Blockchain #8

Attacks on Blockchain

Prof. Byung Il Kwak

Review

- Basics of Ethereum
- Ethereum's consensus

CONTENTS

- Security of Bitcoin

Security of Bitcoin

- 공격 목적
  - 이중 지불 (Double spending)
  - 악의적으로 채굴하여 기본 이상의 보상을 받음
  - 비트코인 네트워크 마비

Technical errors: Programming errors

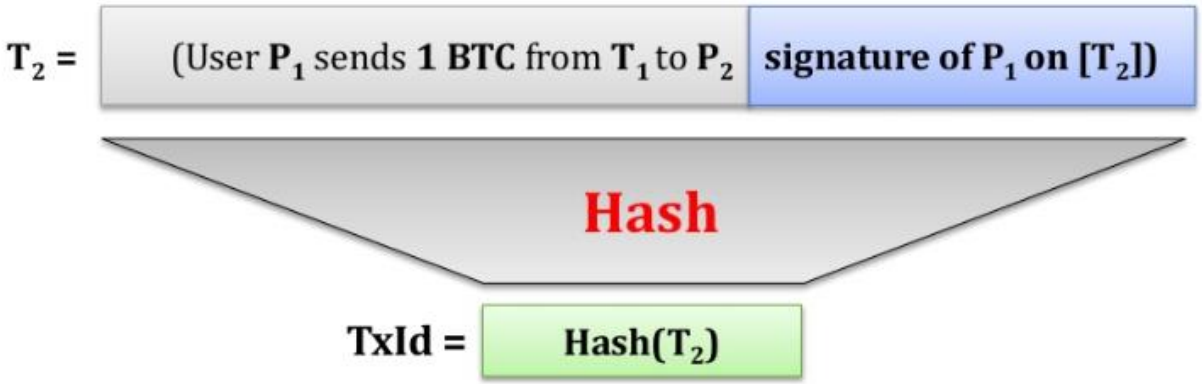
- Block 74638 (2010년 8월), 1,840억 BTC가 넘는 두 가지 출력이 포함된 트랜잭션이 포함됨
  - Bitcoin 소프트웨어의 integer overflow 문제
  - Bitcoin 소프트웨어 업데이트와 “manual fork"로 해결

- Bitcoin 코어의 소프트웨어 업데이트 오류로 인해 블록 225430 (2013년 3월)에서 포크 (6시간 지속, 소프트웨어의 이전 버전으로 되돌리면서 문제 해결)

탈중앙화가 중앙화보다 나은 것인지?

Technical errors: Transaction modification

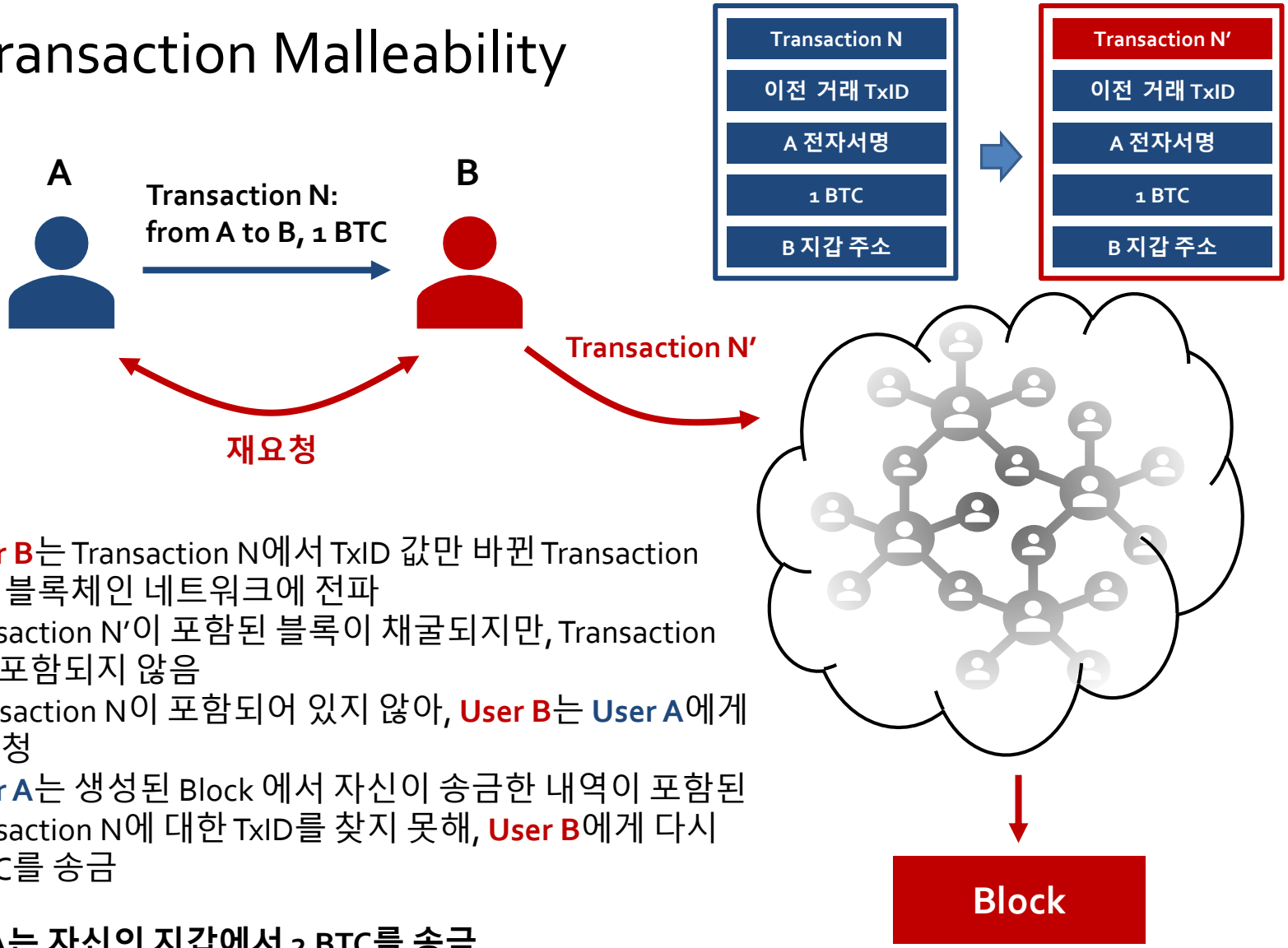
- Transaction Malleability
  - Problem: transactions are identified by their hashes



Hence one can change **TxId** by mauling the signature:

Technical errors: Transaction modification

Transaction Malleability



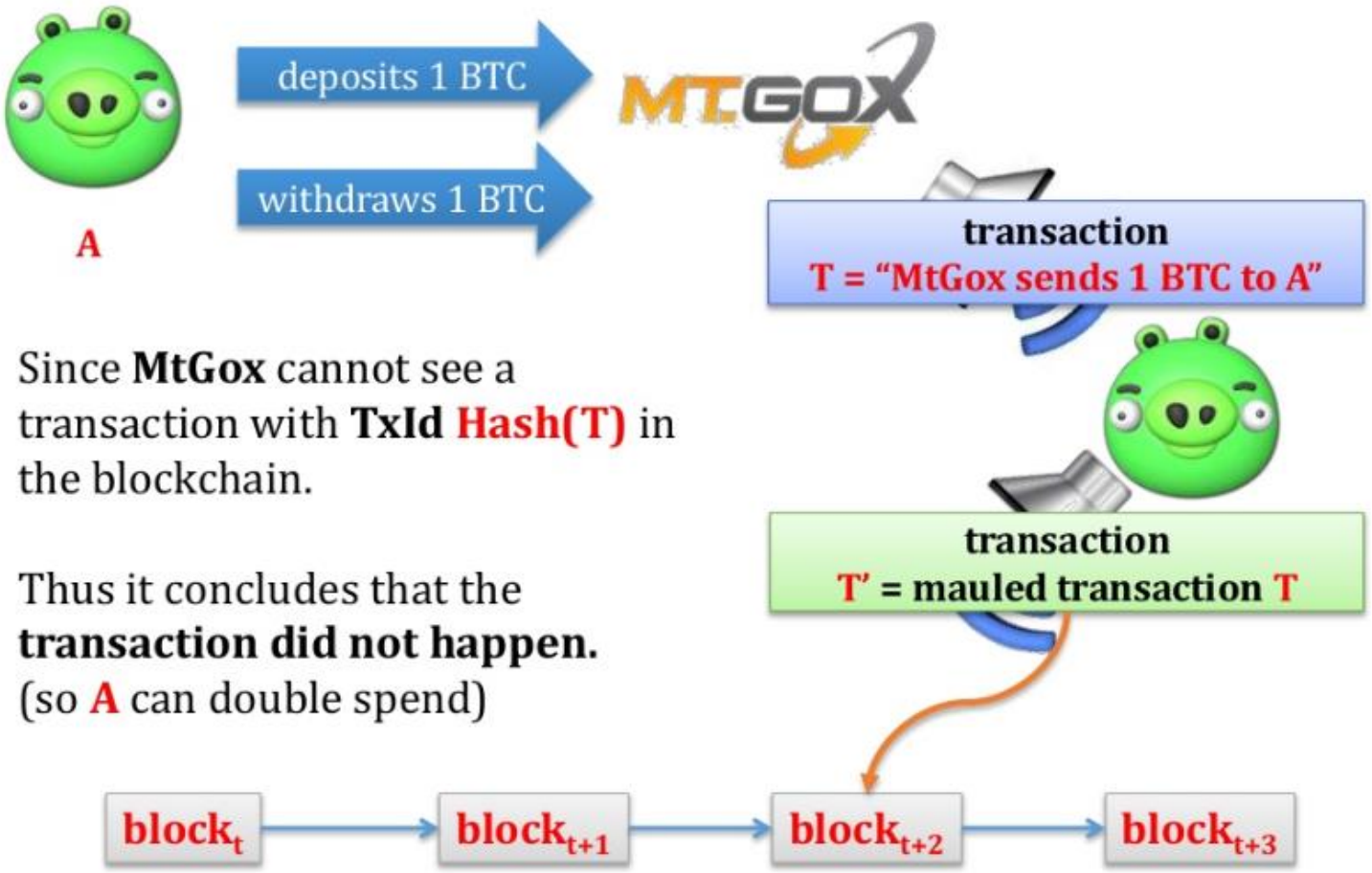
1. **User B**는 Transaction N에서 TxID 값만 바뀐 Transaction N'을 블록체인 네트워크에 전파
2. Transaction N'이 포함된 블록이 채굴되지만, Transaction N은 포함되지 않음
3. Transaction N이 포함되어 있지 않아, **User B**는 **User A**에게 재요청
4. **User A**는 생성된 Block 에서 자신이 송금한 내역이 포함된 Transaction N에 대한 TxID를 찾지 못해, **User B**에게 다시 1 BTC를 송금

**** A는 자신의 지갑에서 2 BTC를 송금**

[Source: https://spectrum.ieee.org/what-you-need-to-know-about-mt-gox-and-the-bitcoin-software-flaw]

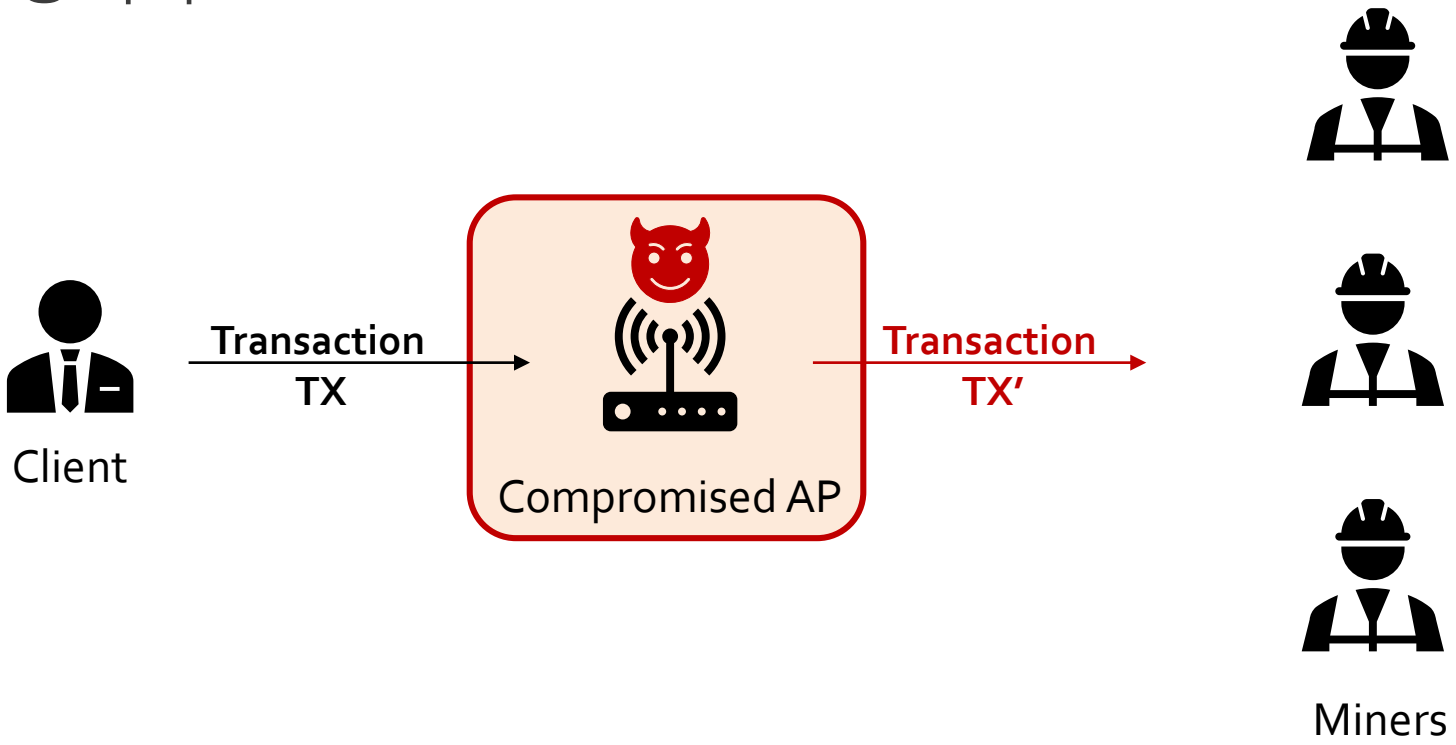
Technical errors: Transaction modification

- ** The clamed attack on MtGox



Technical errors: Transaction modification

- Transaction Malleability
  - 공격자



클라이언트와 마이너 사이의 통신 채널 보호를 위한 보호 장치가 요구됨

Problem: Hardware mining

History of mining:

$$\text{CPU} \rightarrow \text{GPU} \rightarrow \text{FPGA} \rightarrow \text{ASIC}$$

Bitcoin double SHA256 ASIC mining hardware

Product	Advertised Mhash/s	Mhash/J	Mhash/s/$	Watts	Price (USD)	Currently shipping
Achilles Labs AM-850 [1]	850,000	1478	1223	575	695	Discontinued
Achilles Labs AM-1700 [2]	1,700,000	1581	1553	1075	1095	Yes
Achilles Labs AM-3400 [3]	3,400,000	1581	1794	2150	1895	Yes
Achilles Labs AM-6000 [4]	6,000,000	1579	2073	3800	2895	Yes
AntMiner S1 [5]	180,000	500	800	360	299[6]	Discontinued
AntMiner S2 [7]	1,000,000	900	442	1100	2259	Discontinued
AntMiner S3 [8]	441,000	1300	1154	340	382[6]	Yes
AntMiner S4 [9]	2,000,000	1429	1429	1400	1400	Yes

Easier to attack by very powerful adversary!

Problem: Hardware mining

- Hardware mining
  - 채굴자들이 장기적으로 시스템에 대한 안정성을 추구
    - 시스템이 불안정하면 자신들이 작업 증명으로 인한 채굴 수익의 변동성이 커짐..

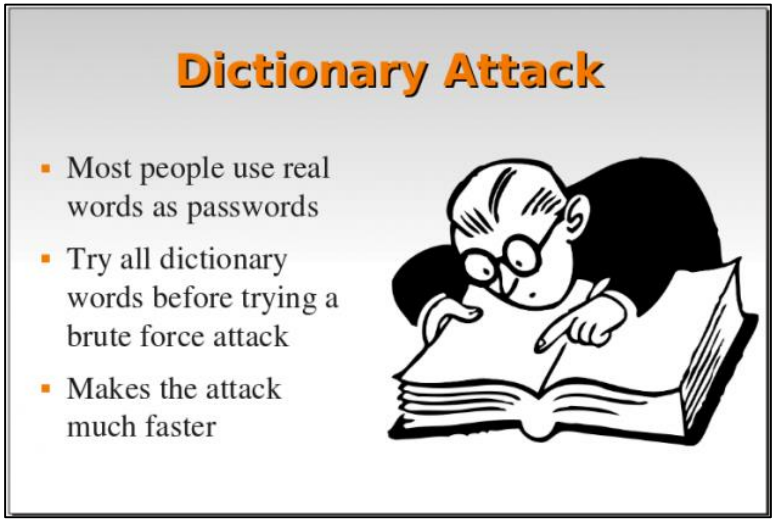
Problem: Lost control

- 개별 광부는 자신이 채굴하는 블록에 대한 통제력이 없음

- 예) Stratum 프로토콜 (마이닝 풀에서 일반적으로 사용)에서 채굴자는 스스로 비트코인 거래를 선택할 수 없음
  - 99%채굴자들은 transaction들 중 어떤 것을 선택하는지에 대해 신경 쓰지 않음.
  - 채굴자들은 가능한 높은 채굴 수익 얻는 것을 목표로 함

Problem: key storage

- 비트코인 저장 방식
  - **PC에 평문으로 저장 => …**
  - 패스워드 암호화 => **Dictionary attacks**
  - 보안 지갑 사용 (e.g., S10's wallet)



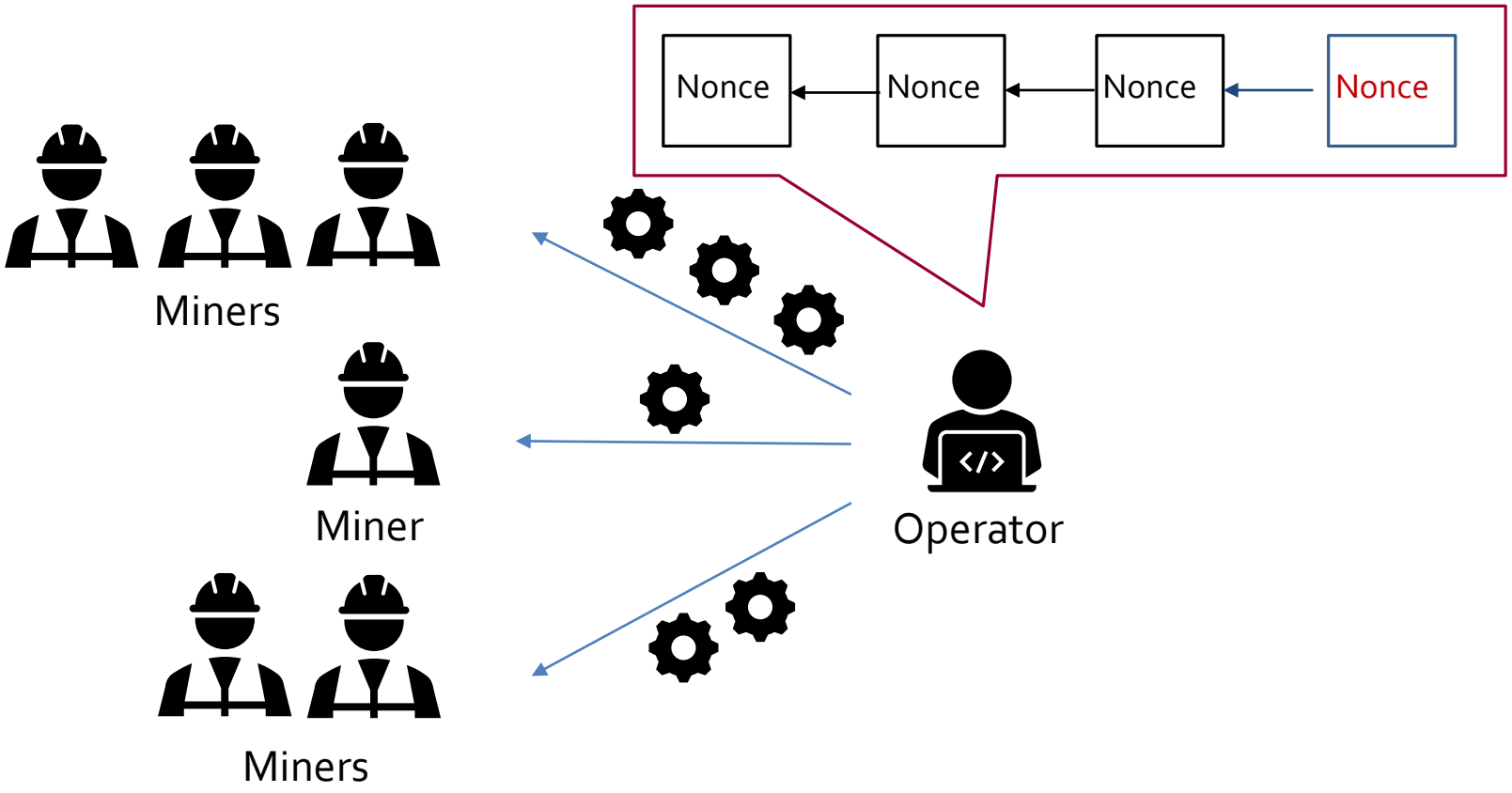
[Source: https://www.news1.kr/articles/?3554385]

CONTENTS

- Attacks on mining pools

Mining pools

- 마이닝 풀은 중앙에서 운영하거나 p2p 방식으로 설계됨

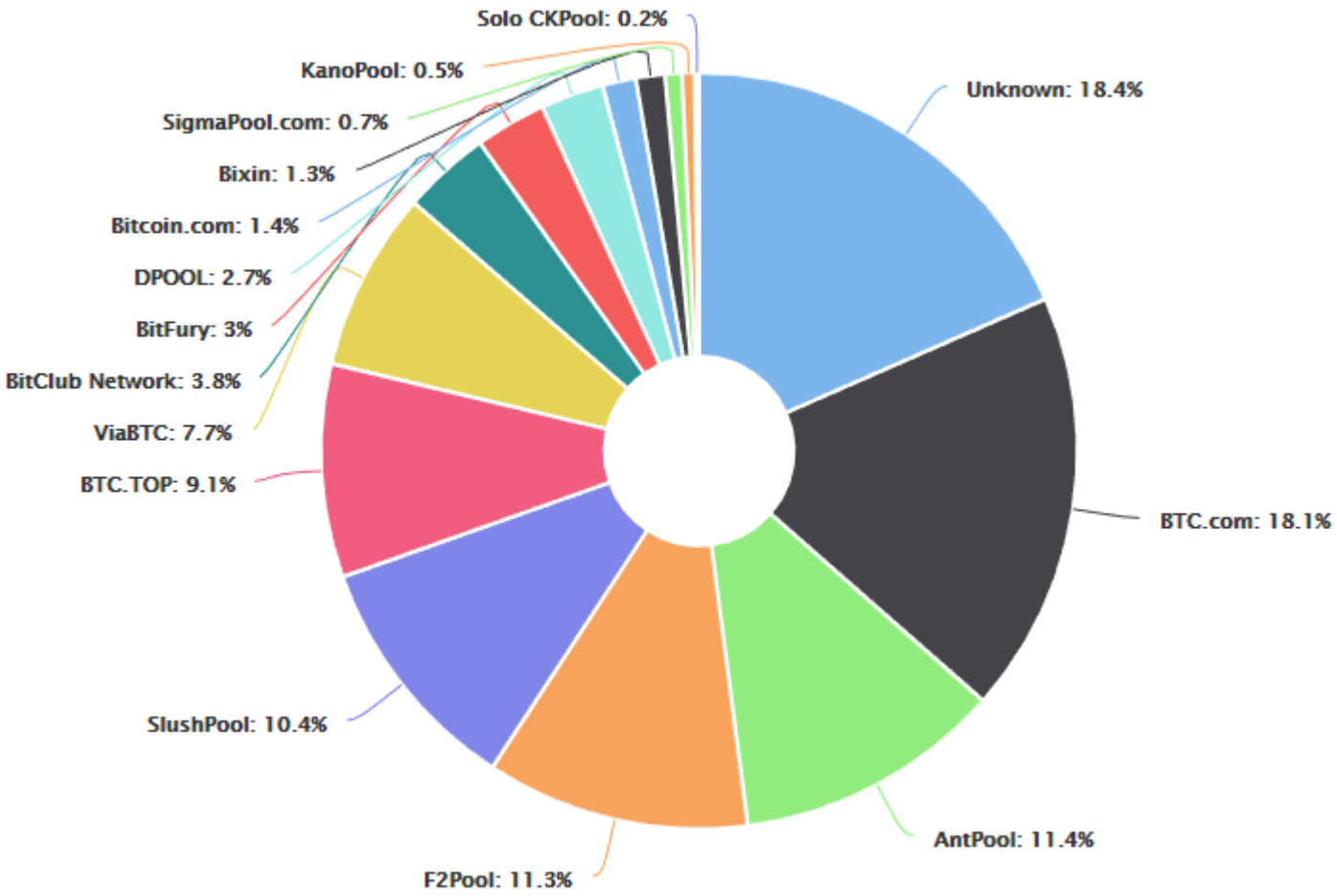


Mining pools

- 일부 마이닝 풀은 서비스 요금을 부과함
  - Mining pool 운영자가 채굴에서 6.25 BTC를 얻은 경우, 해당 mining pool에 참여한 참여자들에게 채굴 보상을 공유
    - 최종 보상 = 채굴 보상 (6.25 BTC) + 거래 수수료 – mining pool 이용 수수료
    - 위의 최종 보상을 참여한 이들의 참여율에 따라 분배
- 즉, mining pool을 통한 수익은 solo mining의 수익보다 약간 낮음.
  - => 솔로 채굴로는 블록 채굴이 어려움 (거의 불가능)

Mining pools

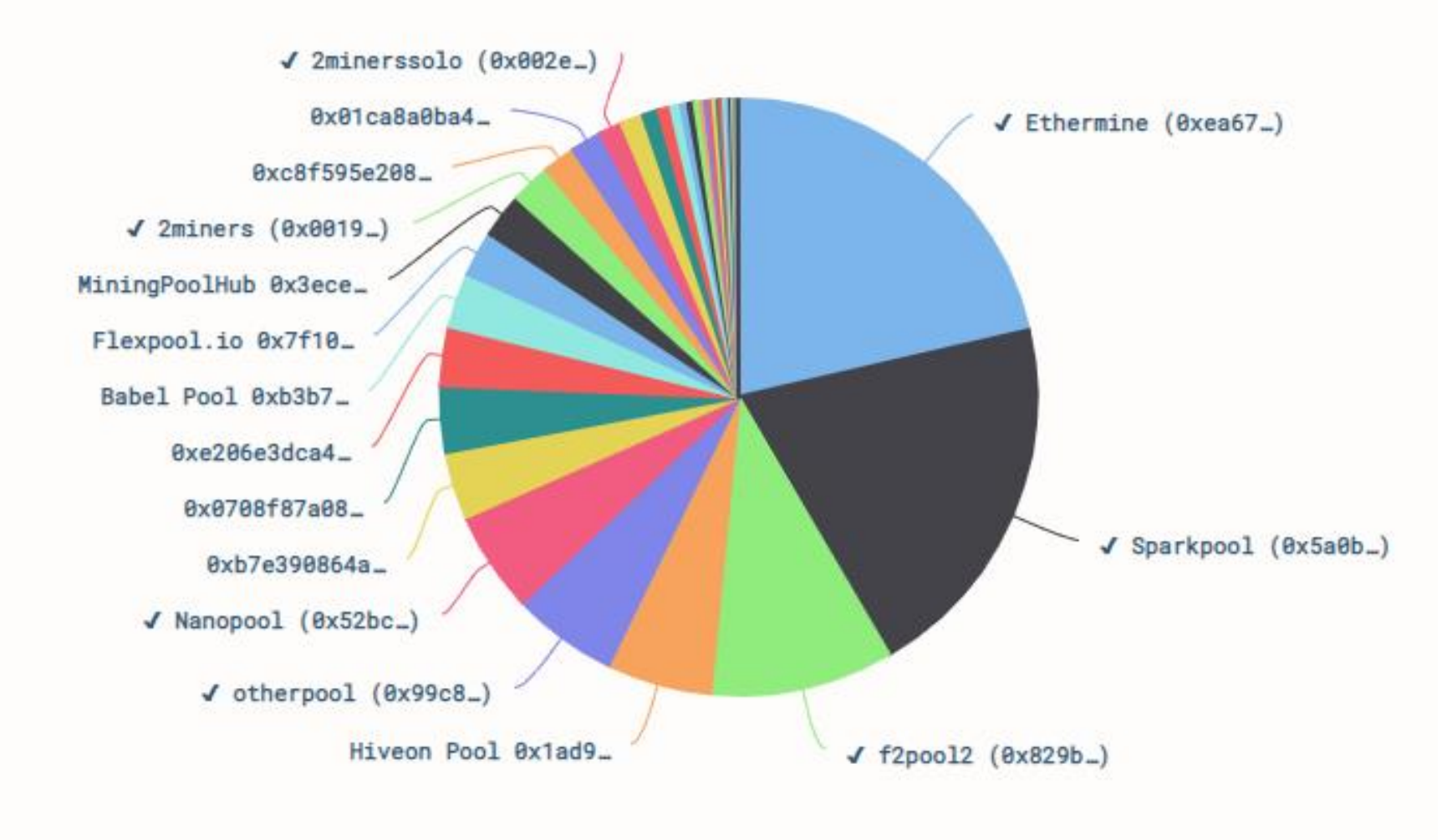
- Bitcoin mining pools



[Source: https://www.blockchain.com/ko/pools]

Mining pools

- Ethereum mining pools

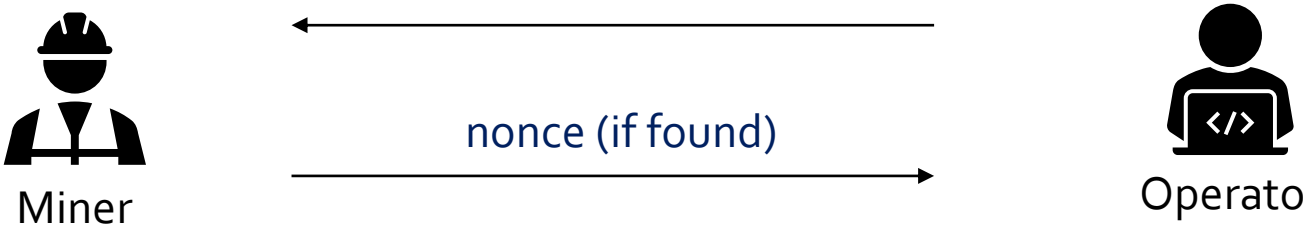


[Source: https://etherchain.org/miner]

Mining pools

- 마이닝풀 디자인

A **list of transactions** (TXs) and the **previous hash** (H_{prev})



Nonce 값 찾기
> H(nonce, H_{prev}, TXs)

Pool 멤버 중 일부가 nonce값을 찾으면 각 멤버들은 자신의 작업에 비례하여 보상을 받음

Problem
- 채굴자가 실제로 얼마나 많은 작업을 수행했는지 확인하는 방법은?

Mining pools

- 마이닝풀 디자인

A **list of transactions** (TXs) and the **previous hash** (H_{prev})

Miner

Nonce 값 찾기
> H(nonce, H_{prev}, TXs)

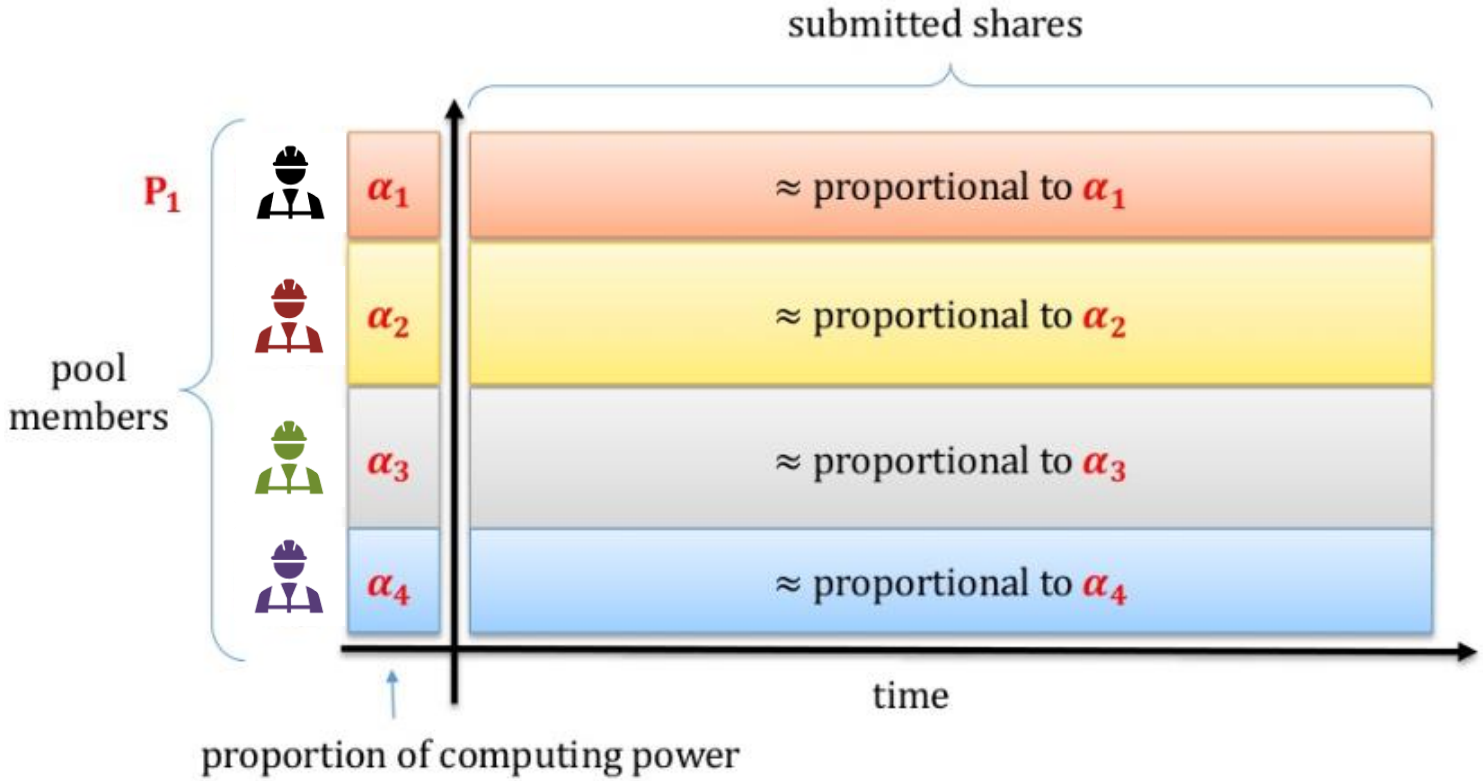
nonce (if found)

Nonce 값을 찾았다면,
H(**nonce**, H_{prev}, TXs) < Target bits
인 hash value 를 Mining pool
운영자에게 전송

Operator

Mining pools

- 채굴자들이 mining pool을 변경하지 않을 경우

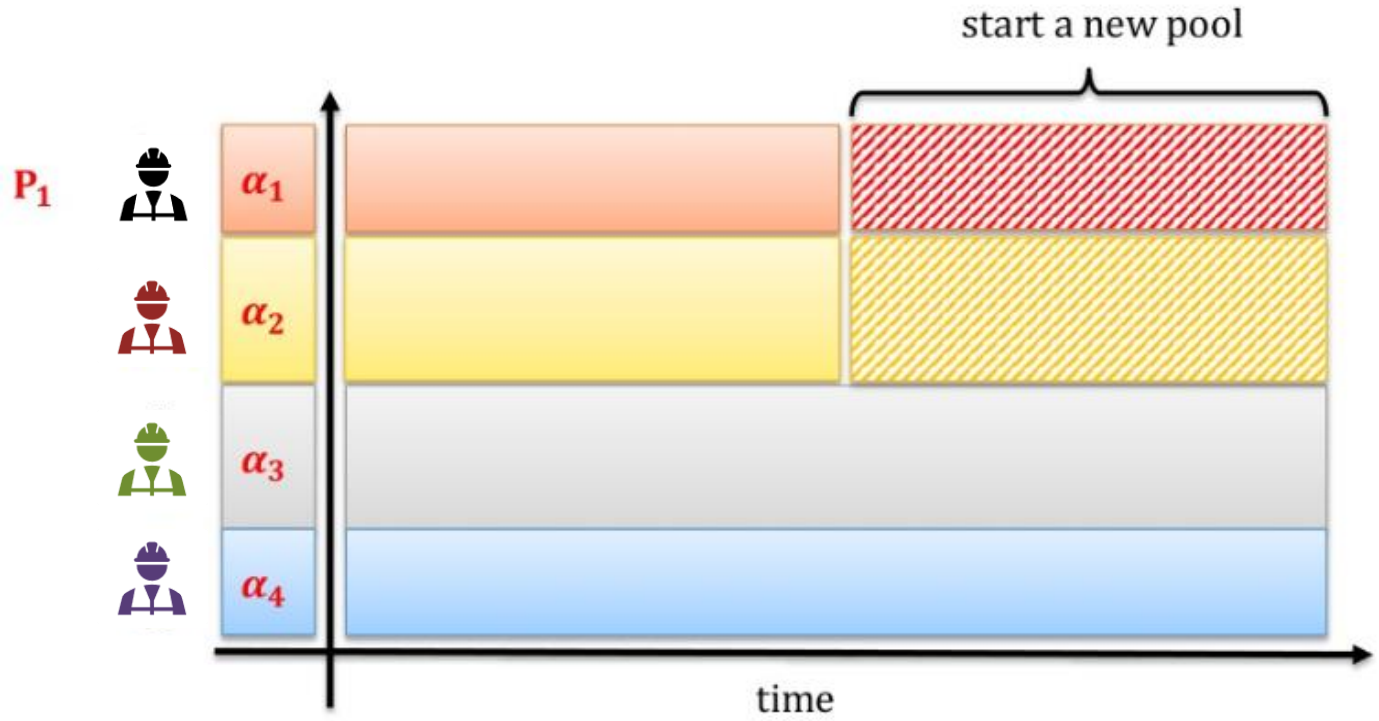


probability of that this pool wins: $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$

reward for P_1 in case it wins: $12.5\ BTC * \frac{\alpha_1}{\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4}$

Mining pools

- 채굴자들이 mining pool을 변경할 경우



Now the expected revenue of P_1 is a sum of

Revenue from the old pool + Revenue from a new pool

Problem: Pool hopping

- Pool hopping 은 총 보상을 늘리기 위해 mining pool을 전환하는 행위를 나타냄
  - Mining pool은 보다 높은 채굴 보상 수수료를 멤버들에게 주기 때문에, 채굴자들이 자신들의 이익을 높이기 위해 여러 mining pool을 옮겨 다니며 이윤을 추구함
  - 한 개 mining pool에서만 채굴을 수행하는 채굴자들은 보다 채굴 수수료를 적게 받음
    - pool hopping을 통한 다수의 채굴자들이 들어오게 되면, 보상 받을 확률이 높지만, 해당 채굴자들이 다른 mining pool로 옮기면 블록 생성에 성공할 확률이 적어지고 결과적으로는 수수료를 받기 어려워 짐

Defense: “Slush’s method”

- 채굴에 참여하는 행위에 대한 점수 **s**를 아래와 같이 설계

- 보상은 점수에 비례하여 할당
  - 시간 할당과 해시 비율을 적용
    - **S = (Time_point)+(Hash_rate_point)**

How to manage mining pools

- Mining pool의 운영자는 채굴자들을 관리하고, 보상 받는 것에 노력을 해야 하므로, 평판상 정직하다고 여김

- **악의적인 채굴자들에 의한 공격**을 피하는 것이 어려움
  - Sabotage
  - Lie-in-wait

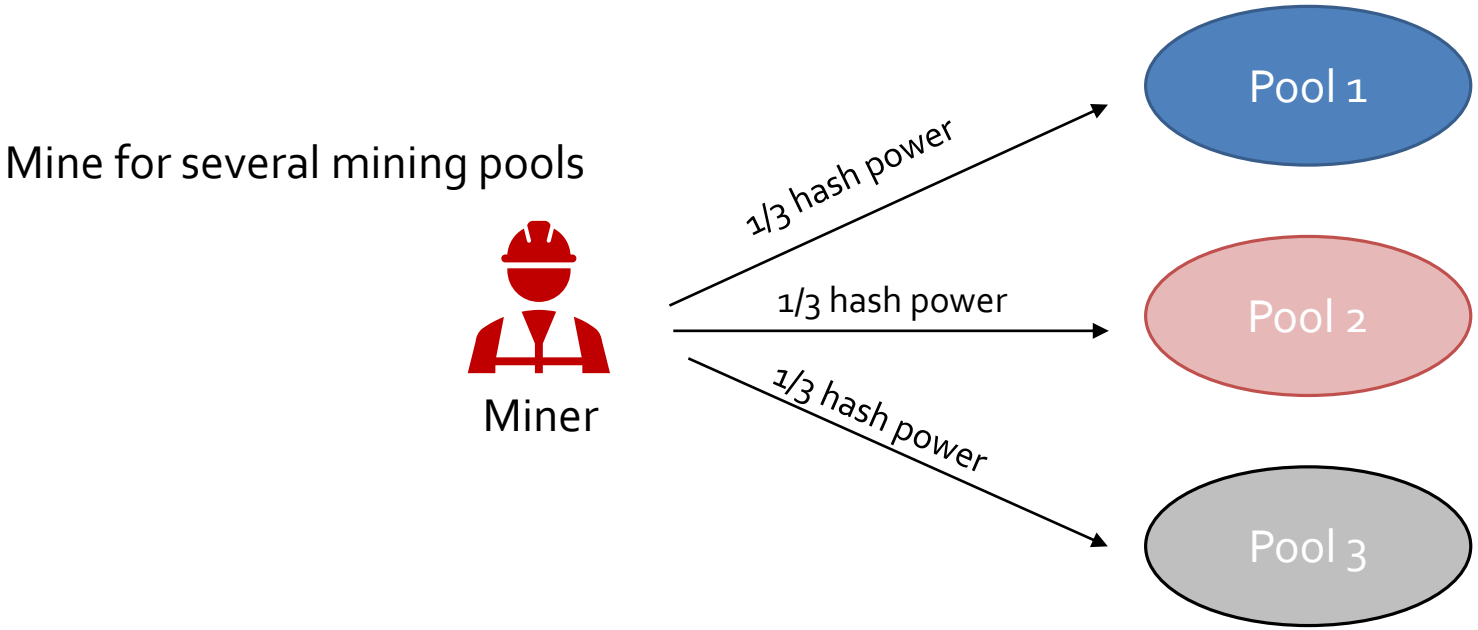
Appendix: Sabotage

Sabotage attacks on mining pools

- 전체 할당된 부분 중 일부만 제출

  - 결과
    - Mining pool은 시간 및 자원을 소모
    - 열심히 채굴하지 못한 채굴 풀은 보상을 받지 못함
  - 공격자의 목표 mining pool의 파산
    - 한편, 공격자는 다른 커다란 mining pool을 소유
  - 2014. 06 에 해당 공격이 mining pool 'Eligius'을 타겟으로 수행되었다는 소문.. (대략적인 손실 금액: 300 BTC)

Lie-in-wait attacks on mining pools

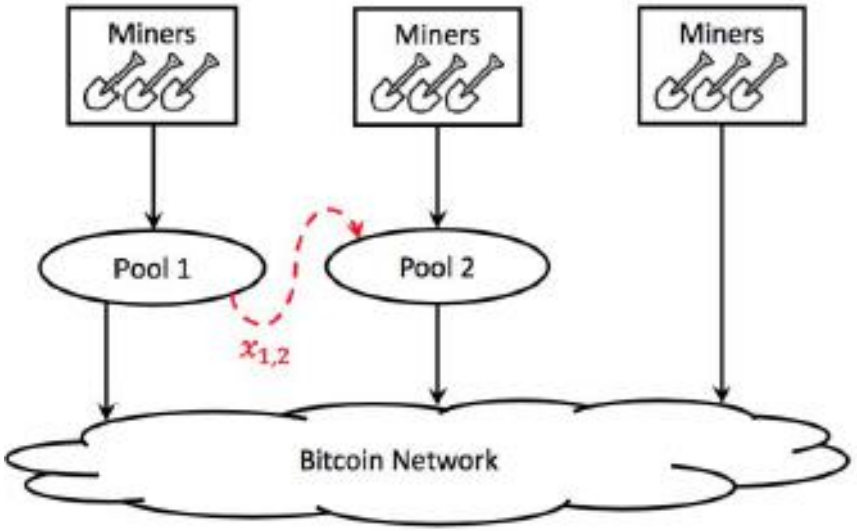


- Mining pool 2에 대한 솔루션을 찾게 될 경우
  - 1. Pool 2의 Operator에게 솔루션 제출 대기
  - 2. Pool 2에서만 채굴 수행 (다른 Mining pool에 있는 자원을 가져와서 채굴에 소비를 많이 한 것처럼 보이게 함)
  - 3. Pool 2의 Operator에게 솔루션 제출 (적정 시간 이후에 솔루션 제출)
- 해당 공격의 현실성 및 수익성이 있음을 나타냄

https://arxiv.org/pdf/1112.4980.pdf

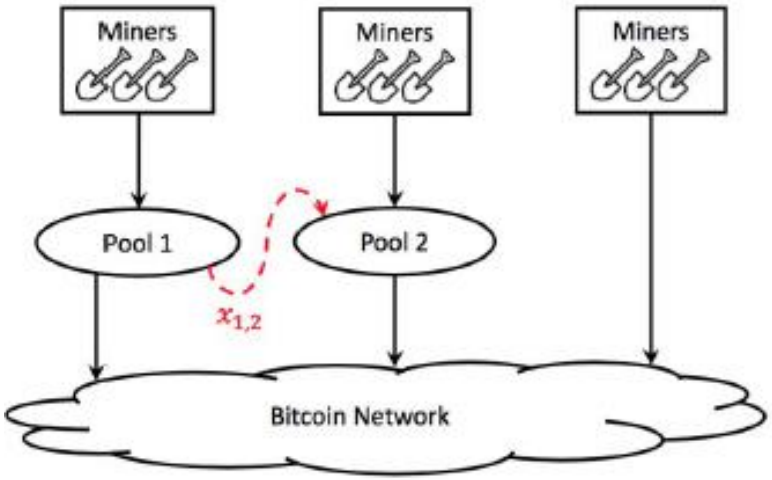
Pool Wars

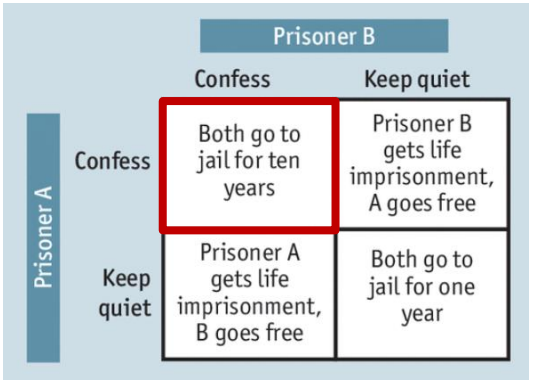
- 공격 결정은 반복적인 게임과 유사
  - A 풀과 B 풀
- 게임의 각 반복은 죄수의 딜레마
  - 공격 or 보류 중 택 1



Pool Wars

- Mining pool A가 mining pool B 를 공격하면, mining pool A는 수익을 얻고 mining pool B는 수익을 잃음
  - Mining pool B는 mining pool A 를 공격하고 더 많은 수익을 얻음으로써 보복할 수 있음
  - 그러므로, '공격' 전략은 매 주기에서의 지배적인 전략
- 풀 A와 풀 B가 서로 공격하는 경우





They will be at a Nash Equilibrium

Pool Wars

- 노 풀 공격은 내쉬 균형이 아님
  - 서로 공격하지 않으면 다른 mining pool을 공격하여 수익을 늘릴 수 있음
- 하지만, 두 mining pool이 서로 공격하지 않기로 동의하면 모두 장기적으로 이익을 얻음
  - 그럼에도 불구하고, 공격자들은 익명으로 다른 mining pool을 공격할 수 있음 (항상 불안정한 상황에 놓임)
- **Mining pool이 공격을 탐지할 수 있다면 장기적으로 mining pool들에게 있어 이득이 됨**

CONTENTS

- Blacklisting

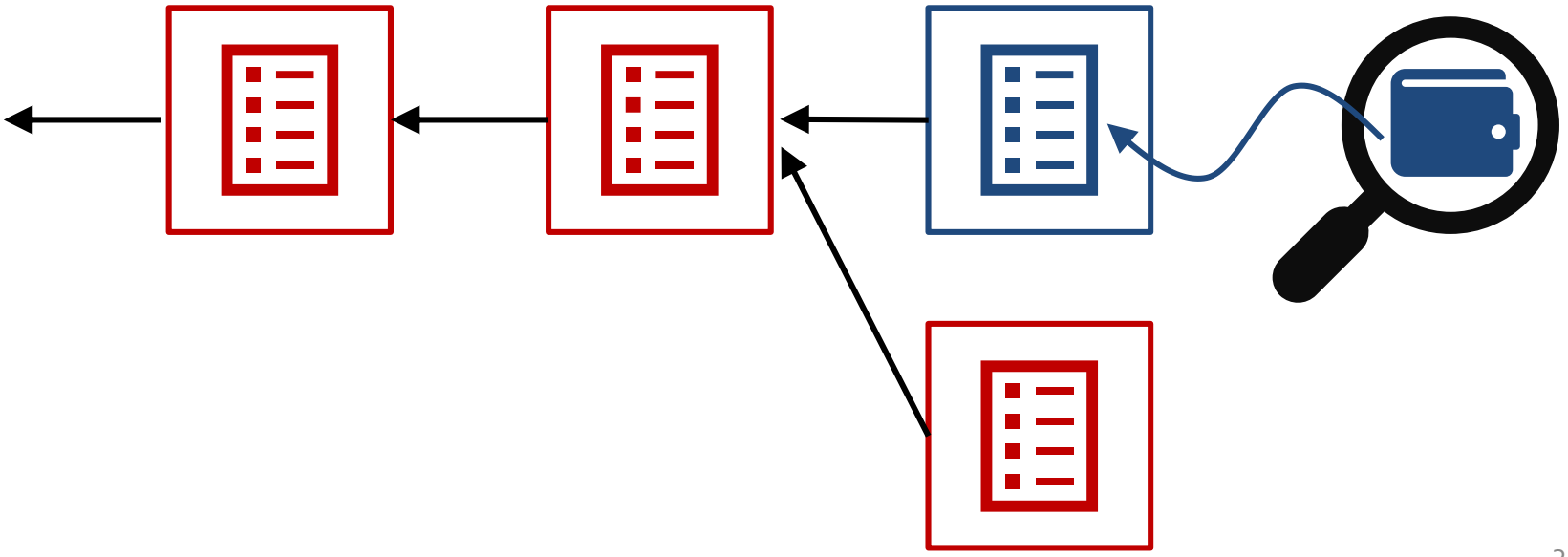
Blacklisting

- 만약, 내가 모든 마이닝 풀을 통제할 수 있다면??

- 목표
  - 특정 사람들이 소유한 비트코인 주소를 검열하고, 해당 비트코인을 사용하지 못하도록 함

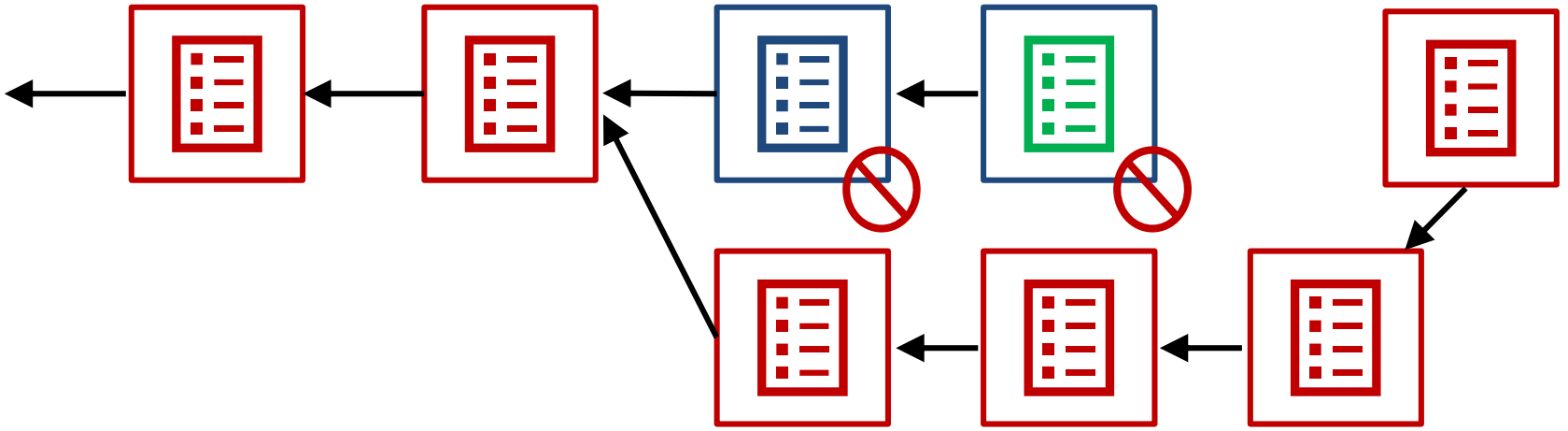
Blacklisting

- **Mining pool 'A'의 hashrate > 전체 네트워크의 hashrate의 51%**
  - Mining pool 'A'는 특정 지갑 'B'로부터의 transaction을 블록체인에 넣는 작업 거부
  - 이러한 상황을 다른 네트워크에 공지



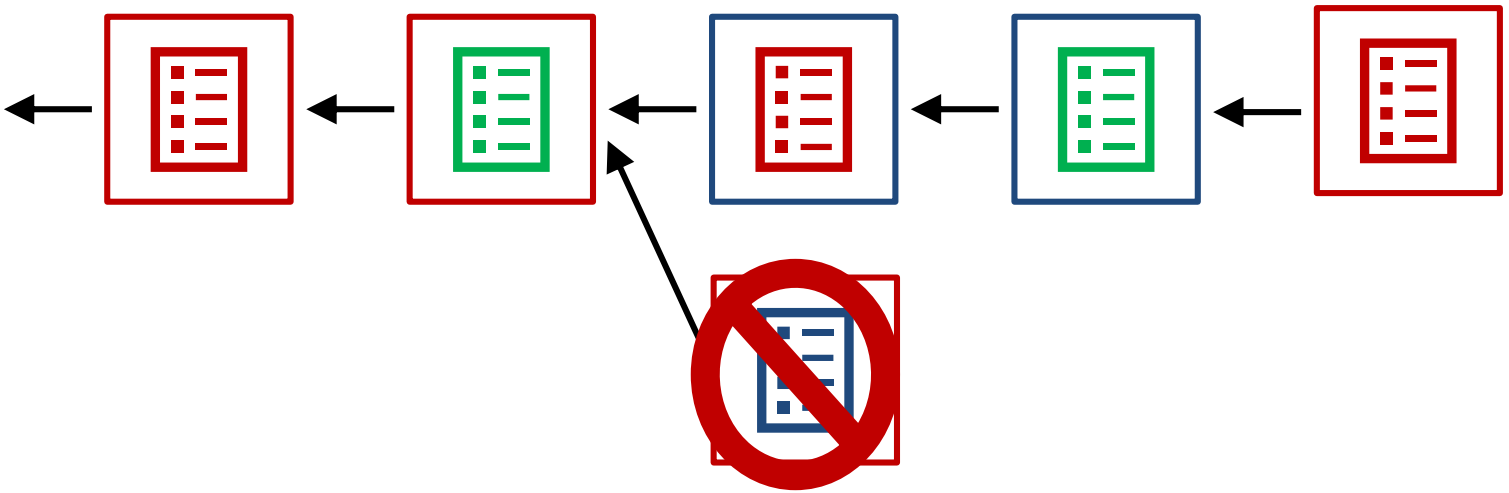
Blacklisting

- 일반적인 정상 mining node가 'B'의 지갑에서 수행된 transaction을 블록에 포함하면, mining pool 'A'는 더 긴 작업 증명 체인으로 포크
  - Mining node 'B'에서 수행된 transaction이 포함된 블록은 무효화되어 사용 안되는 상태



Blacklisting

- Mining pool 'A'를 제외한 다른 mining node들은 결국 자신들이 선택한 블록이 **mining pool 'A'에 의해 무효화 됨을 알고 있음**
  - **블록 선택 및 채굴 시**, 특정 지갑 'B'에 포함된 transaction은 **추가하지 않음**

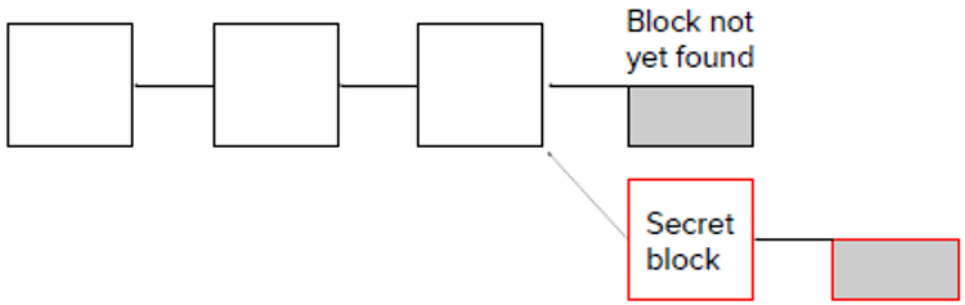


CONTENTS

- Selfish mining

Selfish mining

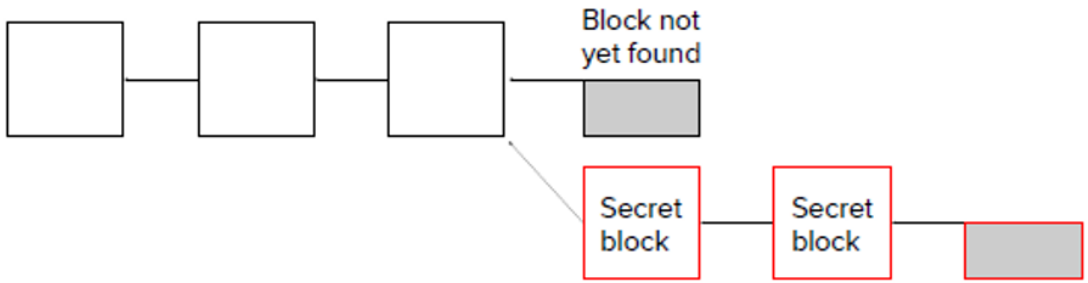
- Mining node에서 방금 블록을 발견했다고(채굴) 가정
  - 채굴 보상을 받는 대신, 네트워크 차단을 선언하고 찾은 블록을 비밀로 유지
  - 기존의 블록체인 네트워크가 다음 블록을 찾기 전에 연속으로 두 개의 블록을 찾으려고 함



Selfish mining or block-withholding

Selfish mining

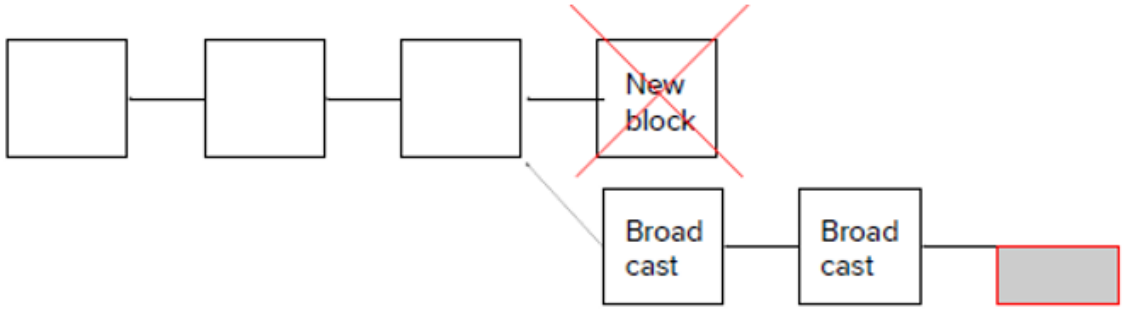
- 두 번째 블록을 찾는 데 (채굴) 성공하면, 블록체인 네트워크를 속이게 됨
  - 블록체인 네트워크는 자신의 블록 체인이 가장 긴 것으로 생각하고 계속 채굴 작업을 수행
  - 공격자는 자신의 분기 부분에서 계속 채굴을 수행



Selfish mining or block-withholding

Selfish mining

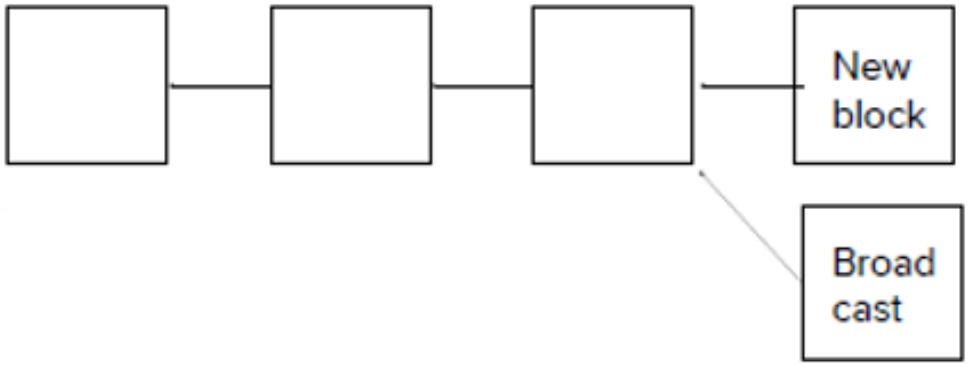
- 혹시라도 블록체인 네트워크가 블록을 찾게 되면, 두 개의 숨겨진 블록을 브로드캐스트하여 기존의 네트워크 블록을 무효화함
  - 기존 네트워크가 블록에 대해 채굴 작업을 수행하는 동안, 혼자서 채굴할 수 있는 시간을 얻음
    - Hashrate이 높을 수록 더 높은 수익을 받게 됨



Selfish mining or block-withholding

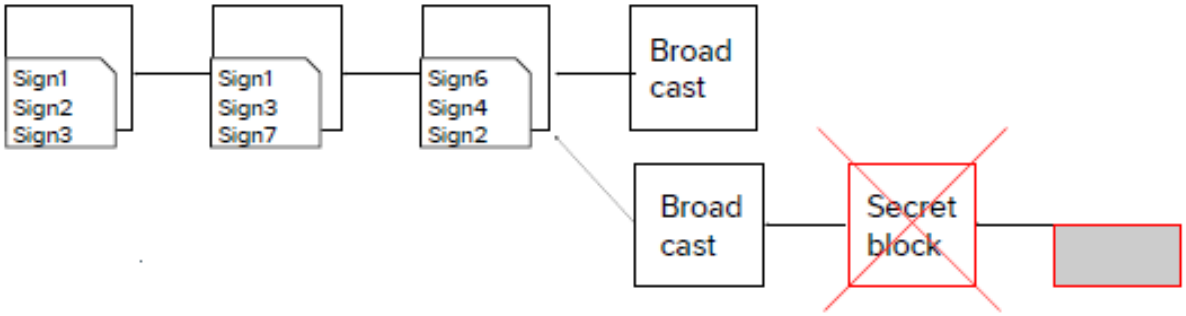
Selfish mining

- 하지만, 기존 네트워크가 더 빠르게 채굴을 수행한다면?
  - 블록 전파에 있어 레이싱 게임이 됨



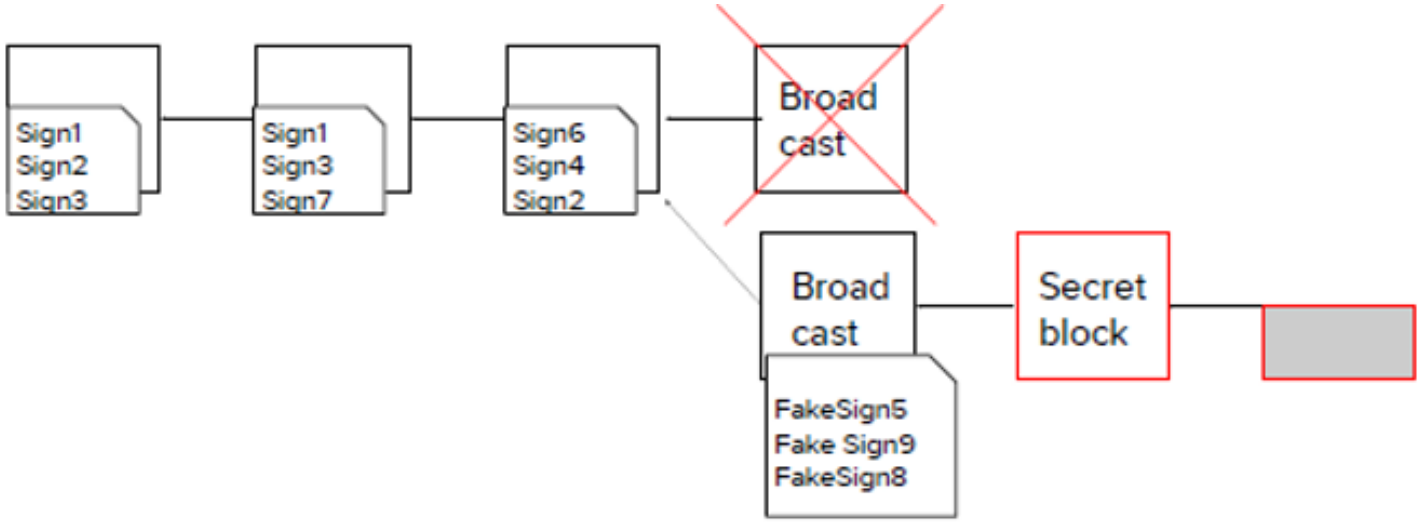
Defenses: block validation

- 전자 서명을 포함한 더미 블록
  - 더미 블록에 전자 서명을 함께 전송
    - 블록들은 네트워크에 의한 확인을 통해 검증 수행
  - 경쟁하는 블록이 없다는 것을 증명하기 위해, 각 블록에 대한 전자 서명을 수행
    - 각 채굴자들이 작업 증명을 수행하기 전에 보류하고 있는 블록이 없다는 것을 증명



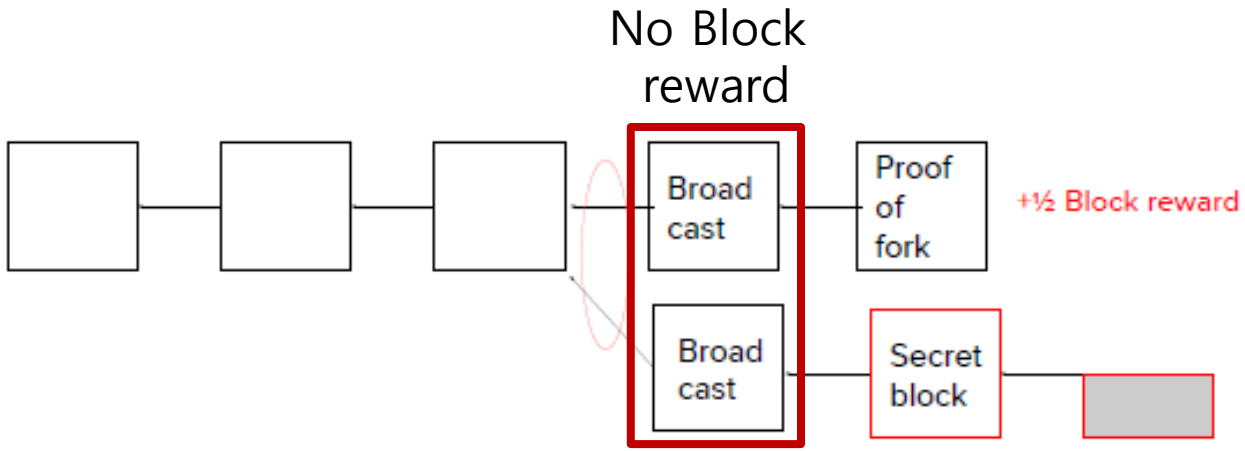
Defenses: block validation

- 블록 검증은 얼마 만큼의 증명의 횟수가 필요한 지에 대한 메커니즘을 제공하지 않음
  - Selfish miner 는 **더미 블록들에 대한 많은 fake signature** 들을 생성



Defenses: fork-punishment

- Fork-punishment
  - Fork가 일어나 분기가 되었을 경우, 경쟁 블록은 블록 보상을 받지 않는 것으로 처리
  - 블록의 fork에 대 증명을 빠르게 연결 및 통합 시키는 쪽에게 첫번째 블록 생성(분기 시)에 몰수한 보상의 일부를 전달함

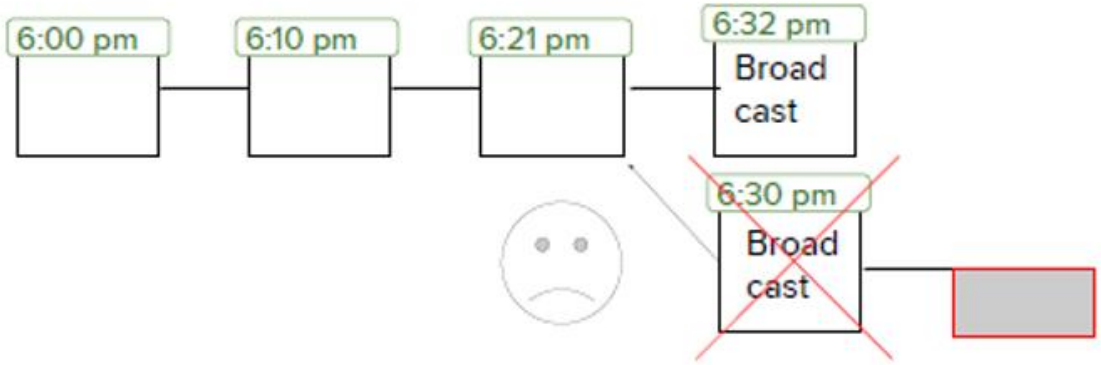


Defenses: fork-punishment

- Fork-punishment
  - 결점
    - 정직한 채굴자의 경우 해당 방어 전략에 피해를 받음
    - 해당 방어 전략으로 인해 다른 종류의 공격 전략이 유도됨
    - 기존 비트코인 시스템에 바로 적용이 제한적임
      - 적용하기 위해서는 Hard fork가 필수적으로 요구됨

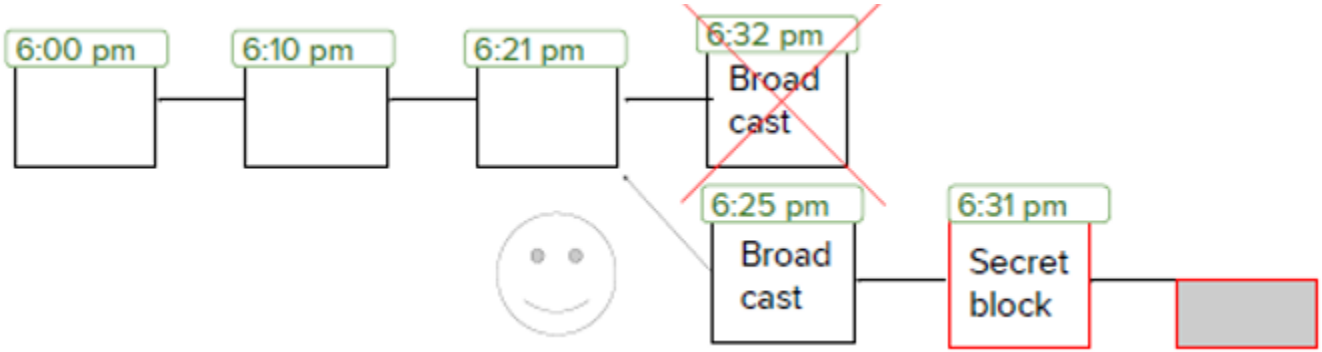
Defenses: Unforgettable timestamps

- Unforgettable timestamps
  - 각 채굴자는 신뢰하는 제 3자가 발행한 위조 불가능한 최신의 Timestamp를 블록 생성에 통합시킴
    - Timestamp는 공개적으로 접근 가능하지만, 예측할 수 없음
    - 60초 간격으로 발행
  - 2개의 경쟁 블록이 120초 이내에 수신 될 경우, 채굴자는 Timestamp를 더 빠른 블록을 선호하여 사용



Defenses: Unforgettable timestamps

- 결점
  - 만약 공격자가 40%를 초과하는 계산 능력이 있을 경우, 해당 방어 전략은 사용되기 어려움



Defenses: Unforgettable timestamps

- 결점
  - **탈중앙화**의 비트코인 및 블록체인
    - **신뢰할 수 있는 제 3자**

CENTRALISATION

CONTENTS

- Attacks on exchange markets

Attacks on exchange markets

Attacks on hot-storage

암호화폐 **거래소** 코인베네 **해킹** 의혹...코스모 등 38개 코인 대상
매일경제 - 10시간 전
암호화폐 **거래소** 코인베네가 **해킹**을 당했다는 의혹에 휩싸였다. 이번 **해킹**으로 코스모 등 38종류의 코인에 부당 입출금이 발생한 것으로 추정된다.

싱가포르 코인**거래소 해킹** 소식에 코인베네 '불똥', 왜?
블록인프레스 - 10시간 전

[FOCUS] 코인베네 **해킹**?...대규모 코인 이동 포착
한국블록체인뉴스 (보도자료) - 9시간 전

3월 27일 코인니스 저녁 뉴스 브리핑
TokenPost - 9시간 전

모두 보기

"나쁜 **해킹** 막아주는 화이트해커 멋져요"
매일경제 - 9시간 전
가상의 코인 **거래소**를 **해킹**하는 `코인 **거래소 해킹**체험`, IoT **해킹** 체험, 눈을 가린 상황에서 알고리즘을 코딩하는 `블라인드 코딩`, 행사장 곳곳에 ...

드래곤엑스 **거래소**, **해킹**으로 '600만 달러' 피해 추정...업계 협조 구해
TokenPost - 16시간 전
싱가포르 소재 암호화폐 **거래소** 드래곤엑스가 **해킹** 공격을 받았다. 25일(현지시간) 코인텔레그래프 보도에 따르면 드래곤엑스는 24일 공식 텔레 ...

싱가포르 암호화폐 **거래소** 드래곤엑스 "**해킹** 사태로 거래 중단"
코인데스크코리아 - 13시간 전
싱가포르 암호화폐 **거래소** 드래고넥스(DragonEx)가 **해킹** 공격을 받았다. 지난 25일 공식 텔레그램 계정을 통해 **거래소 해킹** 사실을 공개한 드래고 ...

Paper Wallets
- Bitcoinpaperwallet.com
- Bitaddress.org

Hardware Wallets
- Trezor, KeepKey

Brain Wallet

} Cold Storage

Attacks on exchange markets

무너진 세계 최대 **비트코인 거래**소...기록 **조작**한 마운트곡스 전 대표...
블록인프레스 - 2019. 3. 14.
비트코인 거래소 마운트곡스의 마크 카펠레스(Mark Karpeles) 전 대표가 전자기록 **조작** 혐의로 징역형의 집행유예를 선고받았다. 15일(현지시간) ...

일본 법원, 마운트 곡스 전 CEO 전자장부 **조작**에 유죄 판결
코인데스크코리아 - 2019. 3. 15.

TOP

`자살 추정` 탑**비트** 대표, 생존 확인...협박당했다 주장
매일경제 - 10시간 전
이들은 전산 **조작**, 장부 거래와 특정 **코인**의 **거래**소 목록 등재, 공지 사항의 ... 탑**비트**에서 이달 초 김 대표의 자살 소식을 알렸을 때부터 커뮤니티를 ...

'사망설' 암호화폐" 거래사이트 '탑**비트**' 김경우 대표 "물의 사죄..책임질 일 ...
데일리경제 - 8시간 전

모두 보기

전자신

업**비트** 전산**조작** 혐의 두나무 임원 3명, 공판 다음달 17일로 연기
전자신문 - 11시간 전
지난해 말 서울남부지검은 국내 최대 암호화폐**거래**소 업비트 임직원이 ... **조작**된 계정으로 임직원이 일반회원인 것처럼 거래에 참여해 **비트코인** 1 ...

References

- Lecture slides from BLOCKCHAIN @ BERKELEY

- https://www.slideshare.net/vpnmentor/mining-pools-and-attacks?from_action=save

Q & A