Plot Compression in Chia Blockchain

Diego Escondrillas and Hendra Wijaya

Introduction

Chia Network:

- Open-source
- Aims to address scalability and energy consumption limitations

PoST

- Farming processes:
  - Plotting
  - Harvesting

Introduction

Plotting:

- Creating plots
- Plot → File containing hashes
- Generated using disk space
- Plotting options:
  - MadMax
  - Bladebit
  - Default plotter
- Plot size → K parameter

Introduction

Farming → Creating blocks

Farmers wait for a challenge to be called out → Check plots

Higher number of plots → Higher probability of winning

Background

PoW:

- Miners solve puzzles ⟹ computational power

PoS:

- Miner is selected beforehand

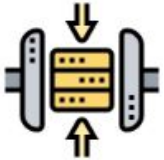
PoST:

- Trades computing power for storage

Motivation

- More users ⟶ more data/plots ⟶ unwieldy Blockchain size

Plot Compression



Proposed Solution

System requirements	Minimum	Recommended	Testbed
CPU	4 cores	8 cores	6 cores
RAM	16GB	32GB	32GB
Boot drive	SSD SATA	SSD NVMe	SSD NVMe
Primary drive	–	HDD 8TB	HDD 4TB
Secondary drive	HDD	SSD	HDD

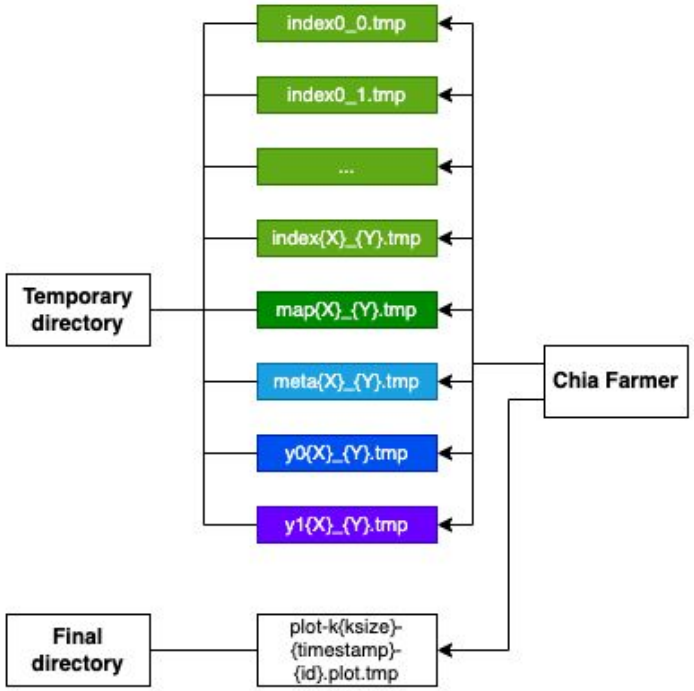
Compare performance of plotters:

- Chia Proof of Space 1.0.11
- BladeBit Plotter 2.0.1 (Disk plot)
- madMAx Plotter (1.1.6-2092041)

Evaluation

Plotting: Phase 1

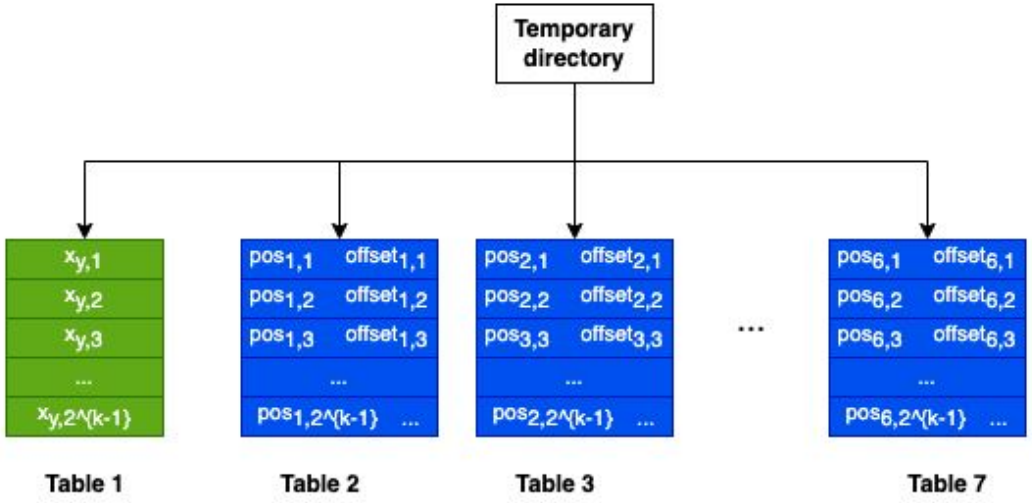
- Create temporary files.
- Fill with cryptographic hashes.
- Up to 5x bigger size than final plot.



Evaluation

Plotting: Phase 2

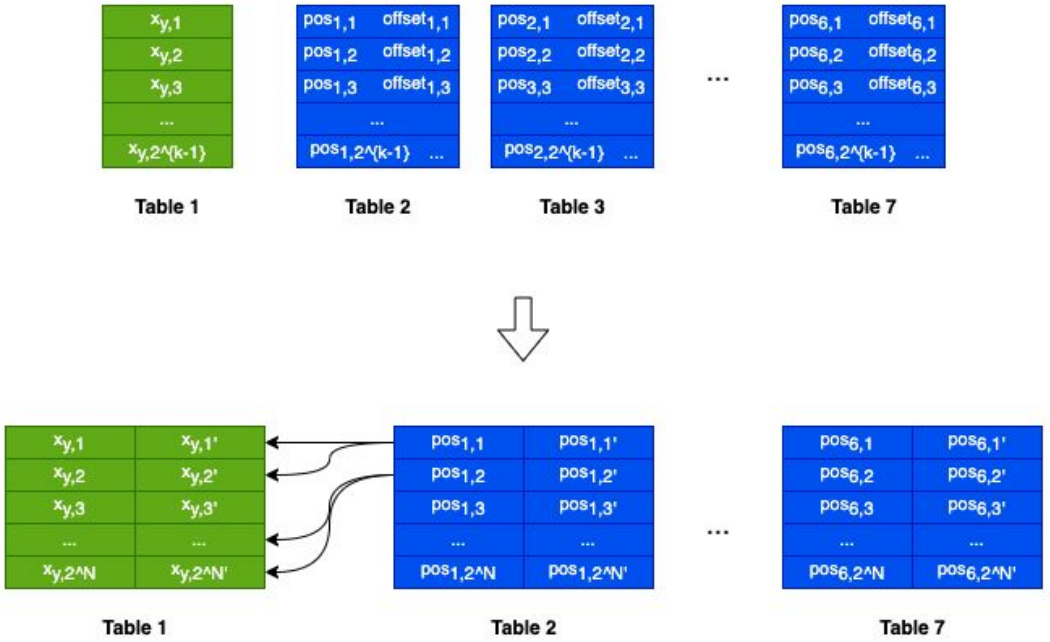
- Backpropagation.
- Sort tables and keep sorted indices.
- Remove unused data in the process.



Evaluation

Plotting: Phase 3

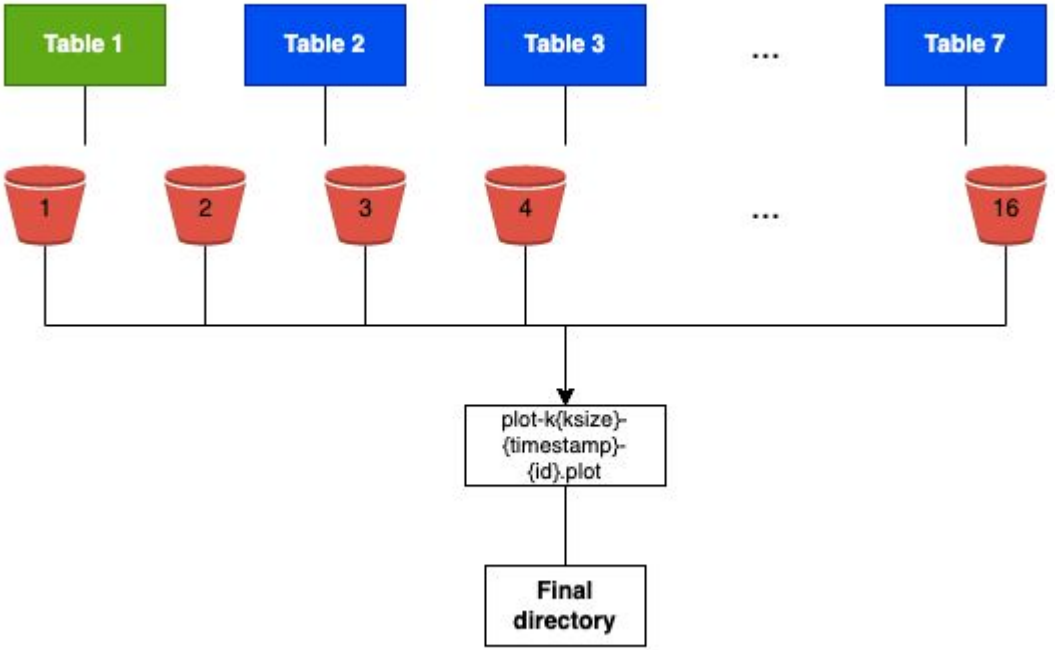
- Lossless compression.
- Replace offset with double-pointers.



Evaluation

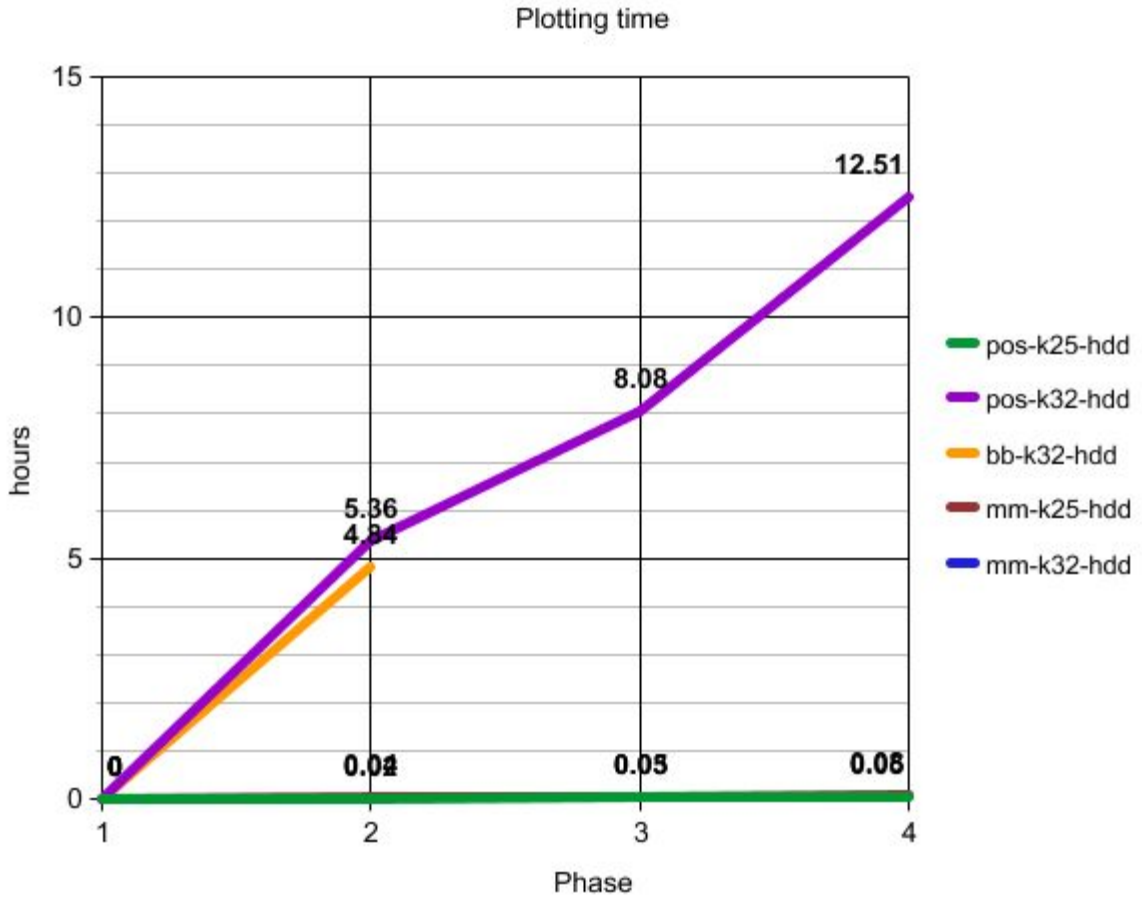
Plotting: Phase 4

- Divide 16 buckets for sorting.
- Write final plot file.
- Remove temporary files.



Evaluation
Findings

- pos: Proof of Space.
- bb: BladeBit.
- mm: madMAx
- hdd: Hard disk drive.



Related work

- Chia´s plot compression is new

- There isn´t much research

Conclusion

1. Plotting is a costly process

2. Compression reduces size of plots

Tradeoff between computation and storage

Conclusion

Future Work

Explore other compression techniques.