

Usefulness in Mining: Decentralization Trade-offs in Proof-of-Useful Work

Authors: Pratyush Dikshit¹, Ashkan Emami Neighabouri¹, Johannes Schönrich-Sedlmeir²

¹University of Luxembourg (Luxembourg), ²Augsburg University of Applied Sciences (Germany)

Presentation at: DeTaP 2026 - 1st Workshop on Decentralisation: Theory and Practice co-located with AFT 2026, London, 6 October

Motivation: Problem in Blockchain

BITCOIN BLOCKCHAIN: Proof-of-Work

Secure, Anonymous, Decentralised, Permissionless

BUT (inefficient)

High computational effort to solve cryptographic hash puzzles → Waste of resources, no social benefit (electricity)

[Approx. 170 TWh (≈ Poland`s annual electricity consumption)]

Motivation: Useful Computation

Repurpose computational effort for practical/societal problems  Proof-of-Useful Work (PoUW)

Socially valuable tasks, like machine learning training, optimization, scientific computation, etc.

Examples of PoUW:

CoinAI (training of deep learning models),

Primecoin (finding prime number chains),

Coinami (multiple sequence alignment of proteins),

Ofelimos (Optimization)

Many proposals, yet no large-scale deployment

Block Reward vs. Useful-Work Reward

PoUW Separates Security From Useful-Work Completion

Block Reward → Security

Probabilistic reward proportional to hash-power contribution to consensus, securing the chain.

Useful-Work Reward → Private Payoff

A separately paid reward for completing useful computation — decoupled from any security contribution.

The Rational Response

Miners shift resources toward the higher-yielding useful work and devote only the minimum to chain security.

-
- ↓ **security budget**
 - ↓ **cost to mount a 51% attack**
 - ↑ **network vulnerability**

Governance implication: a new private reward stream can weaken the institutional coupling that previously produced security as a by-product.

Research Questions

Is PoUW really Useful?

Does making consensus computation useful preserve PoW's decentralisation, or introduce new concentration and dependence?

A Systematisation of 55 PoUW Designs

55

distinct PoUW constructions

12

application domains

3

Phases: systematisation, taxonomy of PoW properties, economic security analysis

We map useful-work mechanisms onto **consensus properties, architectural choices, trade-offs and economic incentives**, asking not only whether PoUW can reproduce PoW's security, but how a new mining objective changes who can participate.

Structure of PoUW

Types of Structure for the PoUW constructions:

Hash-based PoW for security + Useful Tasks

Hash-based PoW for security + (Useful Tasks + Hash-based PoW for security)

Useful Tasks for security (with negligible PoW)

Three Decentralisation Tensions



Market dependence

Incentives are no longer endogenous: participation hinges on demand for useful solutions in external markets, beyond the protocol's control.



Task heterogeneity

Unequal opportunities across miners: incentives for task selection, specialisation and selfish mining around high-value workloads.



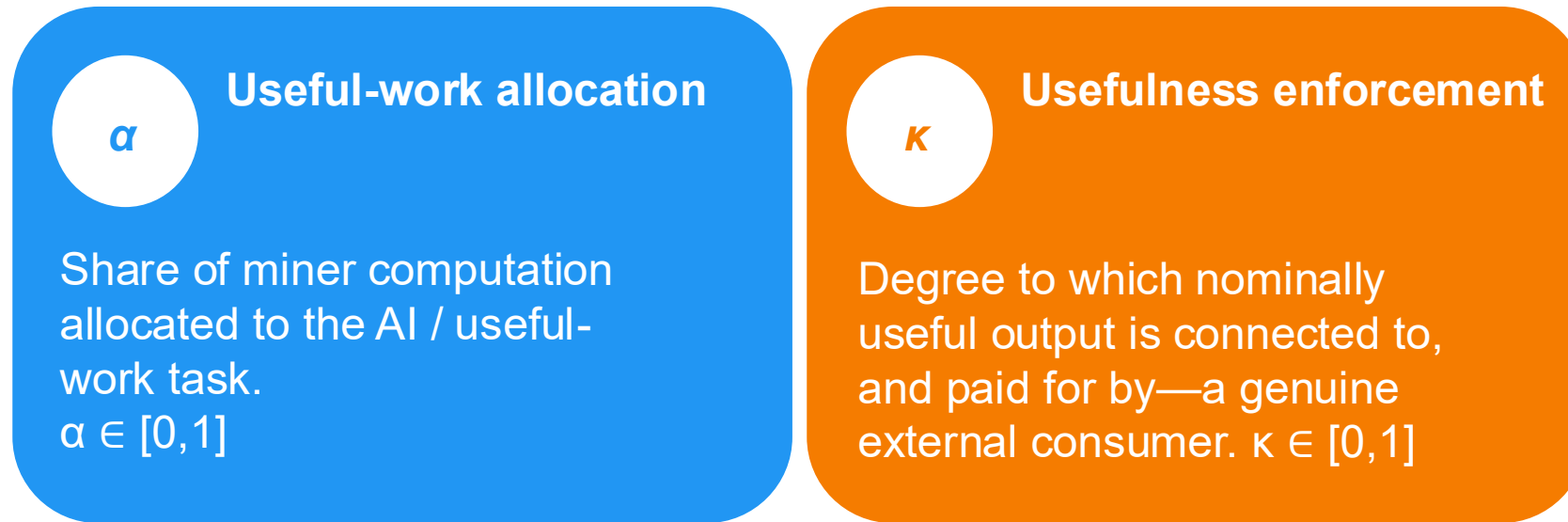
Off-chain value

Useful outputs keep value outside the chain, enabling off-chain trading and strategic behaviour that couples consensus to external markets.

Each opens a new pathway from economic power to consensus power

Useful Work (α) vs. Usefulness (κ)

Two quantities must be separated: how much computation goes to useful work, and how much of that work creates real useful value.



Central Governance Risk: High α + low κ can leave miners economically motivated while delivering little realized useful value, while the attack cost may not fall proportionally.

Incentive Decoupling

Proof-of-Work · Incentive Coupling

Security contribution is the ONLY path to private block rewards. Rational profit-seeking produces collective security as a structural by-product.

*A deliberate governance achievement
(Budish, 2018)*

Proof-of-Useful-Work · Incentive Decoupling

A private useful-work reward stream is introduced, architecturally independent of collective security. Miners face a genuine allocation choice.

*A structural change to the protocol's
institutional architecture (Basu, 2026)*

Important distinction: “verifiable computation” is not automatically “verifiable usefulness.”

Formalization

$$C = S + U$$

Compute splits between security (S) and useful work (U)

$$\alpha$$

Fraction of computation allocated to useful work

$$\kappa \in [0,1]$$

Usefulness enforcement: how far a miner's "useful" output is linked to a genuine external consumer

SECURITY-BUDGET MODEL

$$E[G_{\text{earn}}] = p_i \cdot R + \alpha \cdot \kappa \cdot V_{\text{ext}} - C_i$$

SENSITIVITY TO κ

$$\partial E[G_{\text{earn}}] / \partial \kappa = \alpha \cdot V_{\text{ext}} > 0$$

Returns on useful work rise specifically in κ , holding computation fixed

Existing PoUW constructions assume verified computation is enough

Conclusion

Increasing useful-work rewards induces miners to reallocate resources away from security, reducing the aggregate security budget and **increasing network vulnerability**.

The external value that makes PoUW attractive may also introduce new concentration and market dependence

Preserving Decentralisation:

- Proportional incentives
- Cryptographically unpredictable task assignment
- Succinct verification
- Difficulty adjustment aware of task value and cost



Interdisciplinary Centre
for Security, Reliability
and Trust



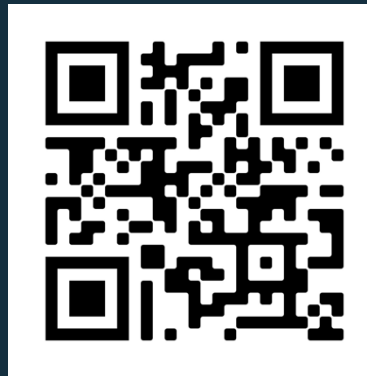
Thanks!

Contact

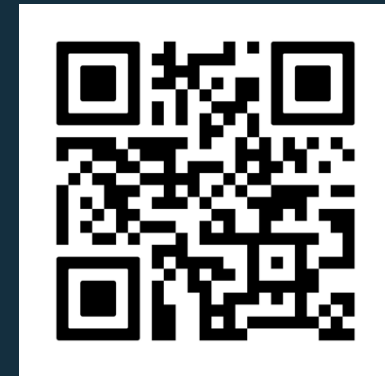
Pratyush Dikshit

Doctoral Researcher

pratyush.dikshit@uni.lu



LinkedIn



Google Scholar