MONASH University

Time-dependent Decision-making and Decentralization in Proof-of-Work Cryptocurrencies

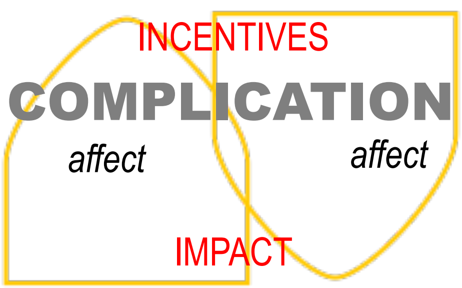
Yevhen Zolotavkin, Julian Garcia, Joseph Liu

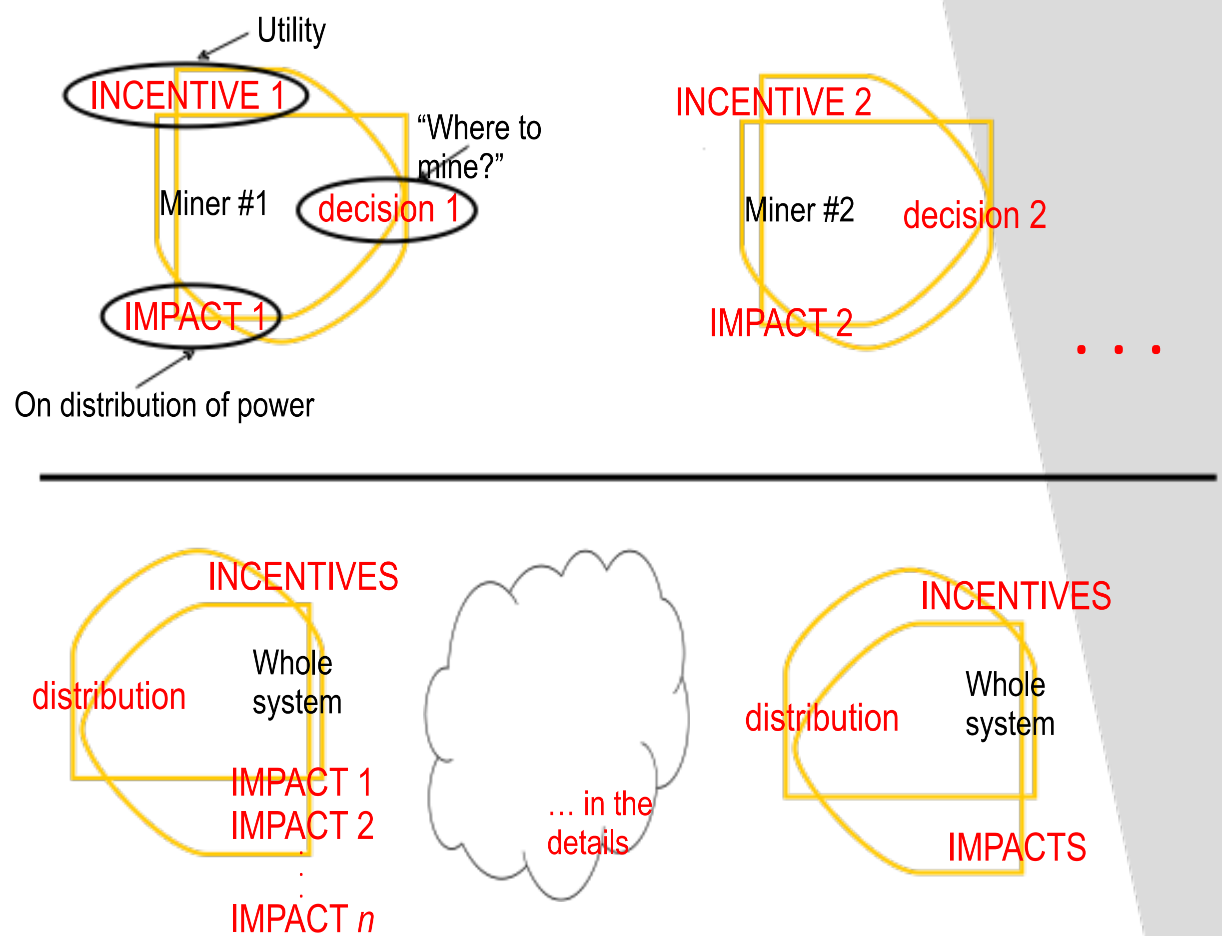
CSF 2019

Main points of the paper

Without miners PoW consensus is impossible

What are the INCENTIVES and IMPACT of the miners?





Incentives and their properties

1. Decision/action of a miner at every moment can be expressed using utility

2. Utility of a miner depends on her past performance and future performance of the pool

Why? Because pools use reward systems that encourage loyal and steady mining behavior

Already defined in PROP, PPLNS, etc.

Why? Because it is important to know how (slow / fast) miners will be rewarded

Needs to be expressed in formal way – **How?**

3. Future is unknown. Miners must have beliefs to calculate utility and make decisions.

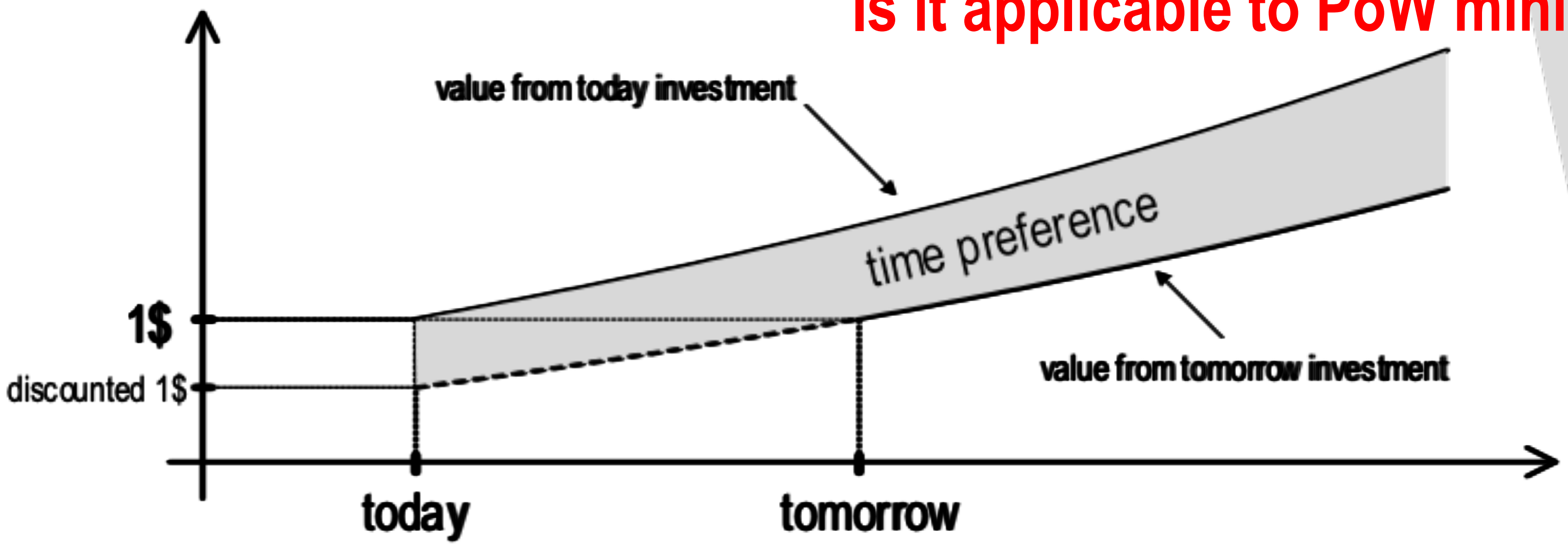
4. **Problems**: a) the space of beliefs is unknown; b) beliefs must be consistent

Future compensations

Utility for mining in a PPLNS pool → *time discounting*

What is more valuable: 1$ received today OR 1$ received tomorrow?

Is it applicable to PoW mining market?



1$ invested today generates profit in the future… similarly, 1$ invested tomorrow…

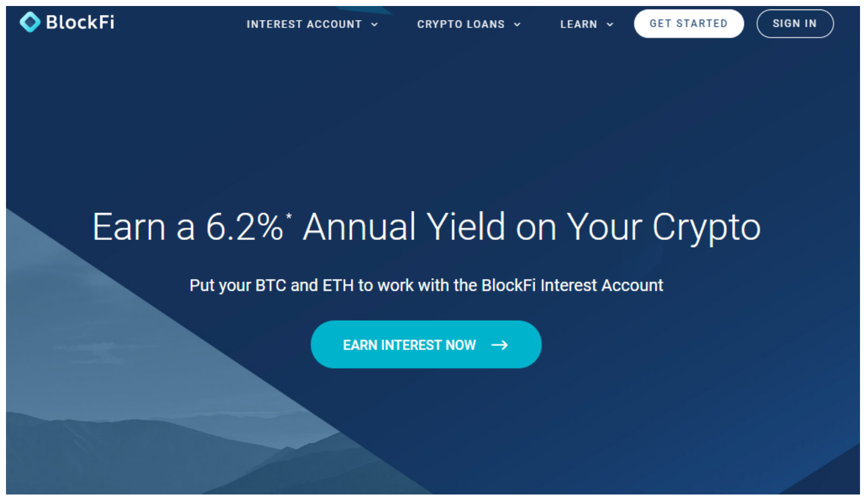
however, today investment outperforms tomorrow investment… therefore, today we should discount tomorrow reward…

and, hence, express time preference in monetary terms.

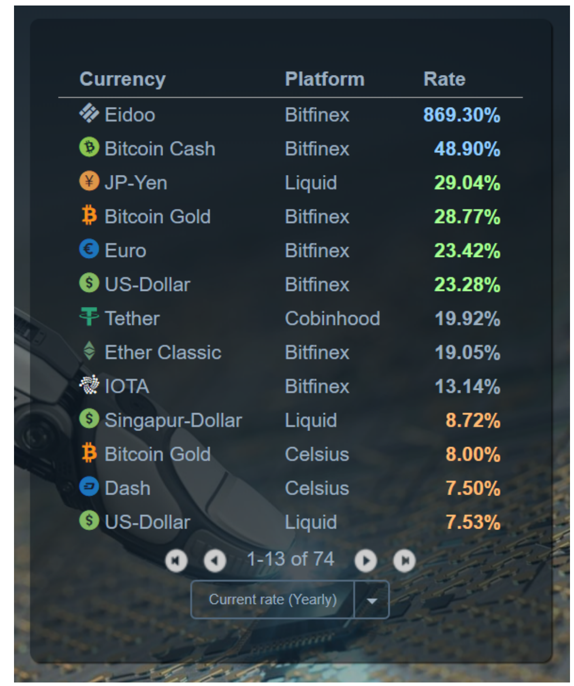
Investment opportunities for cryptocurrencies

For example, we can use exponential model e^{-kn} to discount reward that is deferred *n* days.

BlockFi (https://blockfi.com/crypto-interest-account/)



Coinlend (https://www.coinlend.org/)

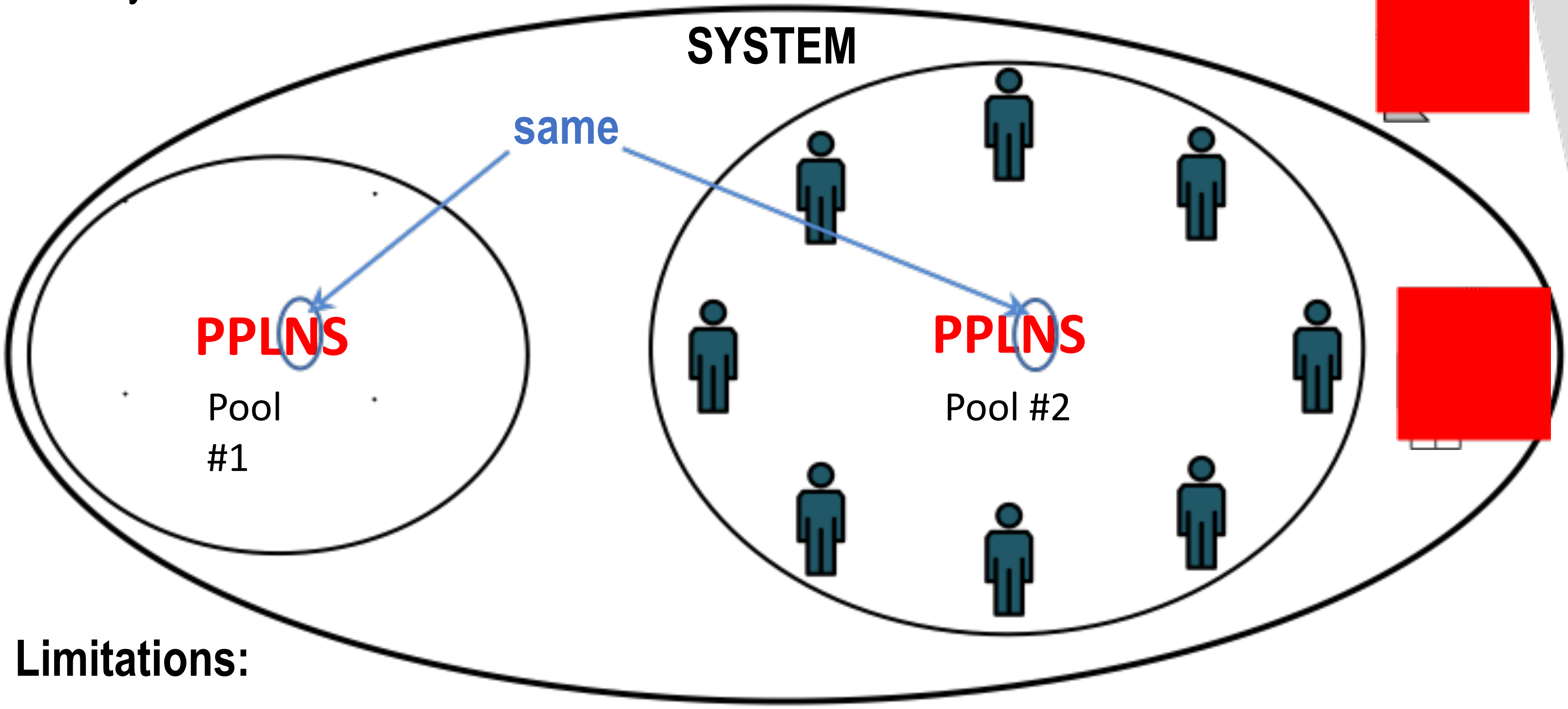


With 6.2% of annual yield we calculate parameter $k = \frac{ln(1.062)}{365} \approx 1.65 \times 10^{-4}$.

Further: we demonstrate that intensity of time discounting plays important role in decentralization of blockchain.

Settings and Limitations

The system consists of Pool #1 and Pool #2



Limitations:

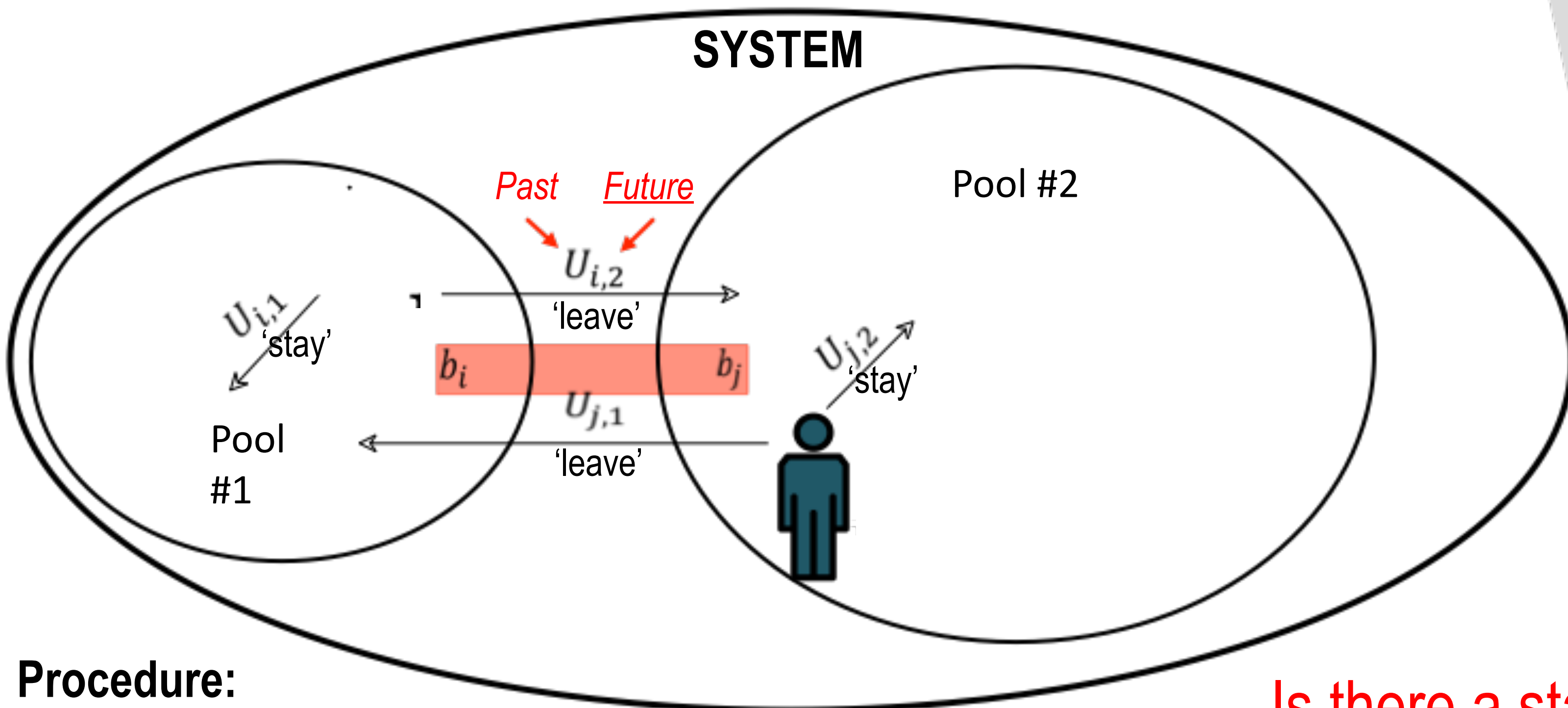
A. We consider a closed system of 2 pools

B. We consider Pay Per Last *N* Shares (PPLNS) pools only

C. Parameter *N* is the same for the both pools

Incentives and Decisions

Miners may move between the pools based on their <u>best response</u> $b_i, b_j \in \{0,1\}$



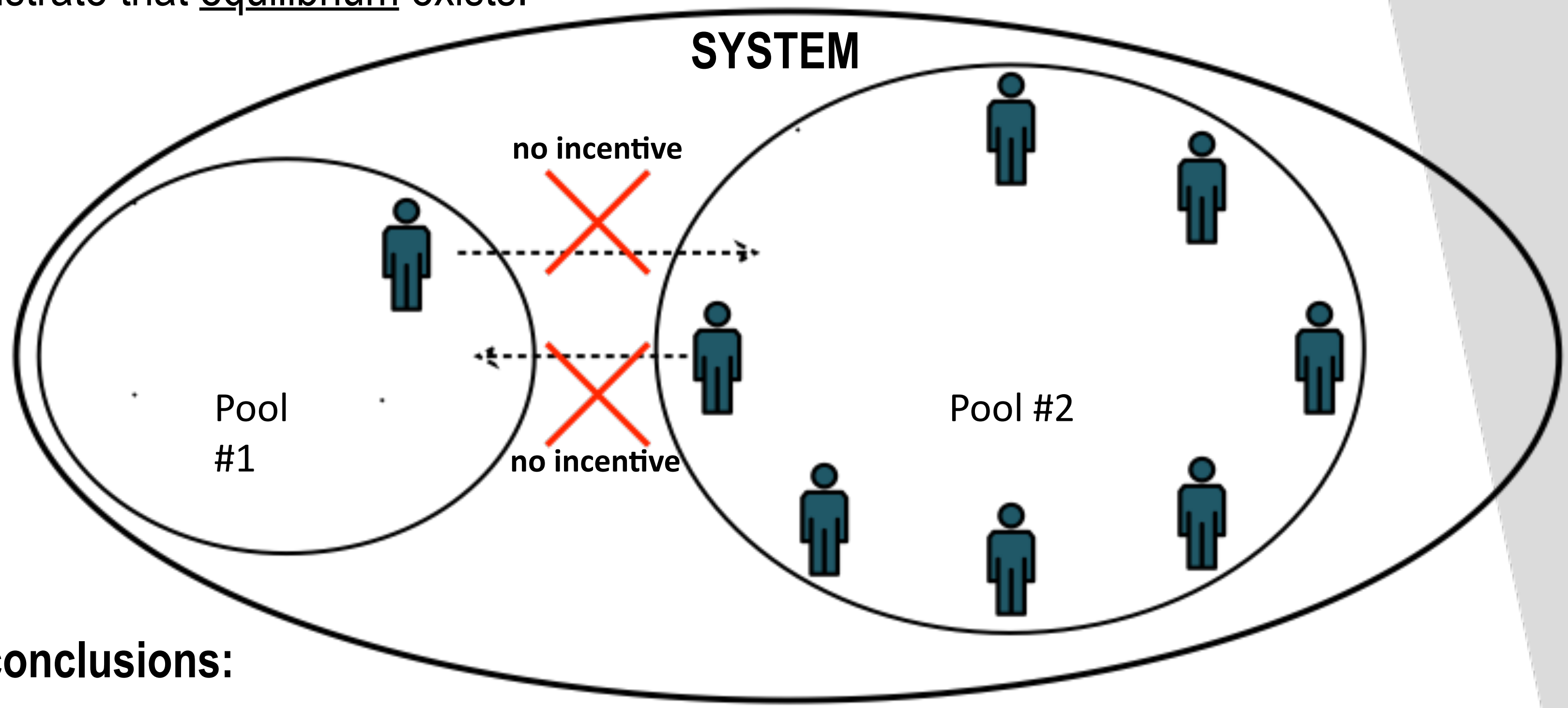
Procedure:

1. Calculate <u>utilities</u> to 'stay' and to 'leave' for each of the miners;
2. Make <u>decision</u> for each miner based on which utility is larger.

Is there a state of stability?

Equilibrium in the system

Assumption about personal beliefs allowed us to reason about utilities, best responses, and to demonstrate that equilibrium exists.



Brief conclusions:

A. Miners tend to leave the smaller pool.

B. Composition of the smaller pool and intensity of time discounting do matter.

The rest of the presentation

In order to understand effects of possible migration between the pools we are going to **discuss**:

- PoW mining in the pools

- PPLNS reward scheme

- Utility of the miners in PPLNS pools

- Simplifying assumptions about beliefs

- Algorithm to find equilibrium

- Simulation and discussion

Purpose of PoW mining: BitCoin

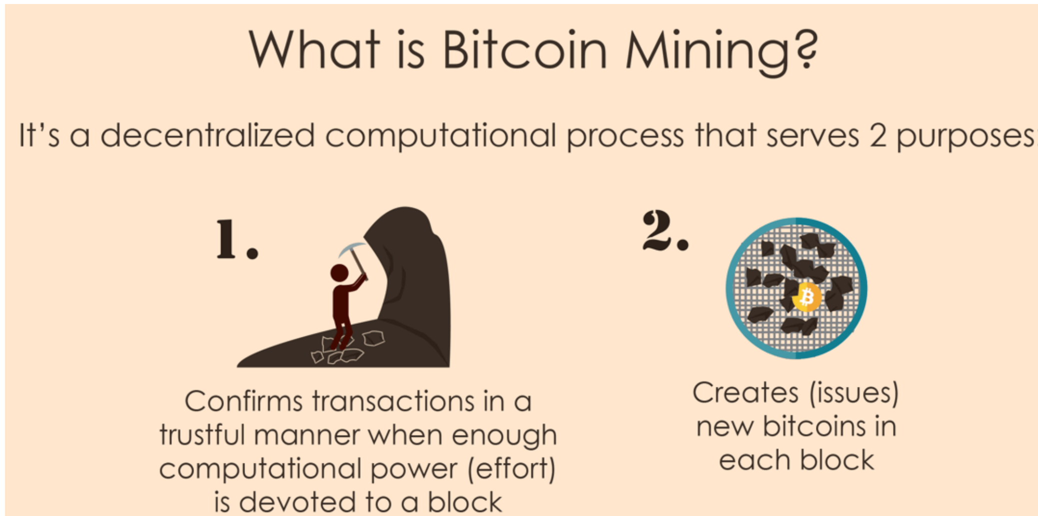


image source: www.weusecoins.com

Bitcoin community awards miners with a standard reward (which is being halved every several years, now it is 12.5 BTC) plus 1.4 BTC on average collected from the fees of transactions included in the block.

Miners are incentivized by new coins but they have to follow the procedure.

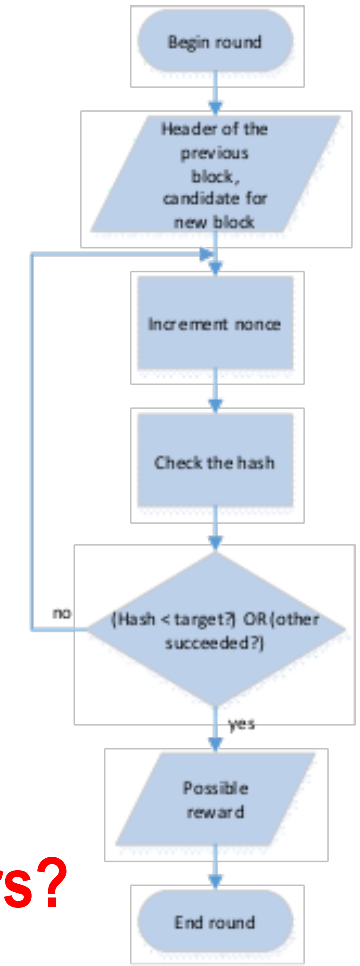
Simplified procedure of block mining

Solving puzzle is the most computationally intense stage

image source: www.weusecoins.com

A round of puzzle solving

Ability to organize parallel computations is the core reason for popularity of PoW mining pools



Partial solutions are allowed in the pools and are called “shares”.

Why is that important for the miners?

Differences in mining power

Not all miners are equal.   Mining difficulty is rising constantly…

As a result, smaller miners may experience significant income variance in case of solo mining.

image source: www.weusecoins.com

Mining farm

image source: www.flickr.com

“Poor man’s” mining equipment

Pools attract miners as they provide steady income (lower variance).

Contribution of the pools to PoW mining

Pools are extremely important for BitCoin network.

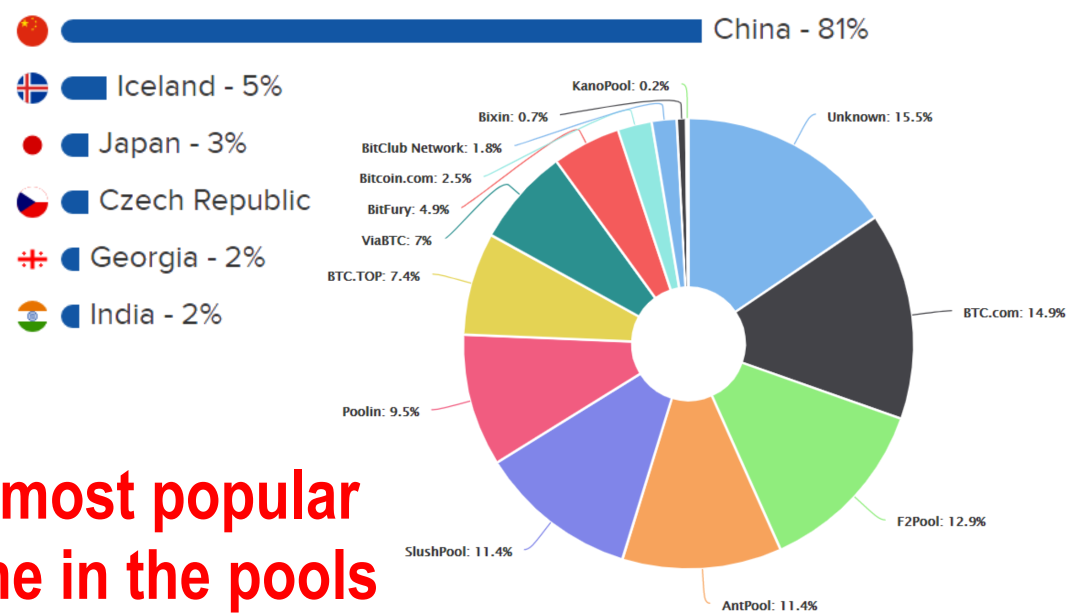


image source: https://blockchain.info

PPLNS is the most popular reward scheme in the pools

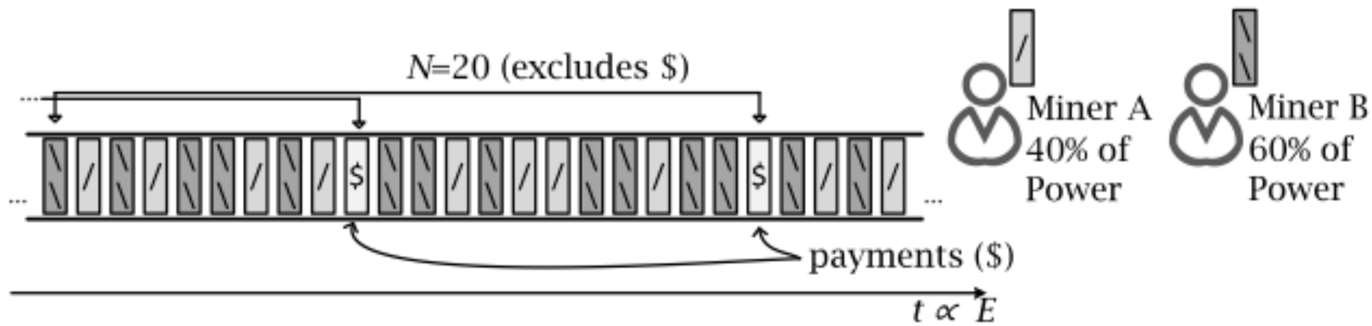
Name	Reward Type
AntPool	PPLNS & PPS
BTC.com	FPPS
BCMonster.com	PPLNS
Jonny Bravo's Mining Emporium	PPLNS
BitcoinAffiliateNetwork	?
Slush's pool (mining.bitcoin.cz)	Score
BitMinter	PPLNSG
BTCC Pool	PPS
BTCDig	DGM
btcmp.com	PPS
BW Mining	PPLNS & PPS
Eclipse Mining Consortium	DGM & PPS
Eligius	CPPSRB
F2Pool	PPS
GHash.IO	PPLNS
Give Me COINS	PPLNS
KanoPool	PPLNS
Merge Mining Pool	DGM
Multipool	Score
P2Pool	PPLNS
PolMine	SMPPS
MergeMining	PPLNS

Many of the reward systems calculate miners' payoffs based on the distribution of their shares in time.

Reward principle of PPLNS

Miners share reward from the full solution in proportions to the numbers of shares that each of them submitted among the most recent *N* shares.

For example, on this scheme we can see that the latest reward is ought to be divided among *N*=20 shares where 8 shares were submitted by miner A and 12 shares were submitted by miner B. In “stable mining”, in expectation, reward is proportional to the individual power of a miner.



However, in order to understand incentives to migrate we need to consider marginal utility of a miner from mining one more share in the pool. It will be demonstrated that <u>*N*</u> and the <u>total power of the pool</u> play important role.

Utility of *miner A* – continuous model (part 1)

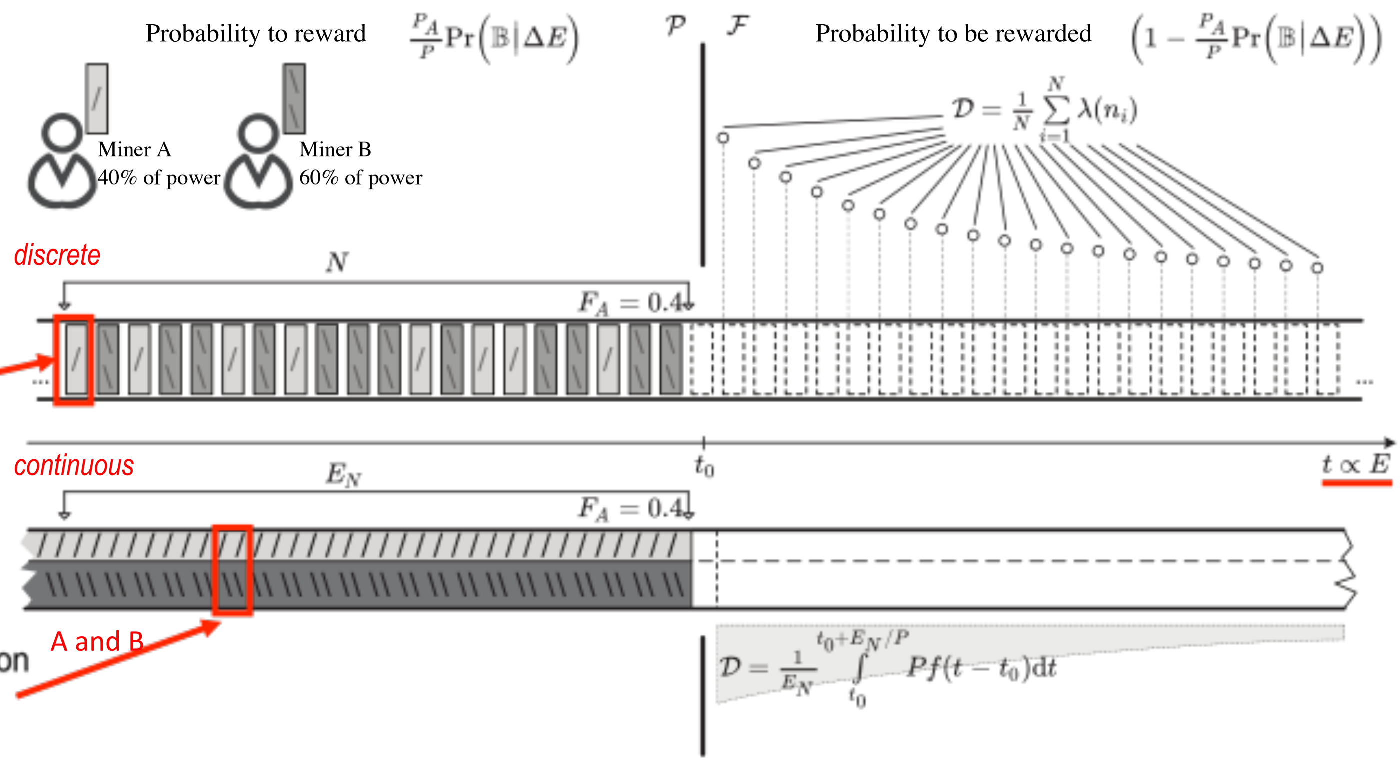
Analogy between discrete and continuous models for mining in PPLNS pool

Energy ΔE is spen…

Assume that produ…

Discrete: Energy ΔE is spent on a a share which is produced by either *miner A* or *miner B*.

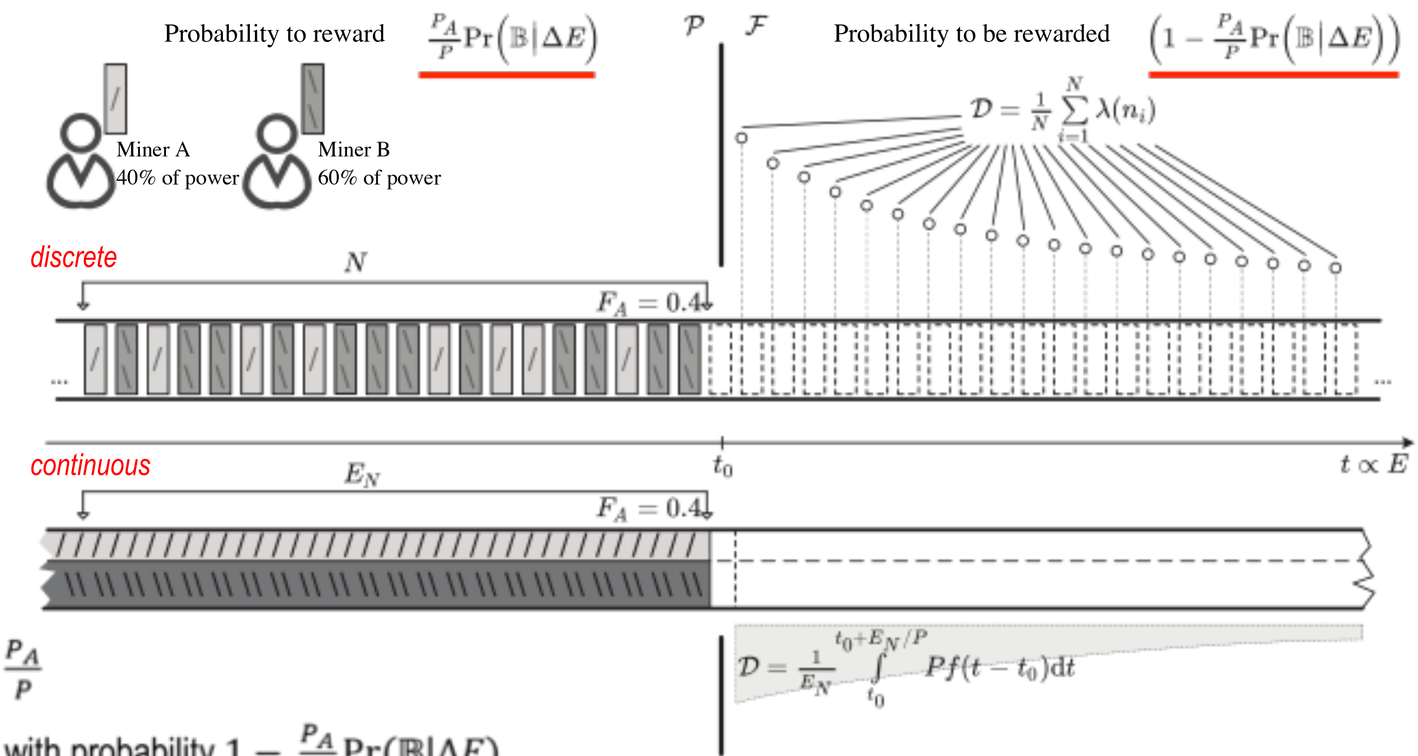
Continuous: each ΔE has a portion that is contributed by *miner A* as well as the portion contributed by *miner B*.



Utility of *miner A* – continuous model (part 2)

Probability to find

Fraction of mini



Probability that *miner A* brings reward to the pool during Δt is $\frac{P_A}{P}\Pr(\mathbb{B}|\Delta E)$.

If this does not happen, *her* contribution $\Delta E \frac{P_A}{P}$ will be rewarded in the future. This happens with probability $1-\frac{P_A}{P}\Pr(\mathbb{B}|\Delta E)$.

Utility of *miner A* – continuous model (part 3)

Among the past *N* s

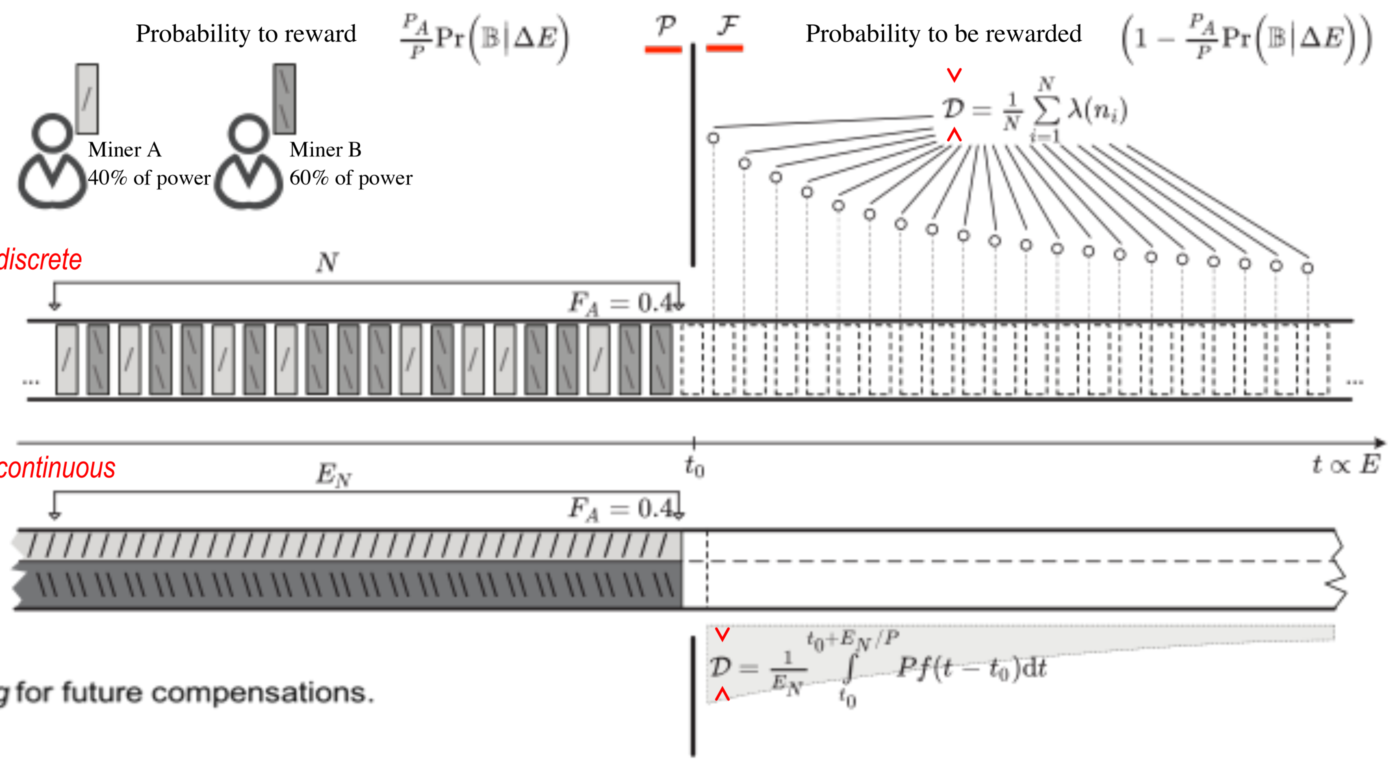
Therefore, *miner A* expects to reward

her **Past** with $R\frac{P_A}{P}F_A\Pr(\mathbb{B}|\Delta E)$,

and to get rewarded in the **Future** with

$R\frac{P_A}{P}\Pr(\mathbb{B}|\Delta E)\left(1-\frac{P_A}{P}\Pr(\mathbb{B}|\Delta E)\right)\mathcal{D}$,

where $\mathcal{D}$ is the coefficient of *time-discounting* for future compensations.



Decision of a miner in the system of two pools

How to express migration between 2 pools?

For a system that consist of a single pool, util

We introduce disjoint sets $\mathbf{M}_1$ and $\mathbf{M}_2$ to denote pool membership

Decision logic: at t_0 miner selects the pool where her utility is larger. Denote $U_{i,1}$ and $U_{i,2}$ utilities of miner i in pools #1 and #2, respectively. For simplicity, we use $\widetilde{U}_i, \widetilde{U}_j$ such that $\mathrm{sgn}(\widetilde{U}_i) = \mathrm{sgn}(U_{i,1} - U_{i,2})$ and $\mathrm{sgn}(\widetilde{U}_j) = \mathrm{sgn}(U_{j,1} - U_{j,2})$. We search for equilibrium:

$$\forall i,j \Big(\big((i \in \mathbf{M}_1) \vdash (\widetilde{U}_i \geq 0) \big) \wedge \big((j \in \mathbf{M}_2) \vdash (\widetilde{U}_j \leq 0) \big) \Big).$$

Simplified utilities $\widetilde{U}$ and $\widetilde{U}$ are defined as

$$\widetilde{U}_i = F_{i,1} + D$$

where are the fractions of past contributions in #1 and #2, resp.

and, are *time-discounting* coefficients in #1 and #2, resp.

Time-discounting coefficients are affected by the moves of other miners who have beliefs about the future.

MONASH University

Assumptions, beliefs and their effects

Assumption: All the miners have identical beliefs about the fu

System of beliefs:
1) Every miner makes at most 1 move;
2) Larger pool remains always larger.

⇨ *Proofs* ⇨ **CONSISTENT**

Effects on the system: a) there is an equilibrium which is ach

simplifies reasoning and computations

How does this help in finding equilibrium?

We still need to analyze decisions of the other miners, but… ⇨

Time-discounting coefficients

Without the loss of generality, total mining power of 2 pools is 1.

Unknown mining power of pool #1, P_1 , affects how fast a miners will be compensated. As a result, this influences *time-discounting* coefficients and we have:

$$\mathcal{D}_{1,i} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/P_1} P_1 f(t-t_0)\mathrm{d}t \quad , \quad \mathcal{D}_{2,i} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/(1-P_1+p_i)} (1-P_1+p_i) f(t-t_0)\mathrm{d}t \quad ;$$

$$\mathcal{D}_{1,j} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/(P_1+p_j)} (P_1+p_j) f(t-t_0)\mathrm{d}t \quad , \quad \mathcal{D}_{2,j} = \frac{1}{E_N} \int_{t_0}^{t_0+E_N/(1-P_1)} (1-P_1) f(t-t_0)\mathrm{d}t \quad ;$$

where $f(t-t_0)$ is the time-discounting function. For *the exponential model* we have

$$f(t-t_0) = = f(E-E_0) = e^{-\theta\frac{E-E_0}{E_N}}.$$

How to desian efficient method

Properties of the model

Assumption that there is an equilibrium at some point t^*, $t^* \geq t_0$,

We improve computational efficiency if we take into account the following properties (*proofs*):

1) None of the miners from larger pool (pool #2) has an incentive to join smaller pool;

2) $\forall E', E''(E'' \geq E' \geq E_0) \vdash \left(\mathbf{M}_2^{E'} \subseteq \mathbf{M}_2^{E''}\right)$, e.

3) $\forall \theta \left((\theta \leq 0.5) \vdash \left(\partial \frac{\widetilde{U}_i}{} \geq 0 \right) \right)$, e.g. in pool #1, i

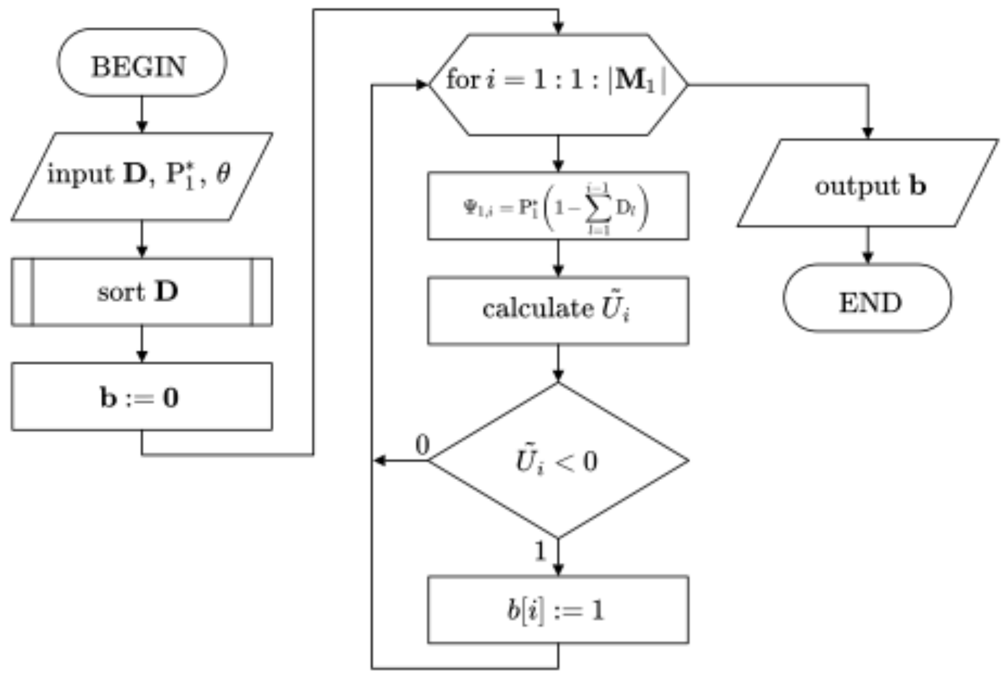
As a result, we can find equilibrium using

Algorithm to find equilibrium

P_1^* -- Total power of pool #1 pri

$\mathbf{D} = \{D_1, D_2, \dots, D_n\}$ – norma

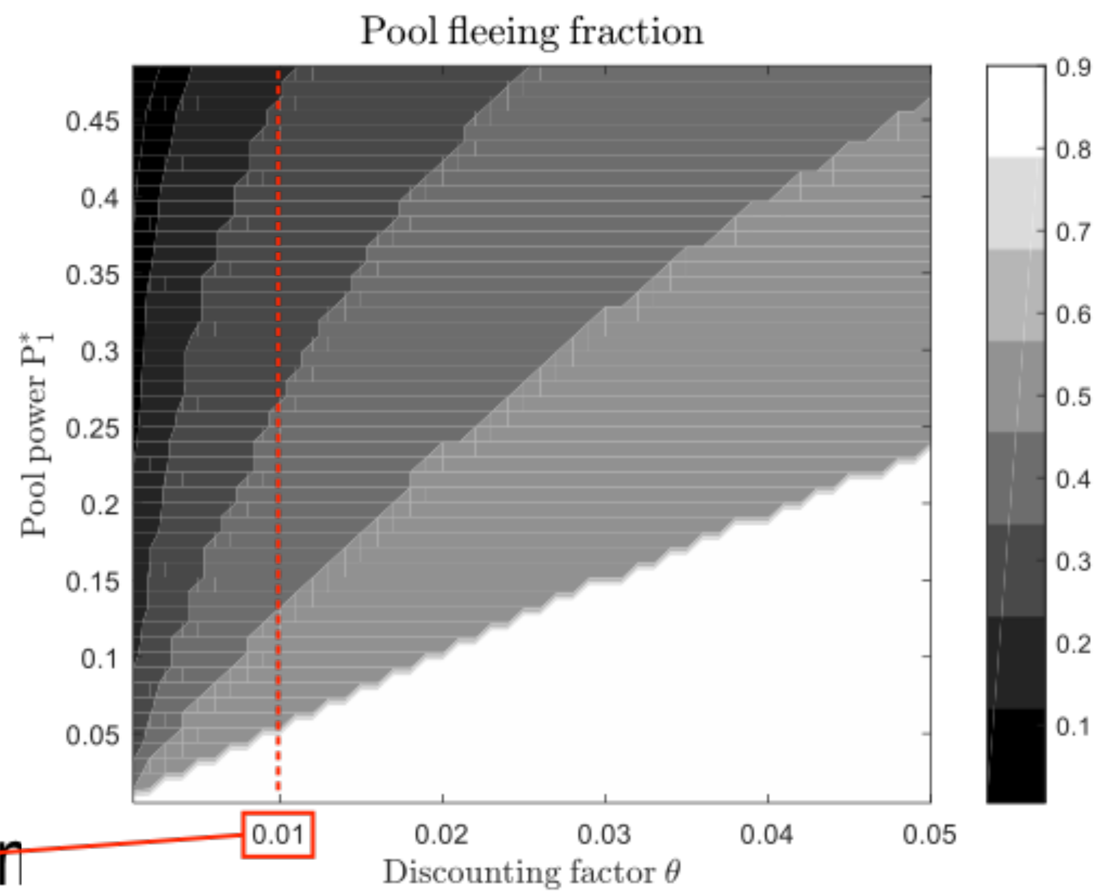
θ – time-discounting factor;



Experimental results

Distribution of mining power inside 'Kano' pool

Power range		Number of miners	Total power
$p_{\min}$	$p_{\max}$		
4.3×10^{-8}	0.0048	692	26.29%
0.0053	0.0081	7	4.36%
0.0102	0.015	4	4.93%
0.0166	0.0185	2	3.51%
0.0247	0.0247	1	2.47%
0.0374	0.0374	1	3.74%
0.0443	0.0443	1	4.43%
0.0706	0.0706	1	7.06%
0.1875	0.1875	1	18.75%
0.2445	0.2445	1	24.45%



Some medium/small po

Example: with $\theta = 0.01$ a n

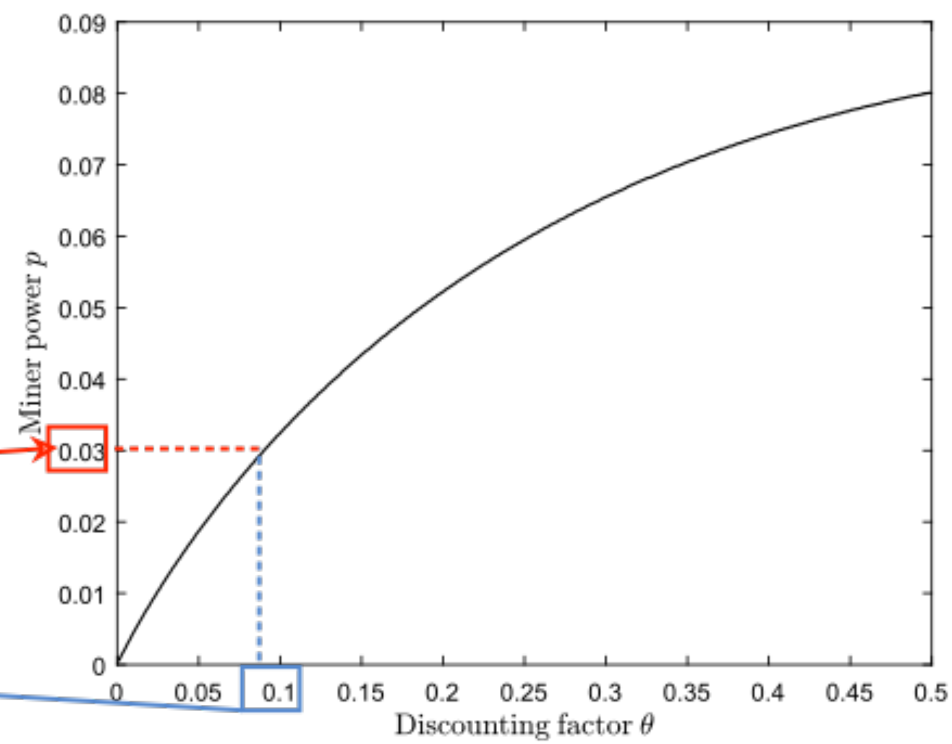
Is there a way to protect smaller pool?

MONASH University

Sufficient Individual Power (SIP)

However, we need such p_1 th

This is expressed as:



Example: composing pool #1 out of miners with individual power greater than 3% of total system power would be sufficient to protect the pool in a quite competitive investment environment.

What are the consequences for miners if SIP is not achieved ?

MONASH University

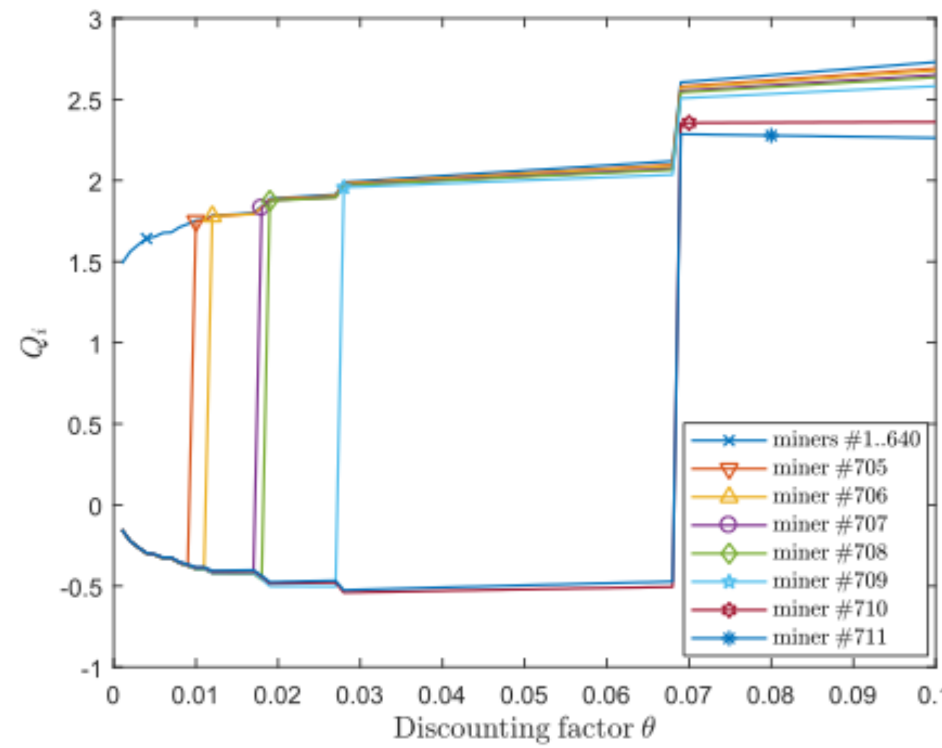
Effects on cumulative utilities of different miners

We calculate the relative change

$$Q_i = \begin{cases} c_i \\ c_i \end{cases}$$

Observation: effects on cumulative utilities differ significantly for different miners!!

Example: initial power of pool #1, $P_1^* = 0.3$.



Conclusions

1) A closed system of two PPLNS mining pools (with the same *N*) is considered;

2) We demonstrated that time-discounting is important for the decision ("which pool to join?") that miners make;

3) We made reasonable assumptions that limit the space of miners' beliefs about the future;

4) For the process of miner migration (from the smalle

6) Even for moderate θ common composition of the sm

7) We suggest two kinds of mitigation: **a**) compose pools with miners who satisfy Sufficient Individual Power (SIP) requirement; **b**) adjust parameter *N* for each pool accordingly.

Thank you for your attention!

MONASH
University