PROBABILISTIC QV

PROBABILISTIC QUADRATIC VOTING

REFERENCE

- 이준모, 박상현, 문수묵.
  “확률적 제곱 투표와 신뢰 실행 환경을 통한
  시빌 공격 저항성을 가지는 안전한 투표 시스템”.
  KSC2020. 2020.

- 논문은 TEE 기반
- 그 전에 진행했던 블록체인 기반 연구

ABSTRACT

ABSTRACT

- 투표
  - 다수의 의견이 충돌하는 상황에서 합의를 이끌고 정책을 결정하기 위함
  - 가장 대표적인 투표 방법론은 1 인 1 투표권을 가지는 평등 투표

ABSTRACT

- 평등 투표에 대한 비판
  - 실질적으로 정책에 영향을 받는 그룹과
  - 그렇지 않은 그룹 모두가 동등한 영향력을 가짐
- 여러 다른 투표 방법론이 제시됨
  - 1인 다(多) 투표권

ABSTRACT

- **제곱 투표(Quadratic Voting, QV)**
  - 한 사람이 여러 투표권을 행사할 수 있는 투표 시스템에서
  - 개인의 의견을 효과적으로 표출하면서도 합리적인 합의를 도출할 수 있는 방법론
- QV의 투표권
  - 그 제곱에 해당하는 비용을 지불함으로써 원하는 만큼 획득
    - 더 많은 비용을 지불할 수록 의견을 강하게 표출할 수 있음
    - 그 제곱에 해당하는 비용을 지불해야 함

ABSTRACT

- 결과에 대한 신뢰 요구 & 제곱에 해당하는 비용 지불
  - QV는 블록체인 기반 시스템에서 자연스럽게 구현 가능
  - 주로 언급됨
- QV는 시빌 공격(sybil attack)에 취약
  - 투표권 분산
  - 블록체인의 익명성과 주소 생성의 비인증 요소를 이용하면 시빌 공격이 용이

ABSTRACT

- **확률적 제곱 투표(Probabilistic Quadratic Voting, PQV)** 방법론
  - 투표권의 수에 비례해 최종 집계에 반영될 확률이 부여됨
- PQV에서 투표권자가 취할 수 있는 여러 행동 중
  - 가장 높은 기댓값을 가지는 방법은 한 번의 투표에 모든 투표권을 사용하는 방법
- 이성적인 투표 참여자는
  - 시빌 공격과 같은 투표권 분산을 이용한 악의적 행위를 취하지 않음

BACKGROUND

BACKGROUND – VOTING

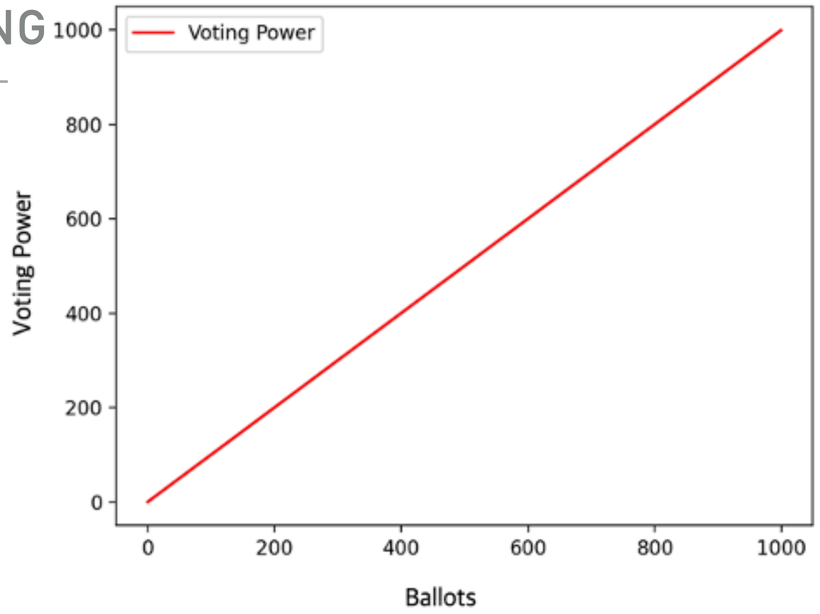
- **평등 투표(Equal Voting)**
  - 1 인 1 투표권의 투표 시스템
- **선형 투표(Linear Voting)**
  - 1인 다(多) 투표권의 투표 시스템
- **제곱 투표(Quadratic Voting, QV)**
  - 1 인 다 투표권의 시스템
  - 투표권의 획득에 선형적이지 않은 비용을 요구

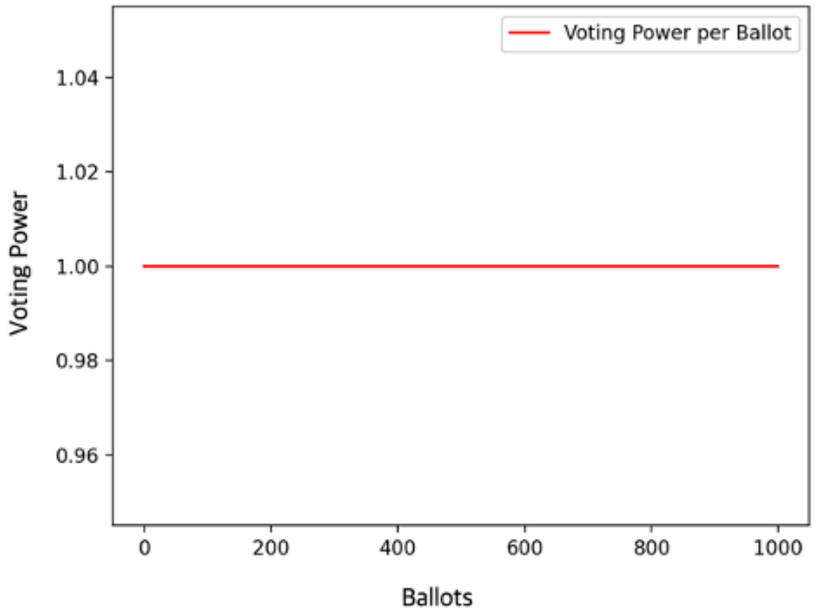
BACKGROUND – VOTING

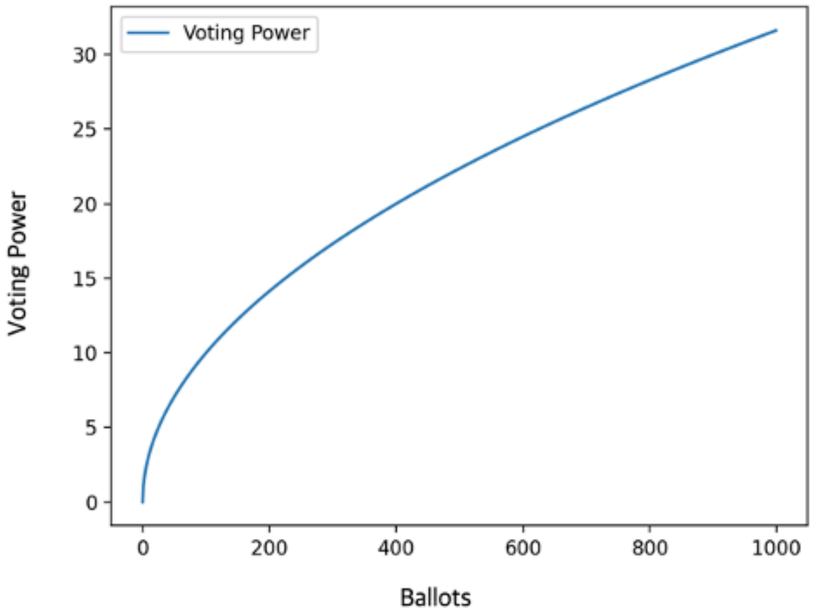
- **제곱 투표(Quadratic Voting, QV)**
  - 제곱 투표에서 투표권은 개수의 제곱에 해당하는 비용을 지불함으로써 획득
  - 1 투표권에 1 달러라 가정하면,
    100 달러를 지불해 $\sqrt{100} = 10$ 에 해당하는 투표권을 획득
- 민주주의의 다수결이 가지는 문제를 효과적으로 해결하면서도
- 선형 투표의 양극화(빈익빈 부익부) 문제를 완화

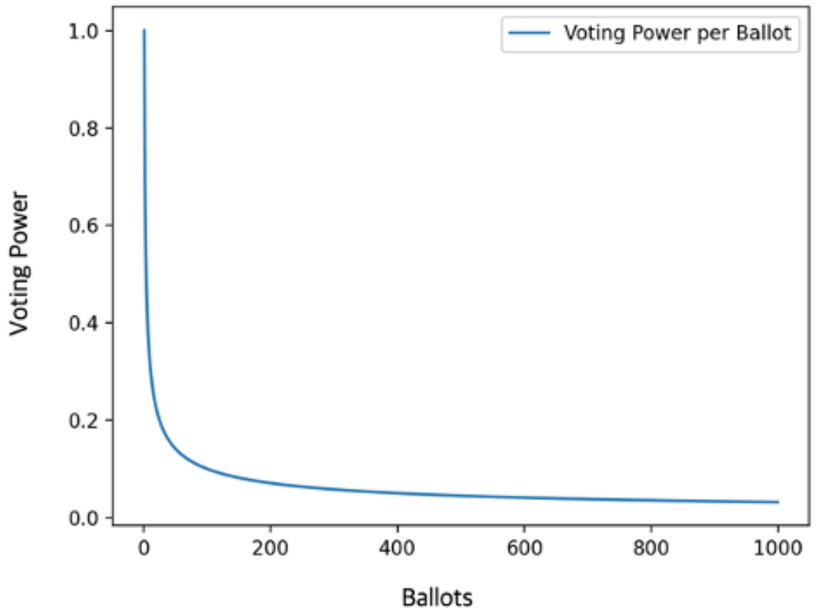
BACKGROUND – VOTING

- 선형 투표의 투표권 수에 따른 영향력 (위 좌측 그래프)
- 투표권 한 장당 영향력 (위 우측 그래프)
- 제곱 투표의 투표권 수에 따른 영향력 (아래 좌측 그래프)
- 투표권 한 장당 영향력 (아래 우측 그래프)









BACKGROUND – VOTING

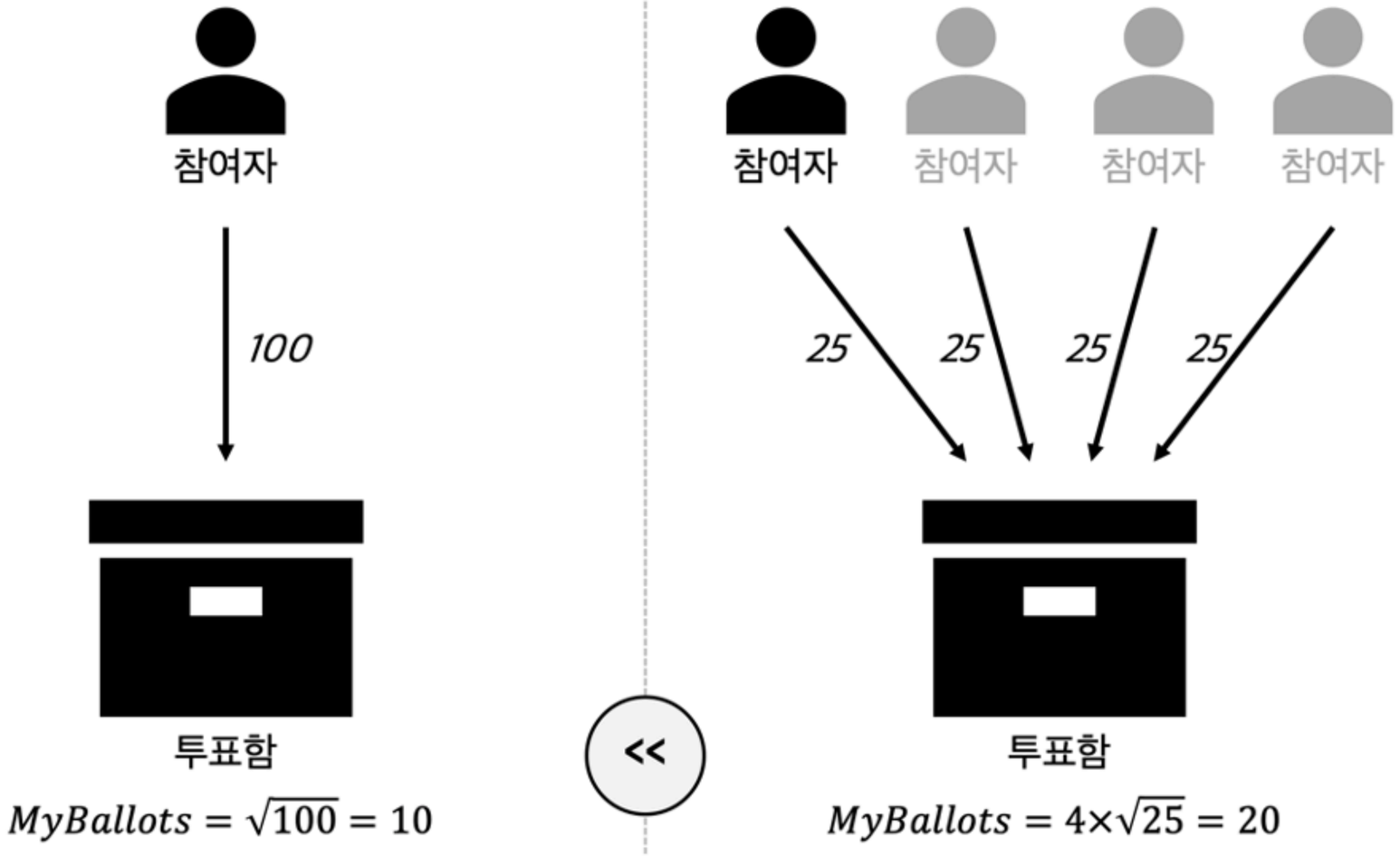
- 선형 투표는 사용한 투표권의 양 만큼의 투표 영향력을 가짐
  - 투표권 한 장당 영향력은 사용한 투표권이 얼마든 상관 없이 1로 변하지 않음
- 제곱 투표에서는 제곱근에 비례하는 투표 영향력을 가짐
  - 투표권 한 장당 영향력은 사용한 투표권의 수가 늘어날 수록 급격히 줄어듦
  - 선형 투표가 가지는 양극화 문제를 완화

BACKGROUND - SYBIL ATTACK

- **시빌 공격(Sybil attack)**
  - 한 명의 공격자가 시스템상에서 여러 명인 것처럼 행동해 의사결정을 방해하는 공격
- 블록체인에서는 계좌를 생성하는 데 제한이 없음
  - 가짜 신원을 거의 무한정 생성할 수 있어 시빌 공격이 용이
  - 가령 한 명이 100 달러를 지불해 $\sqrt{100} = 10$ 투표권을 행사하는 것이 아닌
  - 100 명의 가짜 신원으로 각자 $\sqrt{1} = 1$ 달러를 지불해
    $100 * \sqrt{1} = 100 * 1 = 100$ 의 부정한 투표권을 행사할 수 있음

BACKGROUND – SYBIL ATTACK

- 여러 명의 투표권자인 척 가장
- 블록체인에서의 신원
  - 계좌(account)로부터 식별
  - 계좌 생성에 제한이 없음
  - 누구나 쉽게 시빌 공격을 행함
- 블록체인 기반 제곱 투표는
  - 단순하게 구현될 수 없음



PROBABILISTIC QV

PROBABILISTIC QUADRATIC VOTING

- **확률적 제곱 투표(Probabilistic Quadratic Voting, PQV)**
  - 투표 참여자들이 시빌 공격을 수행하지 않도록 할 요인을 제공
  - 블록체인에 기반한 제곱 투표를 가능하게 함
- PQV를 이용하면
  - 블록체인의 무결성과 신뢰성을 보장받으면서
  - 다수결의 문제를 해결한 QV의 장점을 취할 수 있음

PROBABILISTIC QUADRATIC VOTING

- 투표권의 수에 비례해 최종 집계에 반영될 확률을 부여
  - $$p = \frac{X^e}{N}$$
  - p: PQV에서 투표권이 반영될 확률
    N: 총 투표권의 수
    X: 나의 투표권의 수
    e: 확률의 가중치 (하이퍼파리미터, $e \geq 1$)
    - e가 커질 수록 반영될 확률이 높아짐

PROBABILISTIC QUADRATIC VOTING

- PQV에서는 투표권의 수에 비례해 최종 집계에 반영될 확률이 부여
- 투표권자가 취할 수 있는 행동 중 가장 높은 기댓값을 가지는 방법
  - 최대한 많은 투표권을 한 번에 사용하는 방법
  - 이성적인 투표 참여자는 시빌 공격을 행하지 않음
    - 투표권을 분산시키지 않음

PROBABILISTIC QUADRATIC VOTING

- PQV에서 시빌 공격이 비효율적임을 보이는 부등식 및 조건
- $$\frac{X\sqrt{X}}{N} > \sum_{l=0}^{k} \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l} \sqrt{\frac{X}{k}}(k-l)$$

PROBABILISTIC QUADRATIC VOTING

- PQV에서 시빌 공격이 비효율적임을 보이는 부등식 및 조건
- $$\frac{X\sqrt{X}}{N} > \sum_{l=0}^{k} \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l} \sqrt{\frac{X}{k}}(k-l)$$
  - 부등식의 좌항: PQV에서 한 번에 모든 투표권을 사용해 투표한 경우의 기댓값
  - 반영될 확률(p)과 투표 영향력(u)의 곱

$$pu = \frac{X\sqrt{X}}{N}$$

$$\text{where } p = \frac{X}{N},\ u = \sqrt{X}$$

PROBABILISTIC QUADRATIC VOTING

- PQV에서 시빌 공격이 비효율적임을 보이는 부등식 및 조건
- $$\frac{X\sqrt{X}}{N} > \sum_{l=0}^{k} \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l} \sqrt{\frac{X}{k}}(k-l)$$
  - 부등식의 우항: PQV에서 투표권을 k개로 분산시켜 투표한 경우의 기댓값

$$\sum_{l=0}^{k} p_l u_l = \sum_{l=0}^{k} \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l} \sqrt{\frac{X}{k}}(k-l)$$

$$\text{where } p_l = \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l},$$

$$\text{and } u_l = \sqrt{\frac{X}{k}}(k-l)$$

PROBABILISTIC QUADRATIC VOTING

- PQV에서 투표권을 k개로 분산시켜 투표한 경우의 기댓값
- $$\sum_{l=0}^{k} p_l u_l = \sum_{l=0}^{k} \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l} \sqrt{\frac{X}{k}}(k-l)$$

  where $p_l = \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l}$,

  and $u_l = \sqrt{\frac{X}{k}}(k-l)$

  - l: k개로 나눈 것 중 반영되지 않은 것의 수
    p_l: k개 중 l개가 반영되지 않을 확률을
    u_l: k개 중 l개가 반영되지 않았을 때의 투표 영향력

  - 모든 가능한 l에 대한 p_l과 의 u_l의 곱에 대한 누계가 시빌 공격을 했을 때의 기댓값

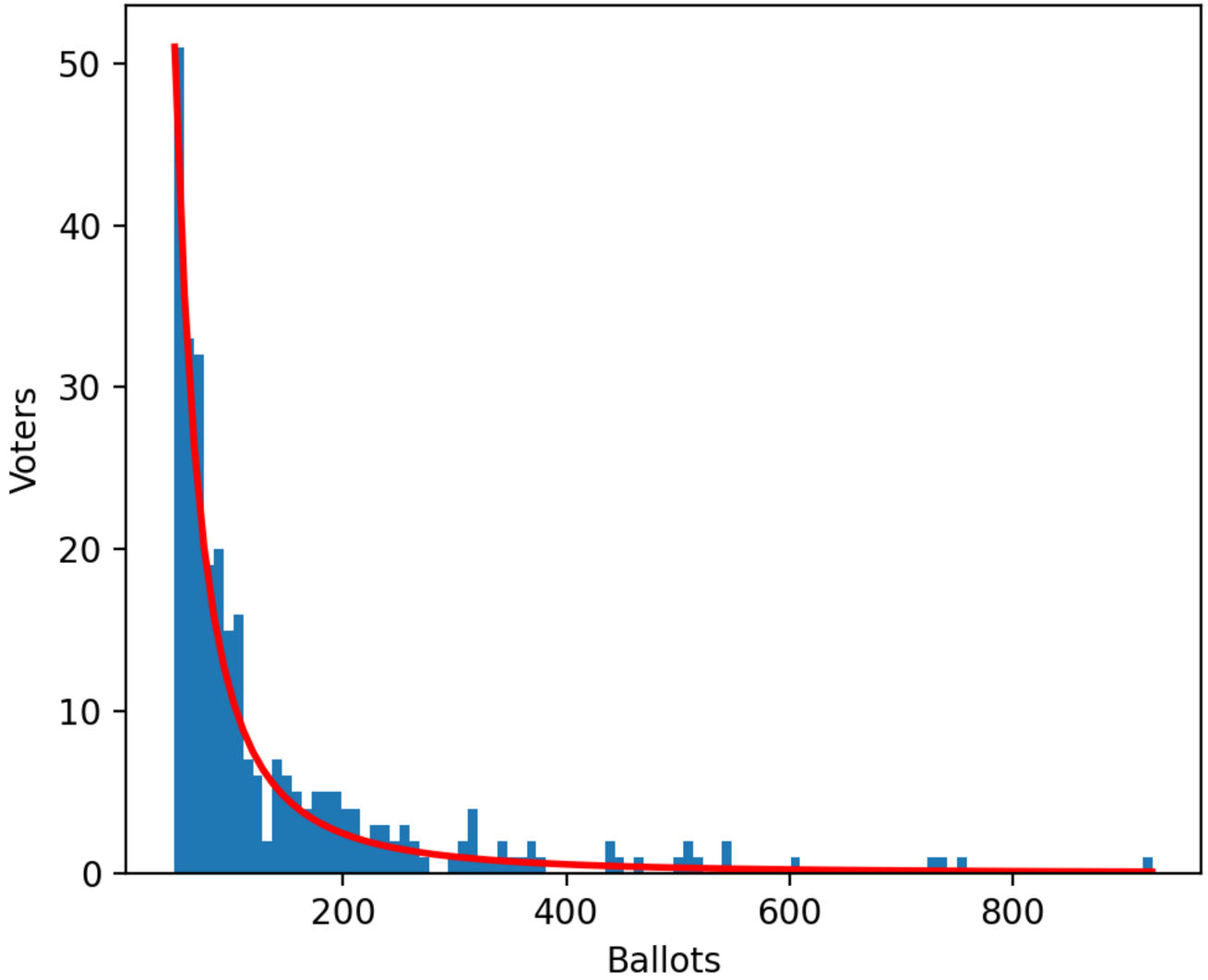
PROBABILISTIC QUADRATIC VOTING

- PQV에서 시빌 공격이 비효율적임을 보이는 부등식 및 조건
- $$\frac{X\sqrt{X}}{N} > \sum_{l=0}^{k} \binom{k}{l} \left(\frac{X/k}{N}\right)^{k-l} \left(1 - \frac{X/k}{N}\right)^{l} \sqrt{\frac{X}{k}}(k-l)$$
- 부등식이 항상 성립하기 위한 조건
- $\frac{kN}{X} \neq 0 \vee k > 1$
  - $k \geq 2, N \neq 0, X \neq 0$ 이므로 항상 만족됨
    - PQV의 이성적 참여자들은 투표권을 나누지 않으며, 시빌 공격을 행하지 않음

EVALUATION

EVALUATION

- 시뮬레이션 환경
  - 300명의 에이전트
  - 16개의 정책
    - 정책 선호도는 각기 0 또는 1
  - 총 100,000개의 투표권
    - 파레토(Pareto) 분포를 따르도록 300명의 에이전트들에게 분배

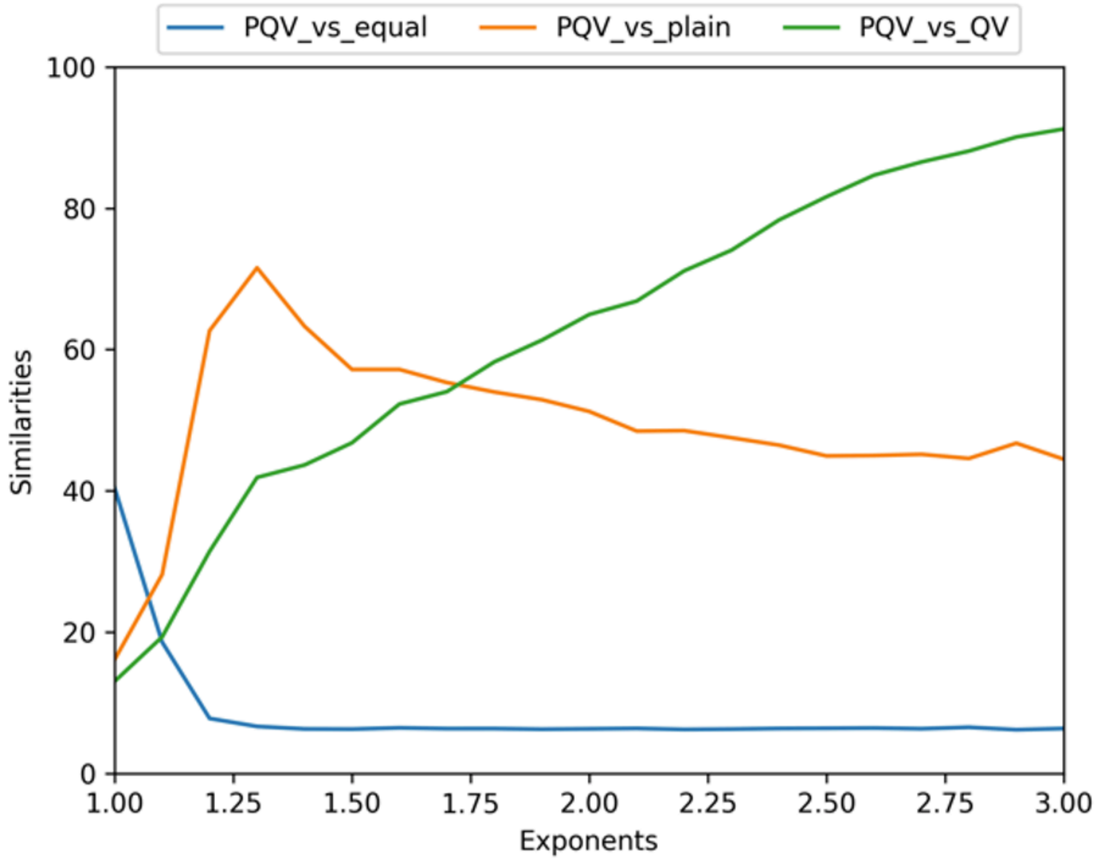


EVALUATION

- 한 실험에서 총 1,000,000 번의 라운드를 반복
  - 각 라운드마다 모든 에이전트가 참여해 투표가 이루어짐
  - 최종 집계 후 선정된 정책의 결과를 기록
    - 정책 간 유사도 기록 (일치하는지 여부를 기록)
  - 에이전트 간 파레토 분포를 초기화
- 100의 실험 후
  - 기록된 유사도 결과의 중앙값을 사용해 분석

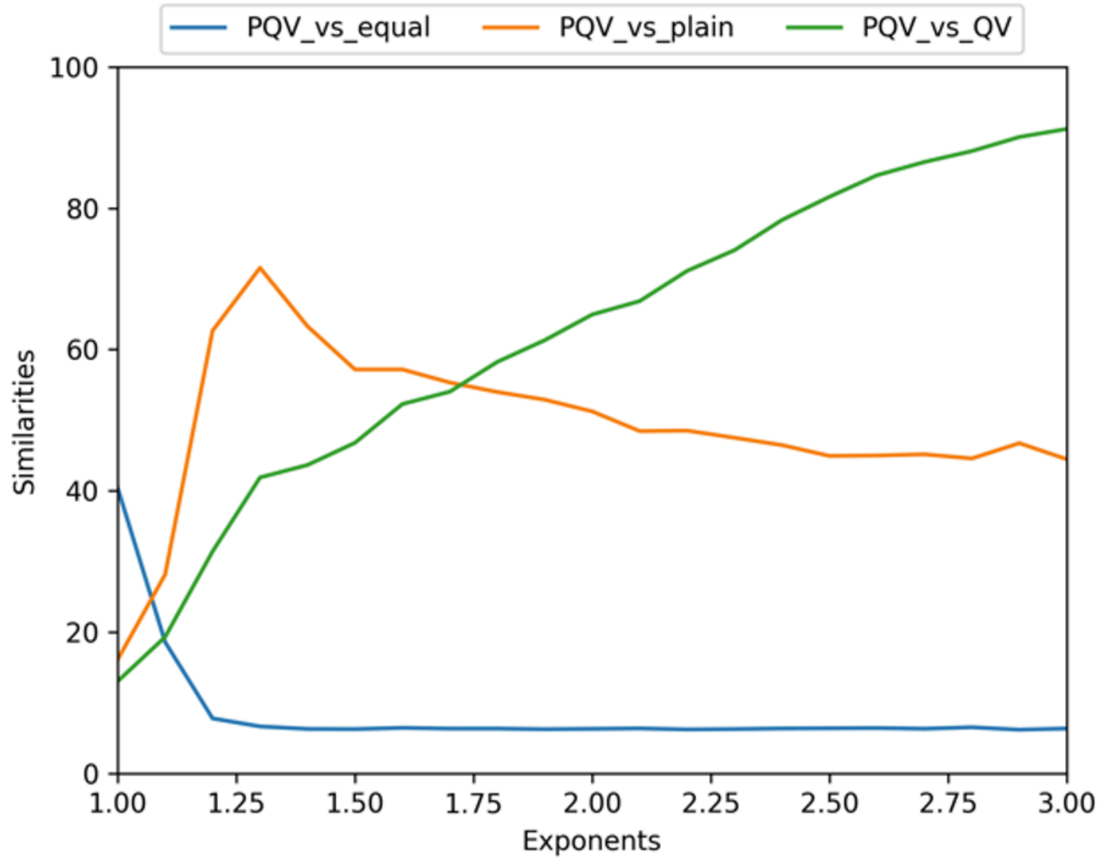
EVALUATION

- PQV와 다른 투표 방식 간의 결과에 대한 유사도
  - x축은 확률 가중치인 e를 나타냄
  - 1.0부터 3.0까지 0.1 간격으로 변화
- PQV vs 평등 투표
  - 투표 참여자의 의견을 충분히 반영할 수 없음
  - PQV와 낮은 유사도를 가짐



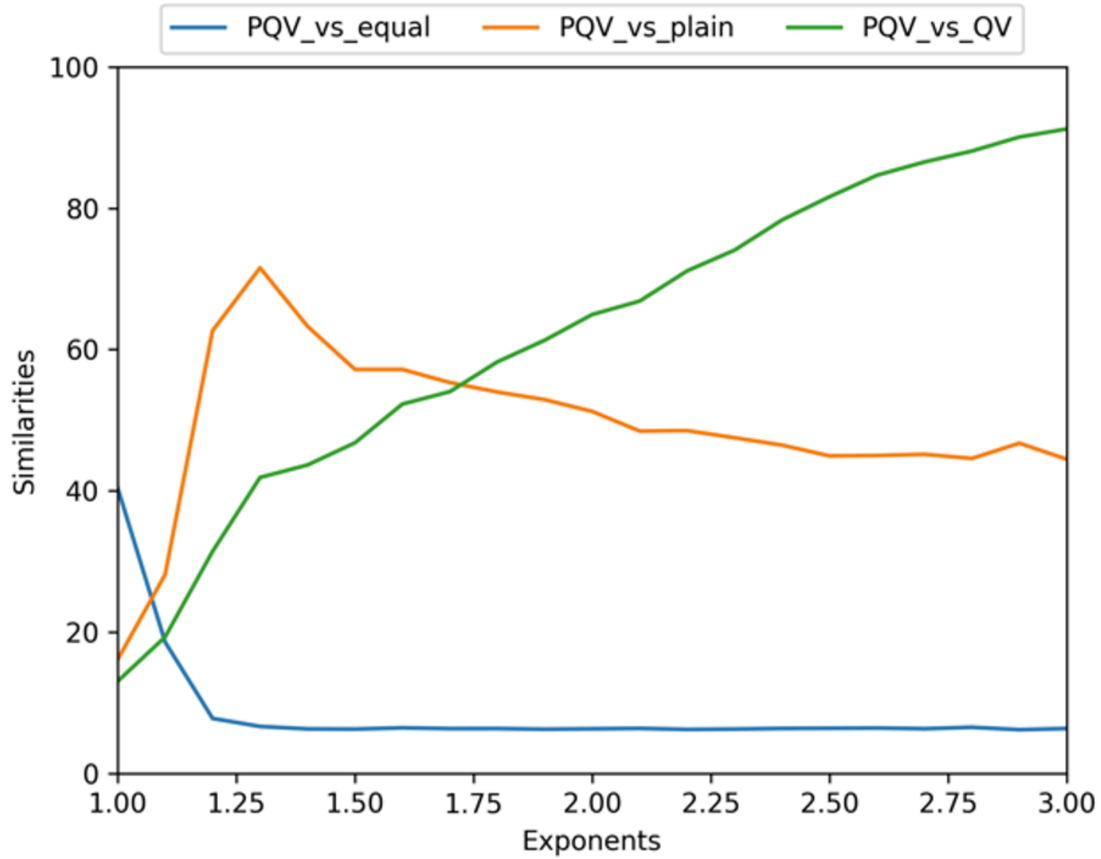
EVALUATION

- PQV vs 선형 투표
  - 의견을 반영할 수 있어 **상대적으로** 높은 유사도
    투표권이 많은 소수의 영향을 많이 받음
  - 높은 유사도를 보이지는 않음



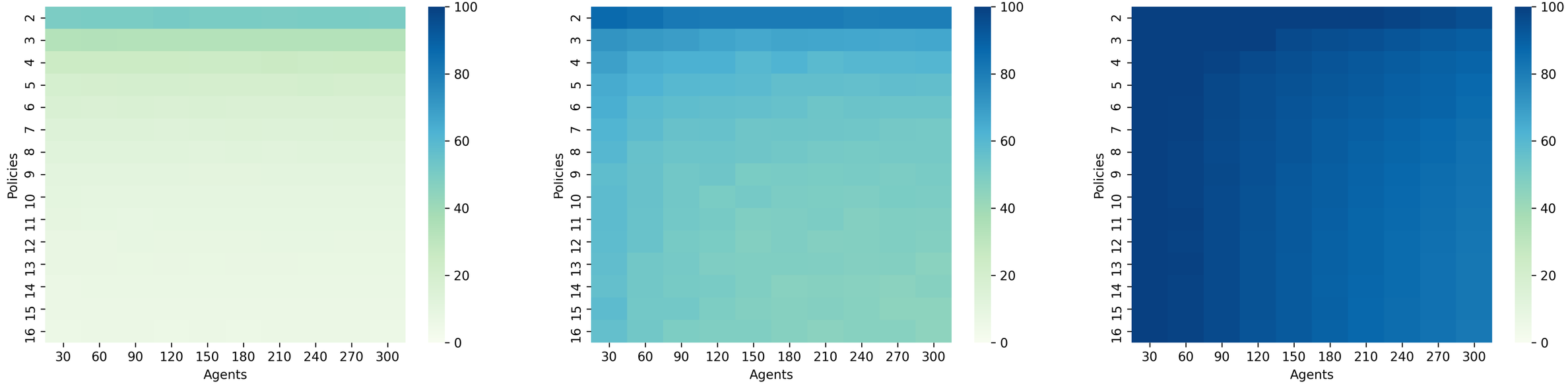
EVALUATION

- PQV vs 제곱 투표
  - e의 값이 증가함에 따라 유사해짐
  - 실제로 e가 무한대로 발산할 경우 제곱 투표와 동등한 결과로 수렴
  - 적절한 e를 사용할 경우 PQV가 제곱 투표를 잘 반영



EVALUATION

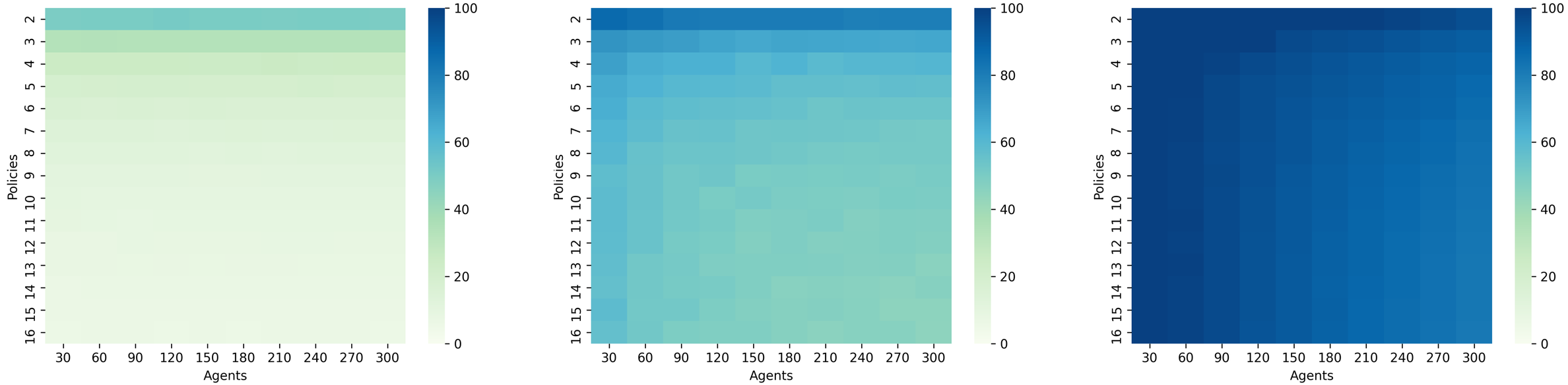
- 참여자 수와 정책 수에 따른 유사도 양상



- 참여자 수(x축)와 정책 수(y축)에 따른 유사도
- PQV 대 평등 투표(왼쪽), PQV 대 선형 투표(가운데), PQV 대 QV(오른쪽)
- $e = 2$

EVALUATION

- 참여자 수와 정책 수에 따른 유사도 양상



- 환경 변수와 관계 없이 평등 투표와 선형 투표는 PQV와 낮은 상관 관계를 가짐
- PQV와 제곱 투표와의 유사도는 높게 나타남
  - 다양한 환경에 대하여 PQV가 제곱 투표를 잘 반영함을 알 수 있음

CONCLUSION

CONCLUSION

- **확률적 제곱 투표(Probabilistic Quadratic Voting, PQV)**
  - 이성적 참여자는 기댓값이 높은 행동을 수행
  - 투표 참여자들이 시빌 공격을 수행하지 않도록 할 요인을 제공
- e의 값에 따른 QV와의 유사도 차이가 존재
  - 적절한 e의 값을 설정하면
  - PQV와 QV의 결과가 거의 유사하도록 만들 수 있음

CONCLUSION

- 블록체인은 특히 시빌 공격에 취약하므로
  - 시빌 공격에 의해 무력화 되는 QV 대신 PQV를 사용해
  - 블록체인의 무결성과 신뢰성을 보장받으면서
  - 다수결의 문제를 해결한 QV의 장점을 취할 수 있음

PROBABILISTIC QV

PROBABILISTIC QUADRATIC VOTING