Linzhi Semiconductors

Linzhi Working Papers

No 12

The Future of Proof-of-Work.

by Chen Min

November 2017

(Originally held at Scaling Bitcoin 2017, Stanford/USA,
re-published as LWP12 in September 2019)

Keywords: LWP12, Proof-of-Work,
Proof-of-Contribution, Scaling Bitcoin, Conference

This publication is available on https://linzhi.io
Telegram discussion https://t.me/LinzhiCorp

The Future of Proof-of-Work

How custom hardware contributes to blockchain scaling – Chen Min

About me

Chen Min (Chip Architect)

6 years designing hardware miners

Avalon Miner generations 1 to 8 (ASICs)

Topic of this talk: Contribution

A little review of bitcoin PoW

Difficulty from 1 to 1,452,839,779,146

Energy efficiency from 3,000W/GH to 0.1W/GH

Hardware cost from $10,000/GH to $0.06/GH

And, all in 8 years

Scale is not reachable in software

Reward system of Bitcoin (Planned economy)

Solo mining

Pool mining (rewarding miners & volunteer nodes)

Reward mining, limit transactions

Economic impact of mining

5B USD per year invested in mining hardware

5% of transistors in entire semiconductor industry is made for mining

Power (off-grid power plant), energy prices up

Hardware price (Ethereum mining drives DRAM prices up)

If this keeps going, someone will buy semiconductor fabs

What will happen if we also invest in storage and network bandwidth?

Is Hardware the Default Attacker?

Why is the attacker model always focused on hardware?

Meaning of anti-ASIC

Anti-SSD Filesystem or Anti-Router protocol

Responsibility of fairness & scalability is in software, not hardware

Story: weird glass company wants control of the whole world

Encourage contribution (even quantum friendly)

Make being a contributor more economic than being an attacker

Hardware business

Hardware always focuses on cost efficiency

- Performance
- Energy
- Reliability

Economic path for long term scaling

Make mining and transaction (smart contract) processing same

Reward by how many transactions have been processed

If too few real transactions then fill with dummy transactions

Key

PROOF OF WORK

Reward securing the blockchain

PROOF OF CONTRIBUTION

Reward scaling the blockchain

Always reward contributors

Only reward contributors

Thank you

Chenmin.ac@gmail.com

Proofofcontribution.org