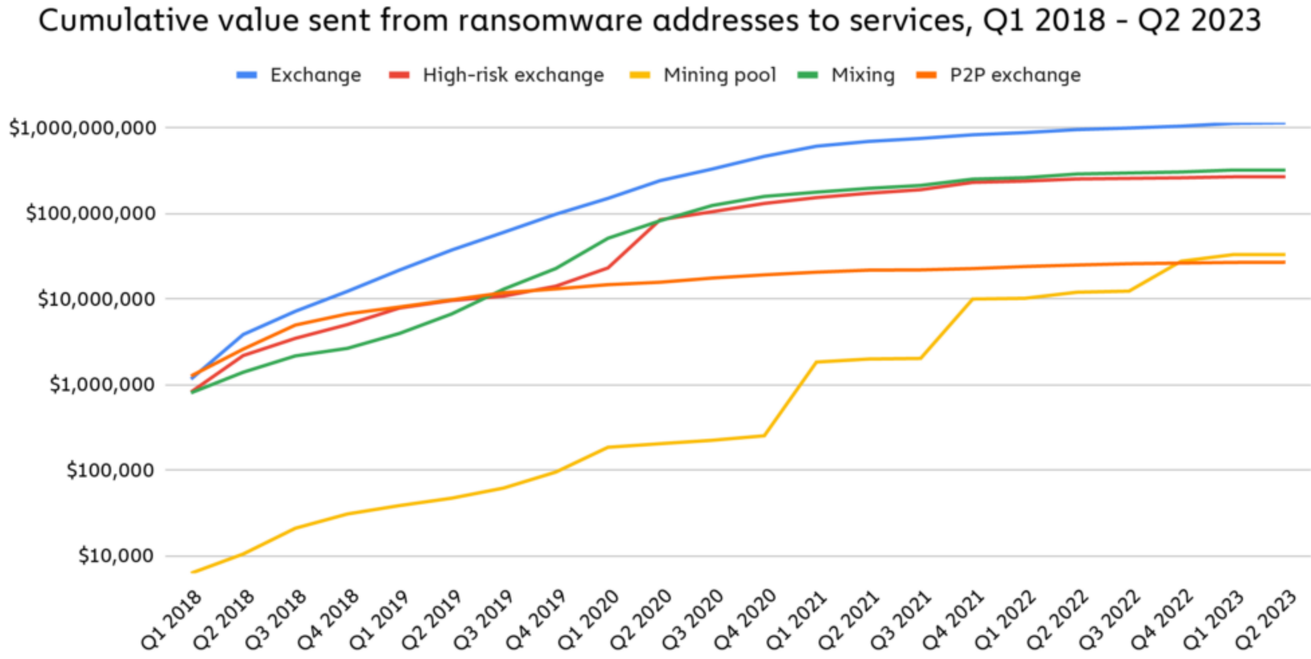



# ng pool 세탁 구조

서 m

자금

채굴




https://www.chainalysis.com/blog/cryptocurrency-mining-pools-money-laundering/

© Chainalysis

라는 chainalysis 보고서 (물론 mixer보다 까다로움)

틴 채굴 풀과 지갑 모두에서 상당한 자금을 받는다"고 보고서는 말한다. 이 주소에 예치된 9,420만 달러 중 1,910만 달러는 랜섬웨어 행위자와 관련

화하기 위해 채굴 풀로 돈을 보냅니다. "이 시나리오에서 채굴 풀은 자금의 출처를 난독하게 하고 자금이 랜섬웨어가 아닌 채굴 수익금이라는 환상을

# Mining pool에 대한 제안..

1. 채굴 서비스에 대한 필터링
2. KYT : transaction 추적
3. 고위험 풀 식별 -> 현재는 거의 이것만 대응하고 있는듯?

# Mining pool에 대한 제안..

1. 채굴 서비스에 대한 필터링
2. KYT : transaction 추적
3. 고위험 풀 식별 -> 현재는 거의 이것만 대응하고 있는듯?

그치만 고위험 풀이 아닌 정상 풀에서도 이와 같은 자금 세탁이 충분히 이루어지는데..

-> 풀에 관련한 규제 + 트랜잭션 관련한 규제 둘 다 필요

# Mining pool에 대한 제안..

1. 채굴 서비스에 대한 필터링
2. KYT : transaction 추적
3. 고위험 풀 식별 -> 현재는 거의 이것만 대응하고 있는듯?

그치만 고위험 풀이 아닌 정상 풀에서도 이와 같은 자금 세탁이 충분히 이루어지는데..

-> 풀에 관련한 규제 + 트랜잭션 관련한 규제 둘 다 필요

# Mining pool 세탁 구조

## Placement

Intermediary wallet 여러 개 거쳐서 mining pool로

Pool 자체의 특징으로 추적 어려워질 수도.. ZKP나 P2P
직접 pool 참여하는 게 아니고 클라우드 마이닝 서비스 활용도 가능

어렵긴 한데 마이닝 풀 운영자가 조력자라면
멤풀에서 트랜잭션 조작해서 채굴

## Layering

채굴이 되면 보상을 해야 하니까

채굴 조건 맞추기 위한 가짜 신원으로 계정 생성하여 위장

Coinbase tx 생성 -> pool에 있는 자금 혼합 -> Payout을 여러 새로운 주소로 분배

## Integration

Coinbase tx -> 자금 출처가 새로 채굴된 코인인 것처럼(합법인 것처럼) 위장

이후 디파이로 빼버리고 swap해서 flashloan등으로 탈바꿈하는 방법도

Shell company 만들어서 빼기

# Mining pool 세탁 구조

이에 대한 backdoor는 합법적?

VASP는 누구로 해야하는지

Pool 자체의 특징으로 추적 어려워짐 수도 ZKP나 P2P

이러면 각 업체의 귀책? 비율을 어떻게 나눠야 하는지

직접 pool 참여하는 게 아니고 클라우드 마이닝 서비스 활용도 가능

여기에 대한 EDD

## Placement

Intermediary wallet 여러 개 거쳐서 mining pool로

어렵긴 한데 마이닝 풀 운영자가 조력자라면

멤풀에서 트랜잭션 조작해서 채굴

Mempool 조작을 어떻게 입증?

## Layering

채굴이 되면 보상을 해야 하니까

채굴 조건 맞추기 위한 가짜 신원으로 KYC를 어떻게 구성해야하는가

Coinbase tx 생성 -> pool에 있는 자금 혼합 -> Payout을 여러 새로운 주소로 분배

## Integration

Coinbase tx -> 자금 출처가 새로 채굴된 코인인 것처럼(합법인 것처럼) 위장

이후 디파이로 빼버리고 swap해서 flashloan등으로 탈바꿈하는 방법도

Shell company 만들어서 빼기