2017/03/06, 2017 동계 세미나-블록체인

On the Security and Performance of Proof of Work Blockchains

Arthors: Arthur Gervais et al.

이 성 범(sungbum@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

Contents

- Introduction
- BackGround
  - Consensus layer and Network layer in PoW Blockchain
- PoW Security Model using MDP
- Simulation and Evaluation

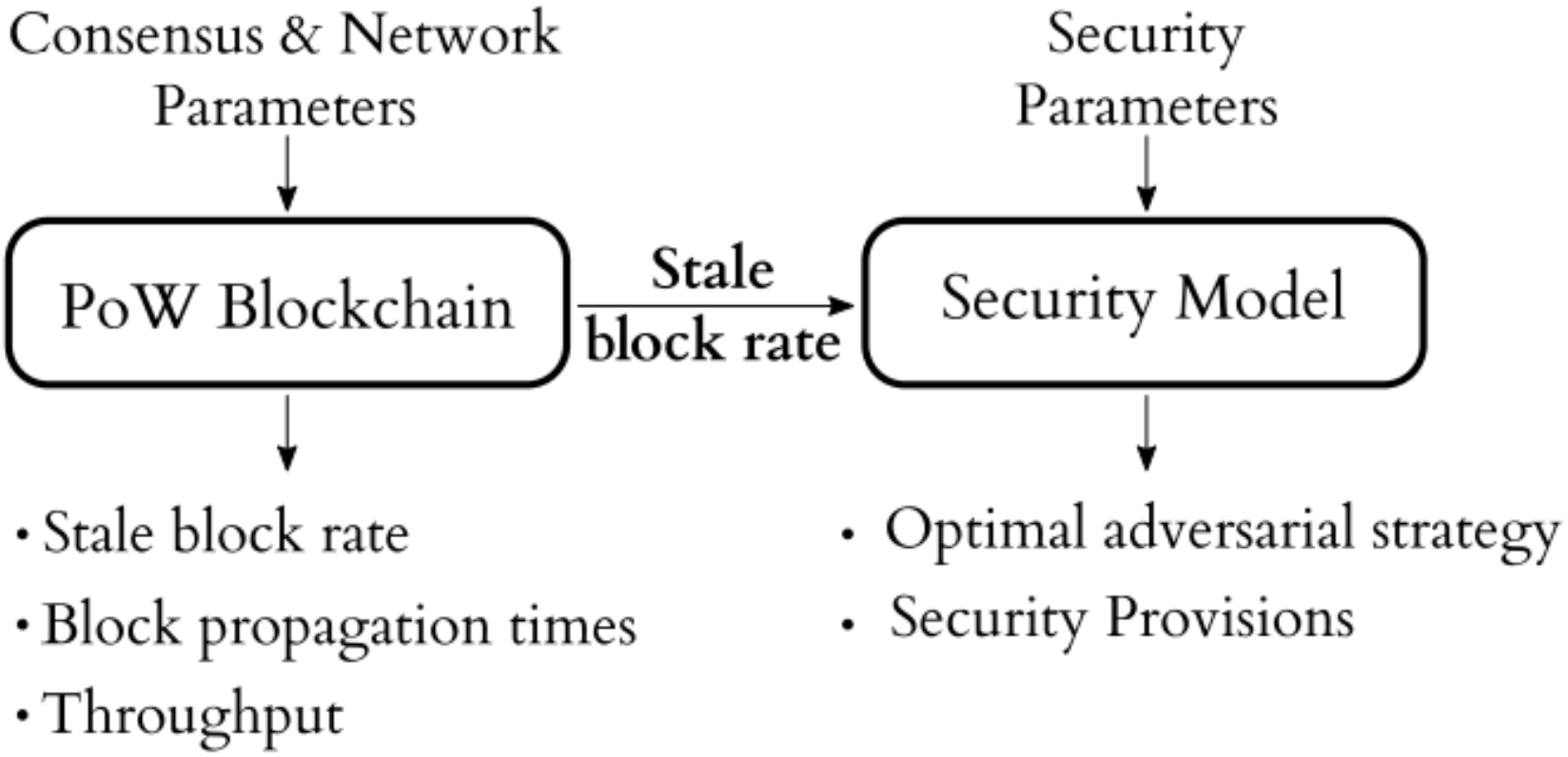
Introduction

- Paper Name
  - On the Security and Performance of Proof of Work Blockchains

- Paper Abstact
  - 자신이 제작한 프레임워크를 기반으로 PoW Blockchains의 보안, 성능 분석
    - Double Spending, Selfish Mining에 대한 최적의 전략 고안

Introduction

- Framework는 두개의 구성으로 나뉨
  - PoW Blockchain, Security Model



Introduction

- Framework는 두개의 구성으로 나뉨
  - PoW Blockchain, Security Model
  - PoW Blockchain Input
    - Consensus & Network Parameter
      - Network Delays
      - Block Generation Times
      - Block Sizes
      - Information Propagation Mechanism 등
        - e.g., Bitcoin, Litecoin, Ethereum은 다른 Blockchain Instacnes를 사용
  - PoW Blockchain Output
    - Block Propagation Times
    - Througput
    - Stale Block Rate
      - Blockchain security model의 입력으로 사용

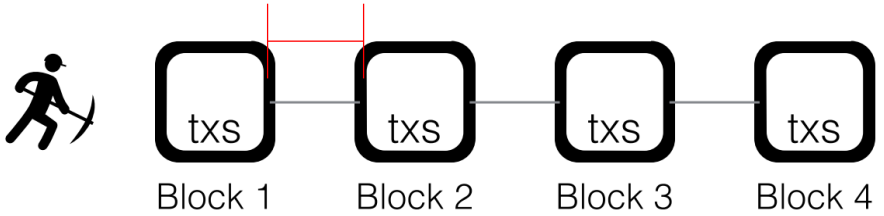
Introduction

- Framework는 두개의 구성으로 나뉨
  - PoW Blockchain, Security Model
  - Security Model Input
    - Security Parameters
      - Stale Block rate
      - Adversarial mining power
      - Block Propagation ability of adversary
      - Eclipse Attack impact
      - Mining costs
      - Number of block confirmations
  - Security Model Ouput
    - Optimal adversarial Strategies
      - based on Markove Decision Processes
      - for Selfish Mining
      - for Double Spending

Background

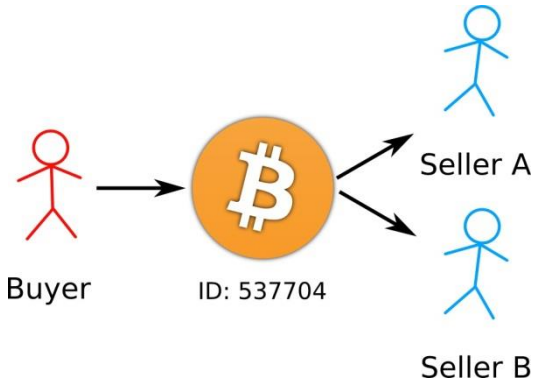
- Blockchain 2 Layers
  - Consensus Layer, Network Layer

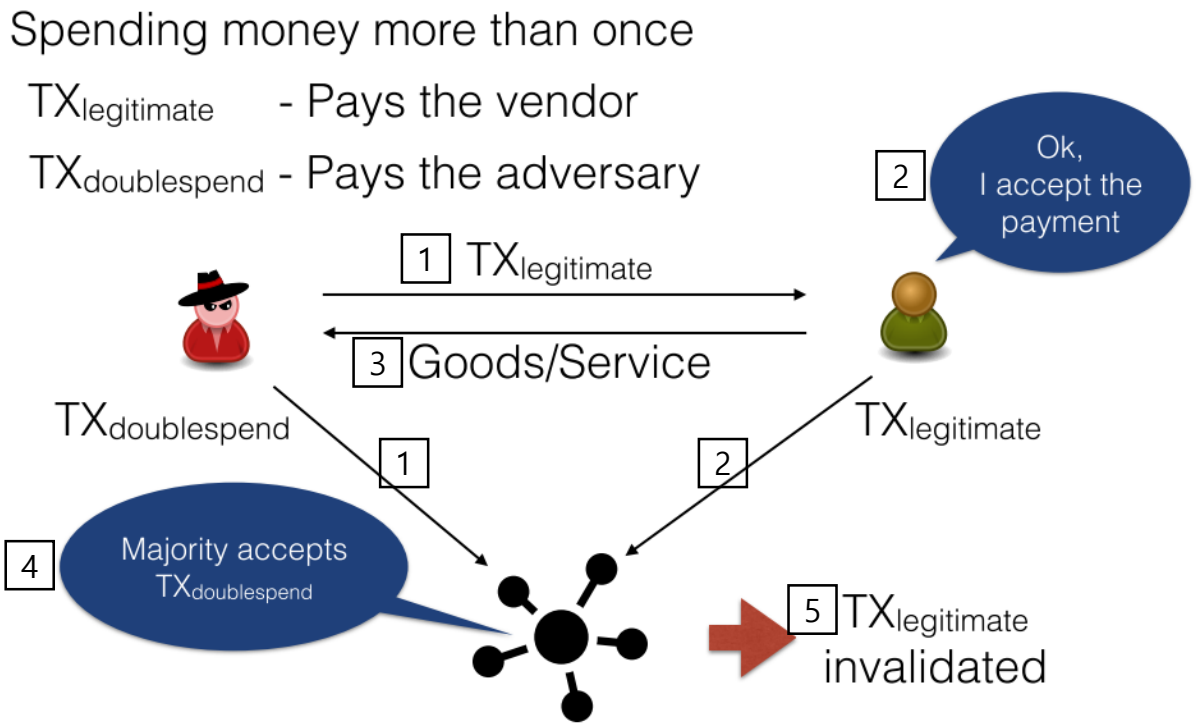
- Consensus Layer(PoW)
  - PoW 합의 알고리즘은 비트코인에서 소개되었고 널리쓰임
  - Block Interval
    - 블록 체인에 블록이 생성되고, 그 다음 블록이 생성되기 까지의 시간
    - 블록 간격이 짧을수록 트랜잭션 처리가 빨라지고,
      블록 간격이 길 수록 트랜잭션 처리가 늦어져 Stale Block생성 확률이 높아짐
    - 블록 간격 조정은 PoW 메커니즘의 난이도 변경과 관련 있음



Background

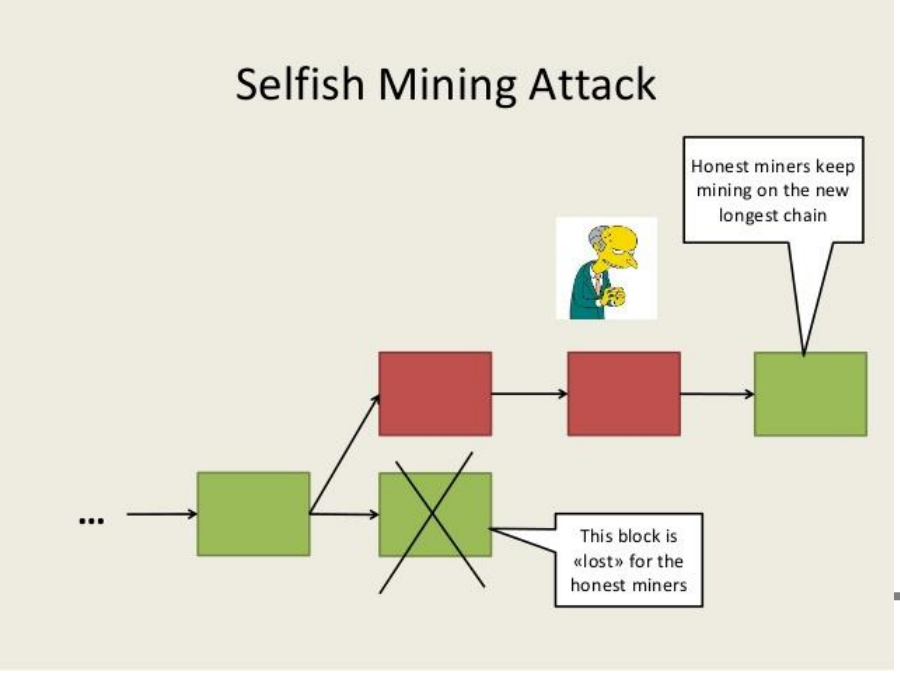
- Consensus Layer(PoW)
  - PoW security
    - 알려진 PoW 공격 방법
      - Double Spending Attack
        - 동일한 비트코인 값으로 다른 거래를 하는 행위





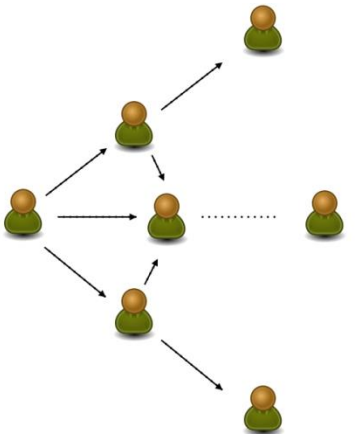
Background

- Consensus Layer(PoW)
  - PoW security
    - 알려진 PoW 공격 방법
      - Selfish Mining Attack
        - 두 개의 블록이 같은 시간에 생성 될때, 블록 경쟁 발생
        - 비트코인 프로토콜은 블록경쟁 시 두 갈래중 다른 한 블록이 연장되는 쪽을 채택, 즉 긴 블록을 채택
          - 블록 경쟁시 미리 생성해둔 블록을 공개하여, 블록을 채택되게 만듦



Background

- Network Layer(PoW)
  - PoW 기반 블록체인에서 중요한 두개의 파라미터
    - Block Size, Information Propagation Mechanism
  - Block Size
    - 최대 블록 크기는 거래의 최대 개수를 의미
    - 크기가 큰 블록일수록 전파속도가 느려지고, Stale Block 생성될 확률이 증가
  - Information Propagation Mechanism
    - 브로드캐스트를 이용한 정보 전달



- ***All transactions, blocks need to be broadcast into the whole network***
- Larger blocks => slower propagation => increased consensus latency
- Risks of network partition (stale blocks …)

Background

- Network Layer(PoW)
  - Information Propagation Mechanism
    - PoW 기반 블록체인에 존재하는 5개의 Network Layer
      - Advertisement-based information dissmination
        - 노드 A가 다른 노드로부터 객체(트랜젝션 혹은 블록)에 관한 정보 수신하면, 노드 B에게 전달
        - 노드 B가 노드 A에게 객체를 요청하면 노드 A는 객체를 응답
      - Send headers
        - 메시지 전파의 대기시간과 대역폭 오버헤드를 줄이기 위해 sendheaders 메시지를 사용
      - Unsolicited Block Push
        - miners는 광고없이 생성된 블록을 브로드 캐스트할 수 있는 방법
      - Relay networks
        - 거래의 common pool을 공유하여 miners들 간에 동기화 성능을 향상
      - Hybrid Push/Advertisement Systems
        - Push, 광고 시스템을 결합한 시스템(Ethereum에서 사용)

Background

- Network Layer(PoW)
  - Stale Blocks
    - 블록은 생성됐지만 블록체인에 포함되지 않은 블록을 의미

	Bitcoin	Litecoin	Dogecoin	Ethereum
Block interval	10 min	2.5 min	1 min	10-20 seconds
Public nodes	6000	800	600	4000 [12]
Mining pools	16	12	12	13
t_{MBP}	8.7 s [9]	1.02 s	0.85 s	0.5 - 0.75 s [13]
r_s	0.41%	0.273%	0.619%	6.8%
s_B	534.8KB	6.11KB	8KB	1.5KB

      - t_{MBP}: 블록 전파 시간
      - r_S: Stale Block Rate
      - S_B: 평균 블록 크기

    - Stale Block은 블록 간격, 블록크기에 큰 영향을 미침

PoW Security Model using MDP

- PoW Security Model
  - PoW 기반 블록체인에서 Double-spending과 Selfish Mining을 막기 위한 Security Model 설계
- Security Model
  - Markov Decision Process(MDP)를 확장한 Optimal adversarial stategies
  - 모델에 필요한 파라미터
    - Stale Block rate, Mining Power, Minig costs, The number of block confirmations k, Propagation ability, The impact of eclipse attacks

PoW Security Model using MDP

- Security Model
  - Markov Decision Process(MDP)
    - 주어진 환경에서 최적의 행동을 결정하는 문제를 푸는 방법

Markov Decision Processes

    - state, action, station probability matrix, reward, dixcounted factor로 이루어짐
      - 로봇이 있는 위치: state, 앞뒤좌우 이동: action, 보석 : reward

PoW Security Model using MDP

- Security Model
  - Markov Decision Process(MDP)
    - 정의

A Markov decision process (MDP) is a Markov reward process with decisions. It is an *environment* in which all states are Markov.

Definition

A *Markov Decision Process* is a tuple $\langle \mathcal{S}, \mathcal{A}, \mathcal{P}, \mathcal{R}, \gamma \rangle$

- $\mathcal{S}$ is a finite set of states
- $\mathcal{A}$ is a finite set of actions
- $\mathcal{P}$ is a state transition probability matrix, $\mathcal{P}^{a}_{ss'} = \mathbb{P}\left[S_{t+1} = s' \mid S_t = s, A_t = a\right]$
- $\mathcal{R}$ is a reward function, $\mathcal{R}^{a}_{s} = \mathbb{E}\left[R_{t+1} \mid S_t = s, A_t = a\right]$
- γ is a discount factor $\gamma \in [0, 1]$.

PoW Security Model using MDP

- Security Model
  - Markov Decision Process(MDP)
    - State: 자신의 상태(로봇이 위치한 곳)
    - Action: 행동(로봇이 움직일 방향)
    - State transition probability matrix: 로봇이 앞 방향으로 action을 했지만 외부 요인으로 인해 왼쪽 방향으로 action이 되어 state가 의도치 않게 변경되는 것
    - Reward: action을 취한후 그에 따른 보상
    - Discount Factor: state에서 action을 취하면 reward를 받게 되는게, 이에 따른 문제 발생
      - agent가 episode를 시작하자마자 1을 받은 경우와 끝날때 1을 받은 경우, 둘다 reward를 1을 받았기 때문에 어떤 경우가 더 나은건지 판단할 수 없음
        - 사람의 입장에서 생각하면 당장 지금 배고픈것을 채우는 것이 내일 배고픈것을 채우는 것보다 중요하다고 생각하고 행동하는 것처럼 discount factor를 통해 시간에 따라 reward의 가치가 달라지게 됨

PoW Security Model using MDP

- Security Model
  - Markov Decision Process(MDP)
    - Policy: agnet는 어떤 state에 도착하면 action을 결정하는데, 어떤 state에서 어떤 action을 할지를 policy라고 함
    - optimal policy를 찾아 reward를 최대화 하여야 함
  - Security Model에서는 MDP를 이용해 어떠한 파라미터의 기준(action)을 정했을때 공격의 영향(reward)이 적은가 판단하여야 함

PoW Security Model using MDP

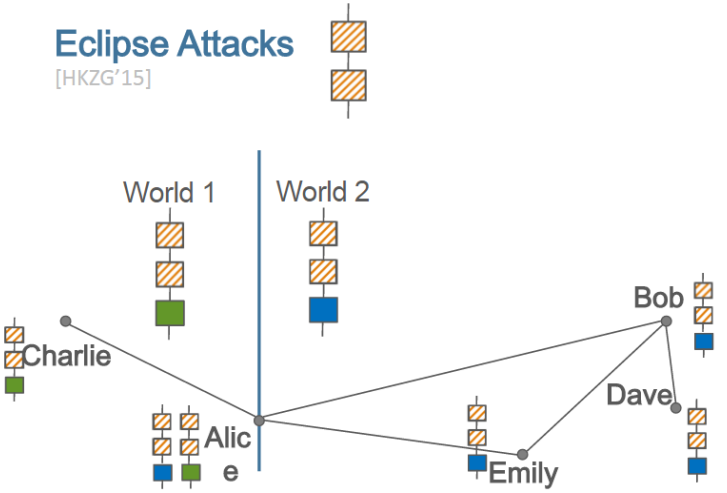
- Security Model
  - Action
    - Adopt: 공격자가 Honest Network의 체인을 받아들이는 행동
    - Override: 공격자가 Honest Network의 체인보다 한 블록 더 발간하여 체인에 덮어 쓰는 행동
    - Match: 공격자는 Honest Network의 체인만큼 블록을 게시하고 블록 경쟁을 발생시키는 행동
    - Wait: 공격자가 블록을 발견할때 까지 Mining 하는 행동
    - Exit: 성공적인 Double Spending을 하였을때 관련된 행동
  - State(S)는 4개의 튜플$(l_a, l_h, b_e, fork)$로 정의
    - l_a, l_h 는 공격자, Honest의 체인
    - b_e는 eclipsed victim으로부터 채굴된 블록을 말함
    - $fork$는 3가지의 값을 가질 수 있음
      - Relevant
      - Irrelevant
      - Active

PoW Security Model using MDP

- Security Model
  - State(S)는 4개의 튜플$(l_a, l_h, b_e, fork)$로 정의
    - l_a, l_h 는 공격자, Honest의 체인
    - b_e는 eclipsed victim으로부터 채굴된 블록을 말함
    - $fork$는 3가지의 값을 가질 수 있음
      - Relevant
        - Honest 네트워크에서 마지막 블록을 발견 했지만, $l_a \geq l_h$인 경우
        - Match Action 적용 가능
        - $l_a, l_h - 1, b_e, \cdot$ 형태의 state는 $l_a, l_h, b_e, relevant$가 됨
      - Irrelevant
        - 공격자가 마지막 블록을 발견 했지만, 마지막 이전 블록이 모든 노드에 도착한 경우
        - Match Action 적용 불가능
        - $l_a - 1, l_h, b_e, \cdot$ 형태의 state는 $l_a, l_h, b_e, irrelevant$가 됨
      - Active
        - Match 동작을 수행한 경우, 블록 경쟁시 state는 Active가 됨

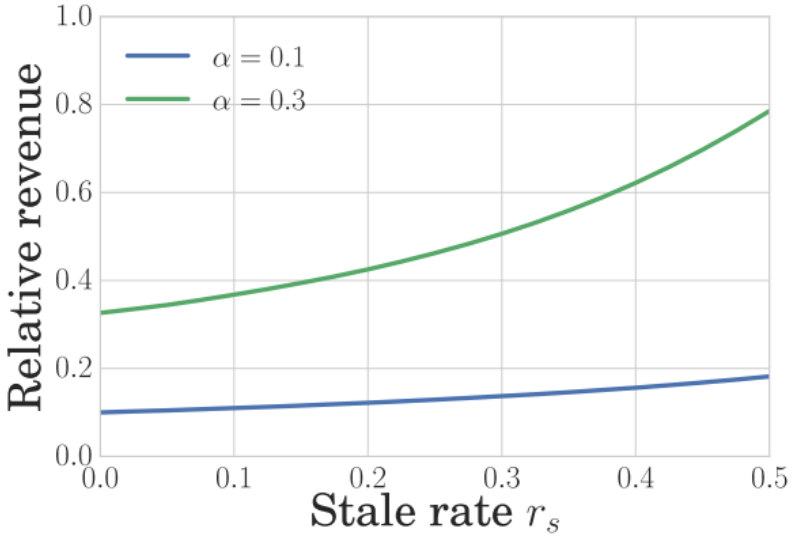
PoW Security Model using MDP

- Security Model
  - Selfish Mining vs. Double Spending
    - Selfish Mining 목적
      - 주 체인에 투입된 공격자의 블록의 비중을 늘리는것
    - Double Spending 목적
      - 수익을 극대화 하는것
    - Eclipse Attacks
      - No eclipse attack
      - Isolate the victim
      - Exploit the eclipsed victim



PoW Security Model using MDP

- Security Model
  - Selfish Mining MDP
    - Optimal Strategies for Selfish Mining
      - MDP를 풀기위해 MDP Solver를 적용하고, 30블록의 컷오프 값을 사용
      - Stale Block이 Selfish Mining에 영향을 끼치는지 여부 파악



      - Selfish Miner의 reward 증가.

PoW Security Model using MDP

- Security Model
  - Double-Spending MDP
    - Optimal Strategies for Double-Spending
      - MDP에서 Optimal Strategies 연산
        - pymdptoolbox library 4 사용
        - PolicyIteration 알고리즘 적용
      - 위 방법을 통해 confirmation k 에서 k의 값이 보안을 확보하기에 충분한지 여부를 평가 할 수 있음

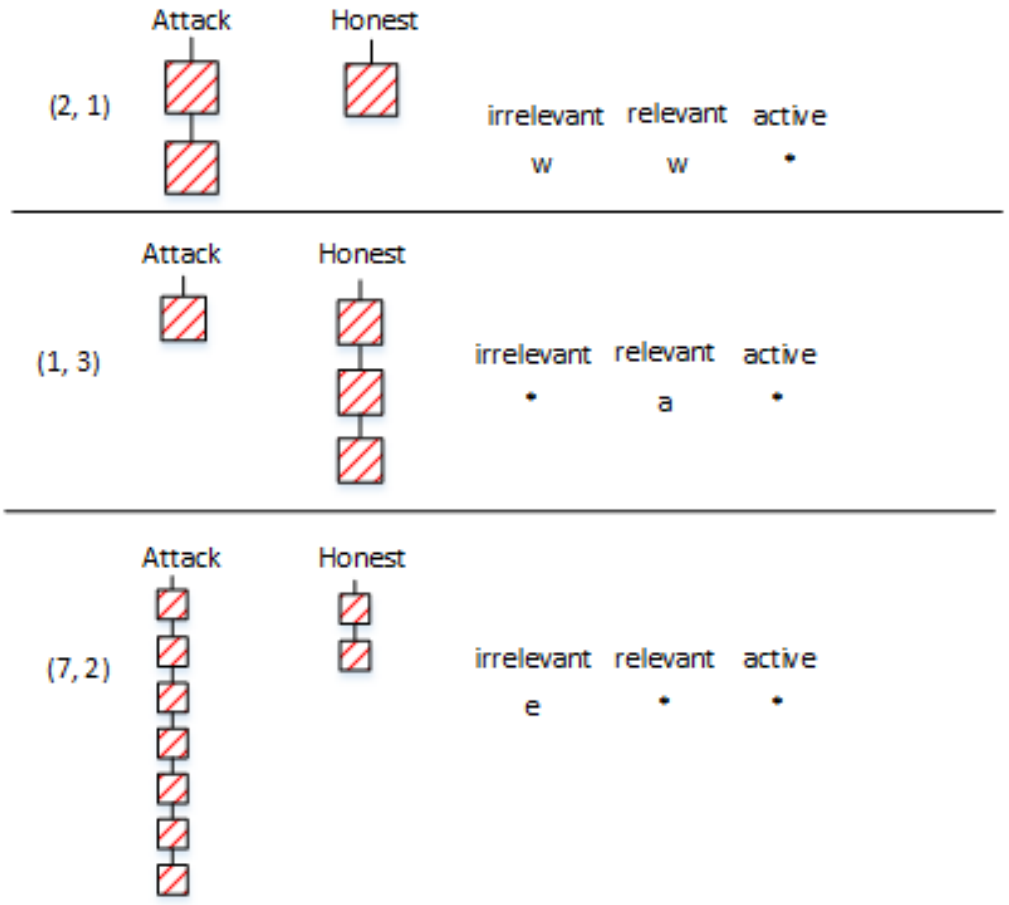
PoW Security Model using MDP

- Security Model
  - Double-Spending MDP
    - Optimal Strategies for Double-Spending
      - 아래의 표는 α = 0.3 (adversarial mining power), γ = 0 (propagation parameter), cm = α (maximum mining costs), ω = 0 (no eclipse attack)에 대한 optimal strategy의 예를 제시
      - l_h : $Honest\ Network\ chain\ length$
      - l_a : $adversary's\ chain$
      - * : 불가능
      - w: wait
      - a: $adopt$
      - e: $exit$

l_a \ l_h	0	1	2	3	4	5	6	7	8
0	w**	*a*	***	***	***	***	***	***	***
1	w**	ww*	ww*	*a*	***	***	***	***	***
2	w**	ww*	ww*	ww*	ww*	*a*	***	***	***
3	w**	ww*	ww*	ww*	ww*	ww*	*a*	***	***
4	w**	ww*	ww*	ww*	ww*	ww*	ww*	*a*	***
5	w**	ww*	ww*	ww*	ww*	ww*	ww*	ww*	*a*
6	w**	ww*	ww*	ww*	ww*	ww*	ww*	ww*	ww*
7	e**	e**	e**	e**	e**	e**	e**	w**	ww*
8	***	***	***	***	***	***	***	e**	w**

PoW Security Model using MDP

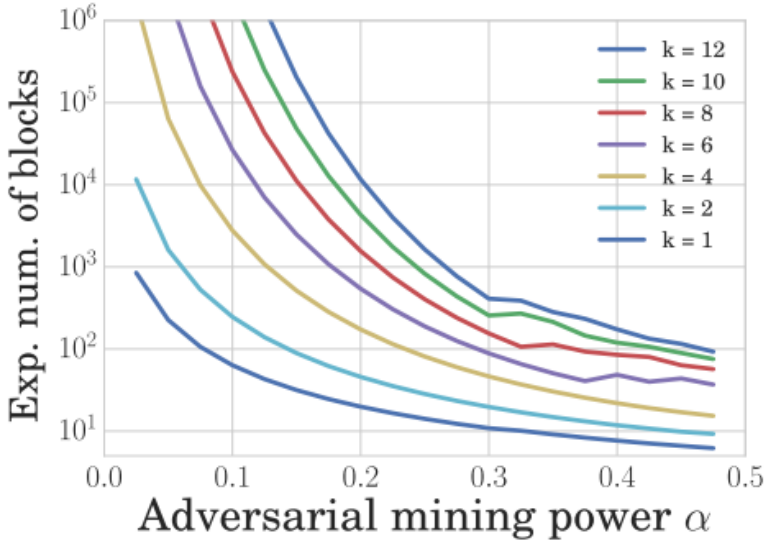
- Security Model
  - Double-Spending MDP



- $exit: l_a > l_h \; and \; l_a \; > k.$

PoW Security Model using MDP

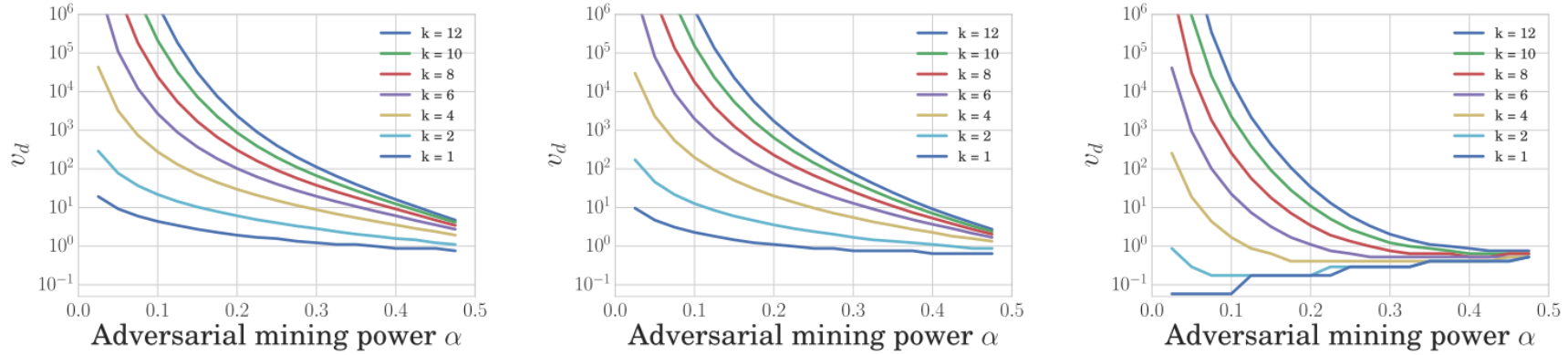
- Security Model
  - Double-Spending MDP
    - Optimal Strategies for Double-Spending
      - 아래의 그림은 Double Spending 공격이 성공하기 위한 예상 블록 수를 나타냄.



      - e.g., 비트코인에서 1주간, Double Spending 공격이 성공하기 위해서는 0.25 이상의 mining power와 1000 블록이 필요. (confirmation = 10)

PoW Security Model using MDP

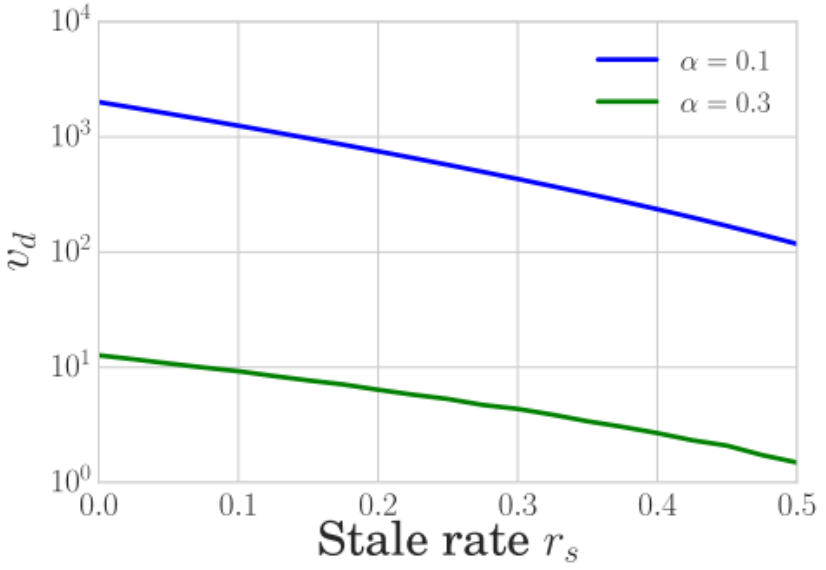
- Security Model
  - Double-Spending MDP
    - Optimal Strategies for Double-Spending
      - Impact of Propagation Parameter
        - Propagation Parameter가 증가하면 adversary 간의 연결 증가.
          - Double Spending 공격 가능성 증가.
      - v_d: $Value\ of\ Double\ Spend$
        - Double Spending을 Honest Mining 보다 더 유리하게 만드는 minimum transaction value
      - γ: $Connectivity\ of\ the\ adversary\ within\ the\ network$
      - $\gamma = 1$ 일때, 최소 $0.5\ blcok\ reward$, $\gamma = 0.5$ 일때, $12.9\ blcok\ reward$



(a) $\gamma = 0$ (b) $\gamma = 0.5$ (c) $\gamma = 1$

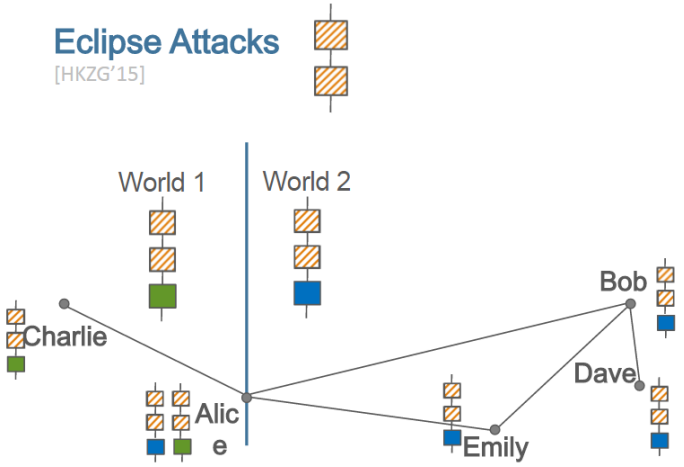
PoW Security Model using MDP

- Security Model
  - Double-Spending MDP
    - Optimal Strategies for Double-Spending
      - Impact of Stale Block rate
        - Double Spending에 큰영향을 미치고 있음
        - PoW 블록 체인의 보안에 가장 중요한 요소 중 하나



PoW Security Model using MDP

- Security Model
  - Double-Spending MDP
    - Optimal Strategies for Double-Spending
      - Impact of eclipse attacks
        - adversary의 mining power를 이용해 victim에게 eclipse attack이 가능
        - Double Spending에 영향을 끼침



      - Impact of Mining Costs
        - Double Spending 에서 영향이 없음

PoW Security Model using MDP

- Security Model
  - Bitcoin vs. Ethereum
    - Ethereum
      - Stale Block 문제를 해결하기위해 Uncle Block 개념 도입
      - Selfish Mining 문제를 해결하기 위해 긴 체인 알고리즘을 수정하여 균일한 tie breaking 도입
      - Bitcoin과 Etereum이 동일하게 6 confirmation일때
        - Double Spending attack 에 대해서 Bitcoin이 더 안전함
      - Bitcoin과 Ethereum의 Stale Block이 동일하다고 가정
        - 두 블록 체인을 객관적으로 비교했을때, Bitcoin이 보안상 더 안전함을 확인

Simulation and Evaluation

- Security vs. Performance of PoW Blockchains
  - 블록 체인 보안 및 성능을 평가

- Blockchain Simulator
  - 직접 개발한 Simulator를 이용한 평가 실시
  - 다양한 블록 체인 파라미터를 평가
    - Block Interval
    - Block Size
    - Propagation Mechanisms
    - Stale Block rate
    - Throughput
    - Block Propagation times

Simulation and Evaluation

- Blockchain Simulator
  - 통합 프레임 워크에서 MDP 모델에 블록 체인 시뮬레이터 연결 가능
    - 블록 체인 인스턴스의 보안을 평가
      - Simulator의 output(Stale Block)을 MDP 모델에 제공하여 분석
  - 시뮬레이터에서 수집한 파라미터

Consensus parameter	Description
Block interval distribution	Time to find a block
Mining power distribution of the miners	PoW power distribution
Network-layer parameter	Description
Block size distribution	Variable transaction load
# of reachable network nodes	Open TCP port nodes
Geo. distribution of nodes	Worldwide distribution
Geo. mining pool distribution	Worldwide distribution
# of connections per node	Within network
# of connections of the miners	Within network
Block request management system	Possible Protocols
Standard mechanism (inv/getdata)	Default
Unsolicited block push	Miner only push block
Relay network	Miner network
Sendheaders	Bitcoin v0.12

  - 시뮬레이터 Download
    - https://github.com/arthurgervais/Bitcoin-Simulator

Simulation and Evaluation

- Evaluation Results
  - Simulator Validation

	Bitcoin	**Litecoin**	**Dogecoin**
Block interval	10 min	2.5 min	1 min
Measured t_{MBP}	8.7 s [9]	1.02 s	0.98 s
Simulated t_{MBP}	9.42 s	0.86 s	0.83 s
Measured r_s	0.41 %	0.27 %	0.62 %
Simulated r_s	(a)0.14%-(b)1.85%	(b)0.24 %	(b)0.79 %

    - Median Block Propagation Time, t_{MBP}
    - Stale Block rate, r_s
    - (a): Bitcoin의 경우 모든 Miner가 중계 네트워크와 비요청 블록 푸시 사용한다고 가정
    - (b): 표준 Propagation Mechanism만 제공한다고 가정

Simulation and Evaluation

- Evaluation Results
  - Impact of Block Interval
    - PoW 기반 블록체인에서 Median Block Propagation time과 Stale Block rate에 Block interval의 영향
    - Mining Power가 30%인 adversary
      - Consensus time이 적을수록 Selfish Minig Attack 확률이 높고, Double Spending Attack 확률이 낮아짐.

Simulation and Evaluation

- Evaluation Results
  - Impact of Block Interval
    - case 1: 표준 블록 요청 관리
    - case 2: 강화된 표준 블록 요청 관리
    - case 3: 이전의 구성 요소를 추가한 릴레이 네트워크
    - case 4: 블록 푸시 및 릴레이 네트워크와 송신 헤더 메커니즘

	Case 1				Case 2				Case 3				Case 4			
Block interval	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}
25 minutes	35.73	1.72 %	12.47	0.34	25.66	0.16 %	12.86	0.33	22.50	0.03 %	12.89	0.33	22.44	0.02 %	12.89	0.33
10 minutes	14.7	1.51 %	12.52	0.34	10.65	0.13 %	12.88	0.33	9.41	0.14 %	12.86	0.33	9.18	0.13 %	12.87	0.33
2.5 minutes	4.18	1.82 %	12.45	0.34	2.91	0.16 %	12.86	0.33	2.60	0.16 %	12.86	0.33	2.59	0.15 %	12.86	0.33
1 minute	2.08	2.15 %	12.35	0.34	1.34	0.35 %	12.81	0.33	1.30	0.25 %	12.83	0.33	1.27	0.29 %	12.77	0.33
30 seconds	1.43	2.54 %	12.06	0.34	0.84	0.45 %	12.78	0.33	0.84	0.51 %	12.77	0.33	0.84	0.52 %	12.69	0.33
20 seconds	1.21	3.20 %	11.73	0.34	0.67	0.86 %	12.68	0.33	0.69	0.85 %	12.68	0.33	0.68	0.82 %	12.68	0.33
10 seconds	1.00	4.77 %	10.73	0.35	0.35	1.73 %	12.46	0.34	0.33	1.41 %	12.54	0.34	0.53	1.59 %	12.50	0.34
5 seconds	0.89	8.64 %	10.08	0.37	0.37	2.94 %	11.85	0.34	0.45	2.99 %	11.80	0.34	0.44	3.05 %	11.78	0.34
2 seconds	0.84	16.65 %	7.35	0.41	0.40	6.98 %	10.47	0.36	0.39	7.28 %	10.37	0.36	0.38	7.10 %	10.42	0.36
1 seconds	0.82	26.74 %	4.37	0.53	0.53	12.44 %	8.34	0.39	0.38	12.59 %	8.24	0.39	0.37	12.52 %	8.30	0.39
0.5 seconds	0.82	38.15 %	2.78	0.60	0.61	20.62 %	6.22	0.42	0.49	20.87 %	6.16	0.42	0.36	21.10 %	6.02	0.42

Simulation and Evaluation

- Evaluation Results
  - Impact of Block Size
    - Block Size가 증가함에 따라 Block Propagation time이 선형적으로 증가
    - Block Size가 8MB 이후 부터는 Block Propagation time과 Stale Block rate가 기하 급수적으로 증가

Block Size	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}	t_{MBP}	r_s	v_d	r_{rel}
0.1 MB	3.18	0.32 %	12.80	0.33	2.12	0.03 %	12.89	0.33	2.02	0.03 %	12.89	0.33	2.02	0.2 %	12.90	0.33
0.25 MB	7.03	0.88 %	12.67	0.33	4.93	0.11 %	12.87	0.33	4.49	0.05 %	12.88	0.33	4.46	0.17 %	12.87	0.33
0.5 MB	13.62	1.63 %	12.48	0.34	9.84	0.13 %	12.87	0.33	8.65	0.05 %	12.88	0.33	8.64	0.06 %	12.87	0.33
1 MB	27.67	3.17 %	11.79	0.34	20.01	0.38 %	12.79	0.33	17.24	0.07 %	12.88	0.33	17.14	0.07 %	12.88	0.33
2 MB	57.79	6.24 %	10.57	0.36	44.6	1.12 %	12.61	0.34	35.49	0.08%	12.87	0.33	35.38	0.1 %	12.86	0.33
4 MB	133.30	11.85 %	8.20	0.38	126.57	5.46 %	10.51	0.35	78.01	0.12 %	12.85	0.33	78.40	0.13 %	12.66	0.33
8 MB	571.50	29.97 %	4.11	0.53	875.97	15.64 %	7.64	0.41	555.49	0.43 %	12.65	0.33	550.25	0.4 %	12.68	0.33

Simulation and Evaluation

- Evaluation Results
  - Throughput
    - 블록의 크기와 블록 간격을 조정하며 측정

tps	v_d	r_{rel}	Block size	Block interval
33.4	12.75	0.33	0.25MB	30 seconds
40	12.38	0.34	0.10MB	10 seconds
50	12.45	0.34	0.25MB	20 seconds
66.7	12.06	0.34	0.25MB	15 seconds
66.7	12.65	0.33	0.50MB	30 seconds
66.7	12.71	0.33	1.00MB	1 minute

    - 이러한 측정을 통해 보안을 크게 손상시키지 않으면서 기존 PoW의 확장성을 향상 시킬수 있는 여지가 있음을 보여줌

감사합니다!

(sungbum@pel.smuc.ac.kr)

Back Up #1: 용어 정의

- r_s: $Stale\ Block\ rate$
- α: $Adversarial\ Mining\ Power$
- v_d: $Value\ of\ Double\ Spend$
- γ: $Connectivity\ of\ the\ adversary\ within\ the\ network$
- c_m: $Maximum\ Minng\ Cost$
- b_e: $The\ number\ of\ blocks\ in\ the\ attacker\ chain\ that\ were\ mined\ bye\ the\ eclipsed\ node$
- k: $the\ number\ of\ confirmation$
- t_{MBP}: Median Block Propagation Time