Proof-of-Importance

https://youtu.be/B_k6pK6_rAo

PoI (Proof-of-Importance)

Importance Score

Future Work

PoI (Proof-of-Importance)

- NEM 암호화폐에서 사용하는 합의알고리즘 (XEM)
- PoS(Proof-of-Stake)의 단점을 해결하기 위하여 개발
- 기득 통화량, 코인 거래량, 노드 간 상호 연결도에 따라 채굴 확률이 증가한다.
- 즉, 네트워크 내 기여도에 따라서 달라지는 셈

- 채굴 과정

  블록 생성 (블록 당 1분 ±0.5s)

  -> 계정의 중요도 점수 계산

  -> 조건이 만족되었는지 확인 $hit < target$

  -> 채굴 완료

PoI (Proof-of-Importance)

$$hit = 2^{54}\left|\ln\left(\frac{h}{2^{256}}\right)\right|$$

$$target = 2^{64}\,\frac{b}{d}\,t$$

$$hit \;<\; target$$

$$h = H(generation\ hash\ of\ previous\ block,\ public\ key\ of\ account)$$

$$\qquad \text{interpreted as 256-bit integer}$$

$$t = time\ in\ seconds\ since\ last\ block$$

$$b = 8999999999\ \cdot\ (importance\ of\ the\ account)$$

$$d = difficulty\ for\ new\ block$$

$$d = \frac{1}{n}\sum_{i=1}^{n}(\text{difficulty of block i})$$

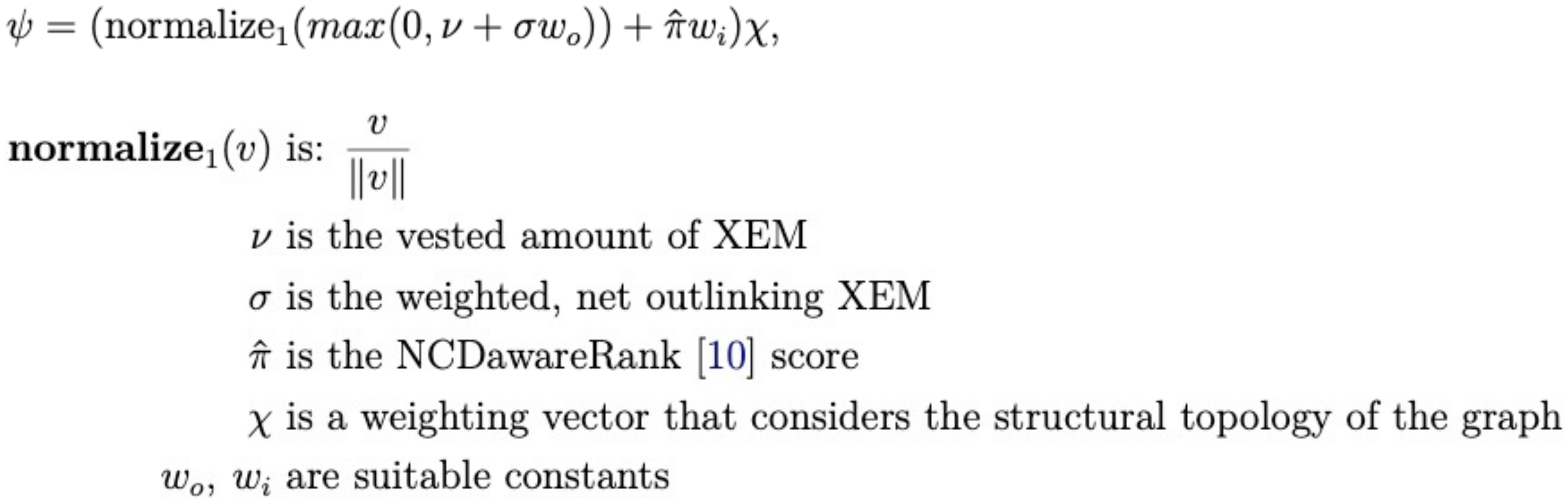
$$t = \frac{1}{n}\sum_{i=1}^{n}(\text{time to create block i})$$

$$difficulty = d\,\frac{60}{t}$$

Initial difficulty = 10^14

Importance Score

- Importance Score, ψ



$$\psi = (\text{normalize}_1(max(0, \nu + \sigma w_o)) + \hat{\pi} w_i)\chi,$$

$\textbf{normalize}_1(v)$ is: $\dfrac{v}{\|v\|}$

ν is the vested amount of XEM

σ is the weighted, net outlinking XEM

$\hat{\pi}$ is the NCDawareRank [10] score

χ is a weighting vector that considers the structural topology of the graph

w_o, w_i are suitable constants

w_o is 1.25 and w_i is 0.1337.

Importance Score

1. ν is the vested amount of XEM

매일 보유 XEM의 10%가 vested됨

* harvester가 되기 위해선 총 10,000 XEM이 vested 되어야 함 *

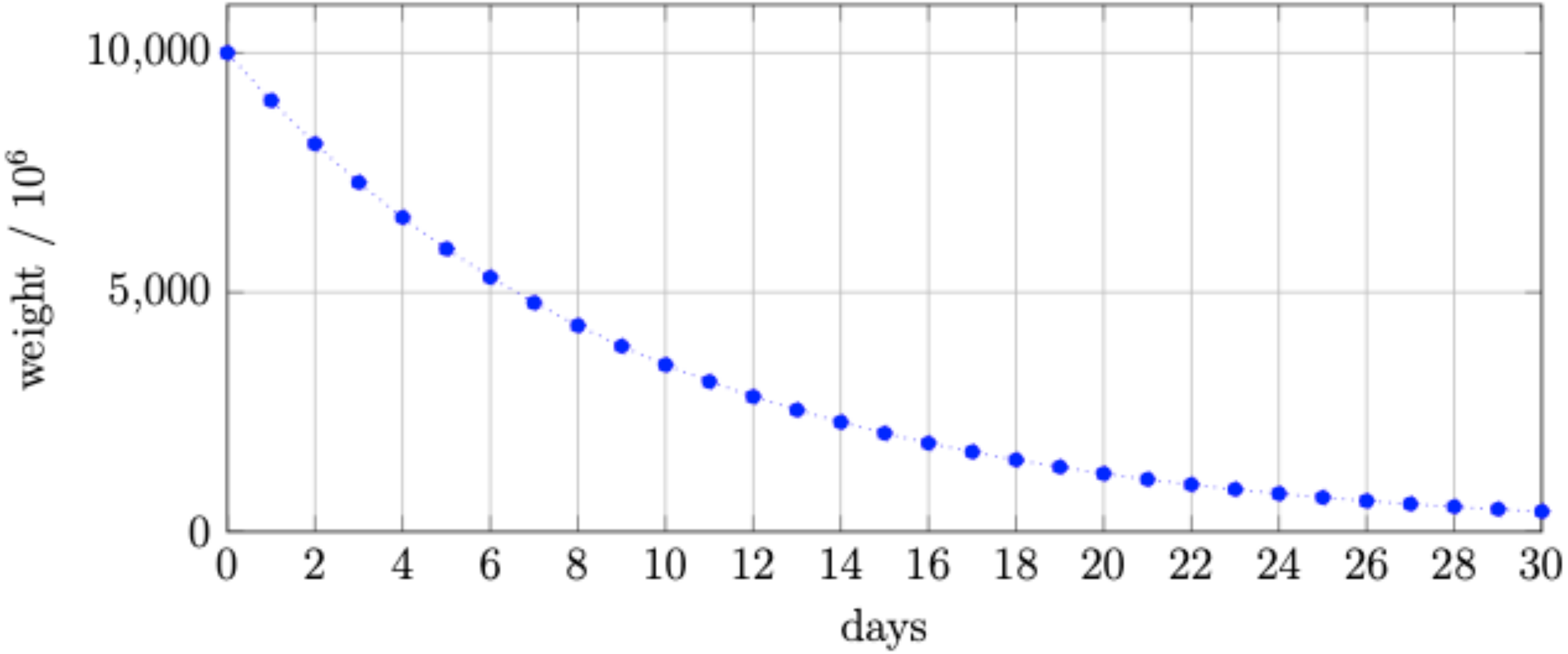


Figure 8: *amount decay of 10000 XEM*

Importance Score

2. σ is the weighted, net outlinking XEM

- Transferred an amount of at least 1,000 XEM
- Happened within the last 43,200 blocks (approximately 30 days)

Block weight

$$w_{ijk} = amount \cdot \exp\left(\ln(0.9)\left[\frac{h - h_{ijk}}{1440}\right]\right)$$

$$\widetilde{w}_{ij} = \sum_{k} w_{ijk}$$

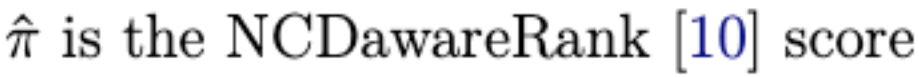
Weighted net flow => outlink matrix

$$\widetilde{o}_{ij} = \begin{cases} \widetilde{w}_{ji} - \widetilde{w}_{ij} & \text{if } \widetilde{w}_{ji} - \widetilde{w}_{ij} > 0 \\ 0 & \text{otherwise} \end{cases}$$

$$o_{ij} = \begin{cases} \frac{\widetilde{o}_{ij}}{\sum_i \widetilde{o}_{ij}} & \text{if } \sum_i \widetilde{o}_{ij} > 0 \\ 0 & \text{otherwise} \end{cases}$$

i, j: account
h: block-height
k: k-th Transaction

Importance Score

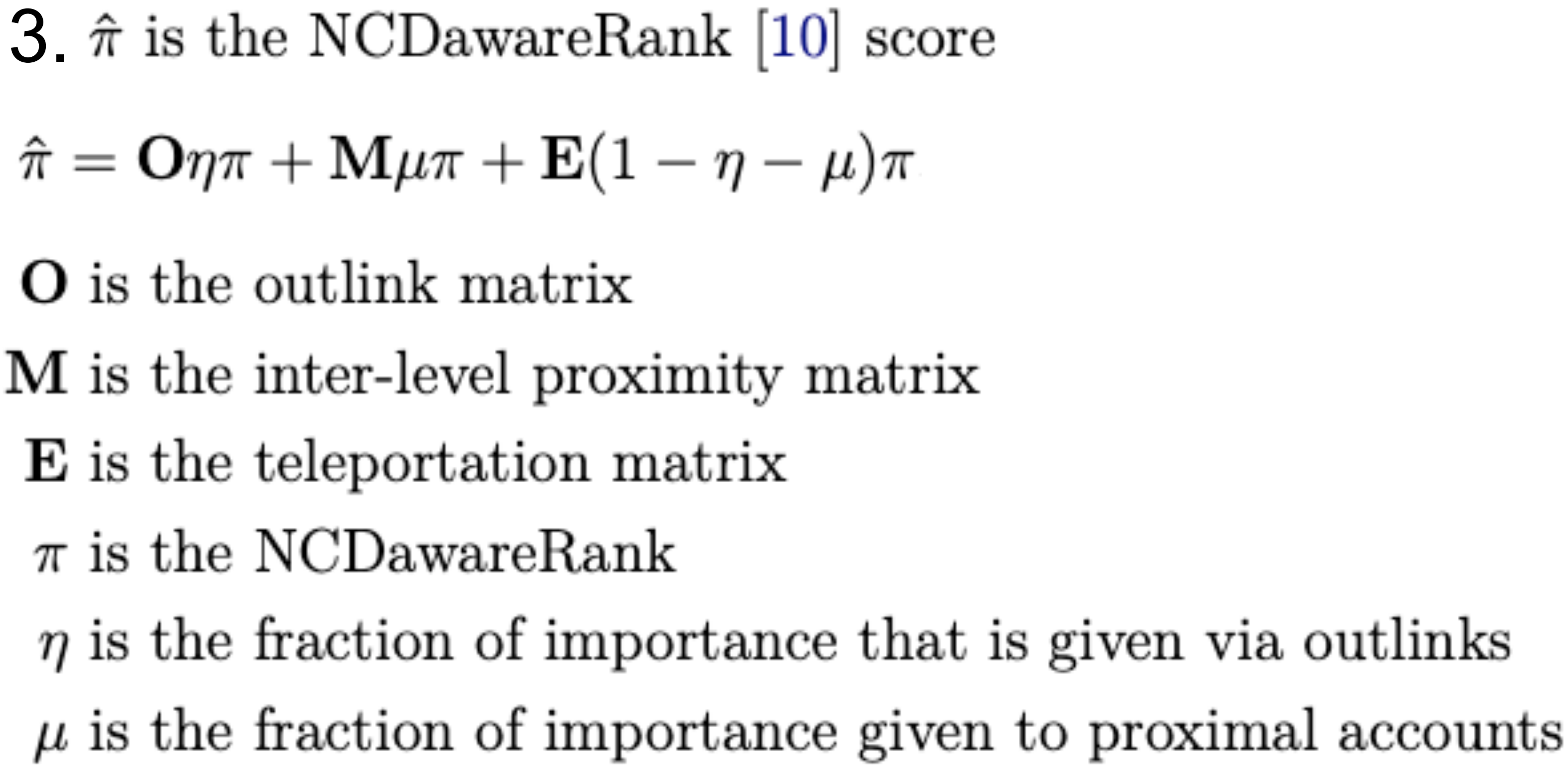
3. 

$\hat{\pi}$ is the NCDawareRank [10] score

- PageRank와 유사
- PageRank에 inter-level proximity matrix와 μ가 추가된 형태
- 그래프를 분해 가능한 구조로써 활용 가능

Importance Score

3.



$\hat{\pi}$ is the NCDawareRank [10] score

$$\hat{\pi} = \mathbf{O}\eta\pi + \mathbf{M}\mu\pi + \mathbf{E}(1 - \eta - \mu)\pi$$

$\mathbf{O}$ is the outlink matrix

$\mathbf{M}$ is the inter-level proximity matrix

$\mathbf{E}$ is the teleportation matrix

π is the NCDawareRank

η is the fraction of importance that is given via outlinks

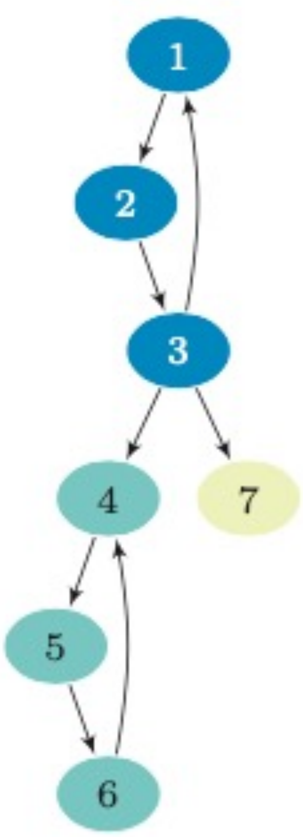
μ is the fraction of importance given to proximal accounts

(η is 0.7 and μ is 0.1) in NEM

Importance Score

- $\mathbf{M}$ is the inter-level proximity matrix

$$M_{v,u} \triangleq \begin{cases} \frac{1}{N_u \left| A_{(v)} \right|} & \text{if } v \in \chi_u \\ 0 & \text{otherwise} \end{cases}$$



$$\mathbf{M} = \begin{bmatrix} 1/3 & 1/3 & 1/3 & 0 & 0 & 0 & 0 \\ 1/3 & 1/3 & 1/3 & 0 & 0 & 0 & 0 \\ 1/9 & 1/9 & 1/9 & 1/9 & 1/9 & 1/9 & 1/3 \\ 0 & 0 & 0 & 1/3 & 1/3 & 1/3 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 1/3 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 1/3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- **W** is set of all **harvesting-eligible accounts.**
- For u ∈ W, **G$_u$** is the set of account that have received more in value transfers from account “u” than have sent “u”.
- **NCD (Nearly Completely Decomposable) blocks** of W are defined as **{A$_1$, A$_2$, A$_3$, …, A$_N$}**.
- **X$_u$** is the **proximal accounts** of each “u”
- **N$_u$** is the **number of NCD blocks** in X$_u$.

$$\chi_u \triangleq \bigcup_{w \in (u \cup G_u)} A_{(w)}$$

Importance Score

- Clustering the transaction graph

- **Γ** is the **set cardinality** and the set of **structurally connected accounts** (inclusive of self)

$$\Gamma(u) = \{v \in V \mid \{u, v\} \in E\} \cup \{u\}$$

- **σ** is the **similarity** between two accounts “u” and “v”

$$\sigma(u, v) = \frac{|\Gamma(u) \cap \Gamma(v)|}{\sqrt{|\Gamma(u)|\,|\Gamma(v)|}}$$

- **$N_\varepsilon(u)$** is the **set of structurally connected accounts** that have structural similarity with an account over a pre-determined threshold ε

$$N_\epsilon(u) = \{v \in \Gamma(u) \mid \sigma(u, v) \geq \epsilon\}$$

- **$K_{\varepsilon,\mu}(u)$** are **core nodes** that used for pivoting and expanding clusters

$$K_{\epsilon,\mu}(u) \Leftrightarrow |N_\epsilon(u)| \geq \mu$$

ε is 0.3 and μ is 4

Importance Score

- Direct structure reachability

$$u \mapsto_{\epsilon,\mu} v \Leftrightarrow K_{\epsilon,\mu}(u) \wedge v \in N_{\epsilon}(u)$$

- Account that are two-hops away from the pivot accounts

$$H(u) = \{v \in V | (u,v) \notin E \wedge (v,w) \in E)\}$$

Importance Score

- $\mathbf{E}$ is the teleportation matrix

$$\mathbf{E} \triangleq \mathbf{e}\mathbf{v}^{\intercal}$$

- “**e**” is the vector with all components set to 1.
- “**v**$^{\mathsf{T}}$” is a teleportation probability vector.

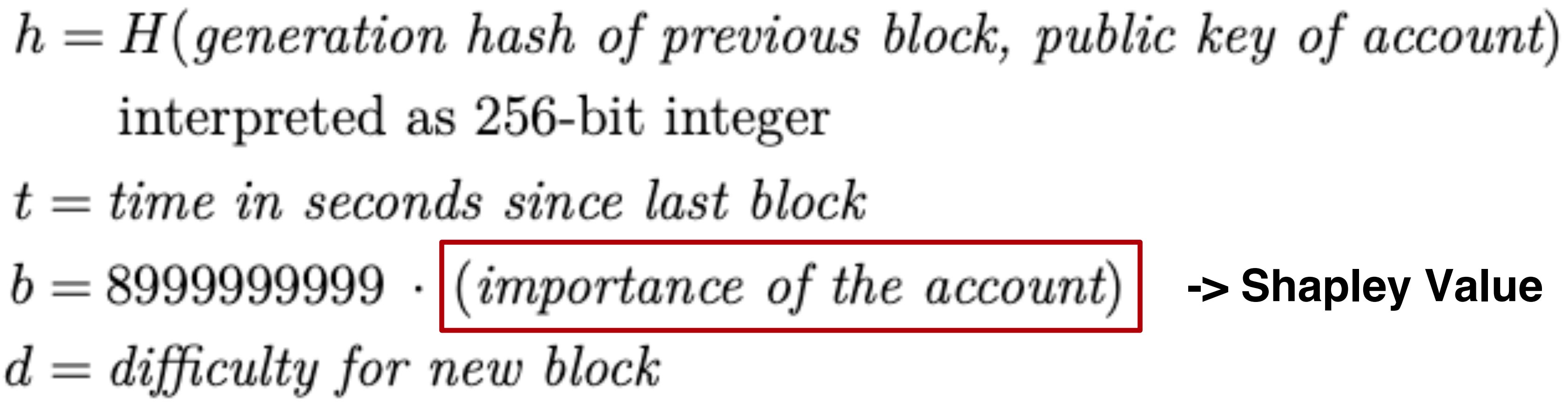
Importance Score

π is the NCDawareRank

$$NCDawareRank^{r}(i) = (1-\eta-\mu)\frac{1}{|G|} + \eta\sum_{k=1}^{s} o_{ik}\, NCDawareRank^{r-1}(k) + \mu\sum_{k=1}^{s} m_{ik}\, NCDawareRank^{r-1}(k)$$

$$\left(\sum_{i \epsilon G}\left|NCDawareRank^{r}(i) - NCDawareRank^{r-1}(i)\right|\right) < \varepsilon$$

Future Work



$h = H(\textit{generation hash of previous block, public key of account})$

$\quad$ interpreted as 256-bit integer

$t = \textit{time in seconds since last block}$

$b = 8999999999 \cdot \boxed{(\textit{importance of the account})}$ -> **Shapley Value**

$d = \textit{difficulty for new block}$

Q & A