Covert Channel

https://www.youtube.com/watch?v=pmTZyHiWa70

은닉 통신(Covert Communication)

- 은닉 통신
  - 수신자와 송신자와의 관계를 보호하기 위한 통신
  - 비밀 통신이 개시된 사실을 숨김으로써 목적 달성

- 안전한 은닉 통신(스테가노그래피 + 크립토그래피)
  - 크립토그래피 : 통신되는 메시지의 기밀성
  - 스테가노그래피 : 암호화된 통신의 유무

은닉 채널(Covert Channel)

- 조건
  - 통신이 진행 중
  - 송신자와 수신자가 접근 가능
  - 높은 확률로 메시지 획득 가능
  - 조작되지 않음

블록체인(Blockchain)

- 암호화폐
  - 비트코인의 내부 메커니즘
  - 계속해서 늘어나는 블록들로 구성된 공개 원장
  - 데이터를 검증하기 위해 중앙화된 제 3자가 필요하지 않음
  - 다수의 노드에 의한 무결성 검증 → 해킹의 어려움
- 활용
  - 스마트 컨트랙트 (이더리움)
  - 사물인터넷
  - 등등

블록체인 & 은닉채널

- 익명성, 채널로의 접근
- 데이터가 교체될 수 없음
  - 불변성
- 데이터가 제거될 수 없음
  - 부인방지

간소화된 블록체인 모델 정의

$$\mathcal{B} = (C, \Sigma, H, \mathsf{Read}, \mathsf{Submit})$$

모델 = (체인, 디지털 서명, 해시 함수, 읽기, 쓰기)

지불 계좌는 한 번만 사용된다.

간소화된 블록체인 모델 요소

1. 지불하는 사람

$$(s_k^{(i)}, p_k^{(i)})$$

2. 수신자 주소

$$a^{(i)} \in \{0,1\}^n$$
$$a^{(i)} = H(p_k^{(i)}$$

3. 지불 금액

$$\mu^{(i)}$$

간소화된 블록체인 모델 요소

4. 블록체인 초기 상태

$$C_0 = \left((a^{(1)}, \mu^{(1)}), (a^{(2)}, \mu^{(2)}), \ldots, (a^{(L)}, \mu^{(L)}) \right)$$

5. 지불

$$P = (p_k^{(i)}, a^{(j)}, \mu, t, \sigma)$$

$$\sigma = \mathsf{Sign}(s_k^{(i)}, (p_k^{(i)}, a^{(j)}, \mu, t))$$

6. 체인 상태

$$C = (C_0, C_1, C_2, \ldots)$$

알고리즘 노테이션

Variable	Explanation
H	hash function
(s_k, p_k)	private and public key pair for the digital signature scheme
$(s_k^{(A)}, p_k^{(A)})$	Alice's keypair
k	secret key for symmetric encryption
λ	message start indicator
n_λ	length of λ
m	hiddentext message
c	$c \leftarrow \mathsf{Enc}(k, m)$
c'	concatenation $c' = \lambda \| c$
N	total number of embedded bits $N = \|c'\|$
$a, a^{(i)}$	address computed by hashing a public key
$\mathcal{H}$	the history of payments Alice has made through the blockchain
$\mathcal{M}_\mathcal{H}$	distribution on the amount of money in Alice's payment conditioned on the history of payments $\mathcal{H}$
μ	payment amount
t	unique payment identifier
σ	digital signature
C, C_i	block in the blockchain
P	payment
L_A	total number of payments made by Alice

알고리즘 (메시지 삽입)

Algorithm 2 Embedding Algorithm

procedure Embed$((k, \lambda), m, \mathcal{B})$
  $c \leftarrow \mathsf{Enc}(k, m)$
  Concatenate $c' = \lambda || c$
  Set $N = |c'|$
  Interpret c' as a bit representation $c'_1 c'_2 \dots c'_N \in \{0,1\}^N$
  $i = 1$
  while $i \leq N$ **do**
    Generate unseen $(s_k, p_k) \leftarrow \mathsf{Gen}_\Sigma(1^s)$
    $a \leftarrow H(p_k^{(i)})$
    Interpret a as a bit representation $a_1 a_2 \dots a_n \in \{0,1\}^n$
    if $a_n = c'_i$ **then**
      $\mu \leftarrow \mathcal{M}_\mathcal{H}$
      Generate a unique identifier t for the payment
      $\sigma \leftarrow \mathsf{Sign}(s_k^{(A)}, (p_k^{(A)}, a, \mu, t))$
      $\mathsf{Submit}(p_k^{(A)}, a, \mu, t, \sigma)$
      Wait for the blockchain to publish a new block
      Update $\mathcal{H}$
      $i \leftarrow i + 1$
    end if
  end while
end procedure

알고리즘 (메시지 추출)

Algorithm 3 Extraction Algorithm

procedure Extract($(\lambda, k), \mathcal{B}$)
  $i = 1$
  $j = 1$
  while have not found λ yet **do**
    $C = \text{Read}(j)$
    if $C = \perp$ **then**
      Wait until a block appears and read it: $C = \text{Read}(j)$
    end if
    for any payment $P \in C$ **do**
      if P is from $p_k^{(A)}$ **then**
        Extract address a from P and get the LSB a_n
        Scan if we have found the entire $\lambda \in \{0,1\}^{n_\lambda}$
      end if
    end for
    $j \leftarrow j + 1$
  end while
  $i = 1$ ▷ Now reading the encrypted hidden message
  while $i \leq N - n_\lambda$ **do**
    $C = \text{Read}(j)$
    if $C = \perp$ **then**
      Wait until a block appears and read it: $C = \text{Read}(j)$
    end if
    for any payment $P \in C$ **do**
      if P is from $p_k^{(A)}$ **then**
        Extract address a from P and get the LSB a_n
        $c_i \leftarrow a_n$
        $i \leftarrow i + 1$
      end if
    end for
    $j \leftarrow j + 1$
  end while
  Compile $c = c_1 c_2 \ldots c_{N-n_\lambda}$
  $m \leftarrow \text{Dec}(k, c)$
  output m
end procedure