SNIA CMSI | COMPUTE, MEMORY, AND STORAGE

Why Cryptocurrency and Computational Storage?

SNIA BrightTalk Webcast

Live: February 15, 2022 at 10:00 am PT

Presenters:

Jonmichael Hands (Chia Network), Computational Storage Special Interest Group

Eli Tiomkin (NGD Systems), Computational Storage Technical Work Group

Today's Speakers

Presenter:
Jonmichael Hands
Chia Network
Member, SNIA Computational Storage
Special Interest Group

Presenter:
Eli Tiomkin
NGD Systems
Member, CMSI Computational Storage
Technical Work Group

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be, construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

What Does SNIA Do?

- SNIA is a non-profit global organization dedicated to developing standards and education programs to advance storage and information technology.

Who is CMSI?

- Part of SNIA, the SNIA Compute, Memory, and Storage Initiative is a community of storage professionals and technical experts who support:
  - The industry drive to combine processing with memory and storage,
  - The creation of new compute architectures and software to analyze and exploit the explosion of data creation over the next decade.
- CMSI's three Special Interest Groups – Computational Storage, Persistent Memory, and Solid State Drives – evangelize and educate on these technologies to the industry

www.snia.org/cmsi

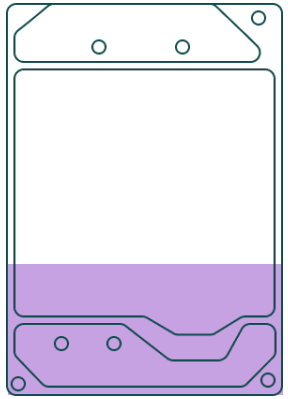
Agenda

- What is Cryptocurrency and Proof of Space and Time?
- What is Computational Storage?
- Why Cryptocurrency and Computational Storage?

Cryptocurrency

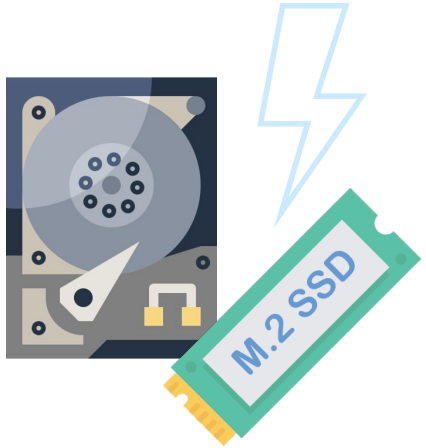
Proof of Space and Time

Why Storage for Cryptocurrency?



Storage is underutilized

Proof of Space and Time leverages underutilized storage to secure the network. Farming was designed to be energy efficient.



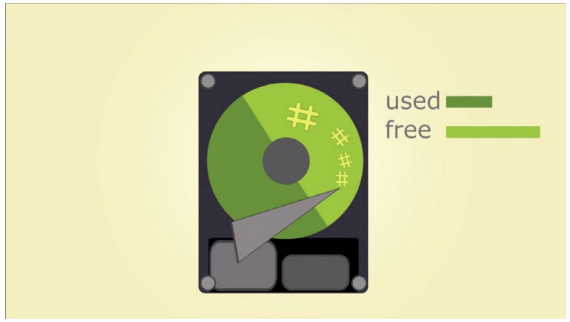
Storage is power efficient

Non-Volatile memory designed to store data power efficiently and network power scales with innovations in areal density.
Currently 1/600 annual energy use of Bitcoin.

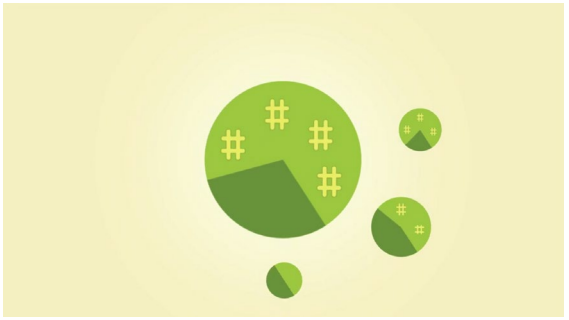
Incentivizes circular economy

Chia farming is a new use case for used storage that will help reduce e-waste and promote the secure reuse of storage.

Farming, Not Mining!



Chia farmers store cryptographic hashes in plot files on hard drive



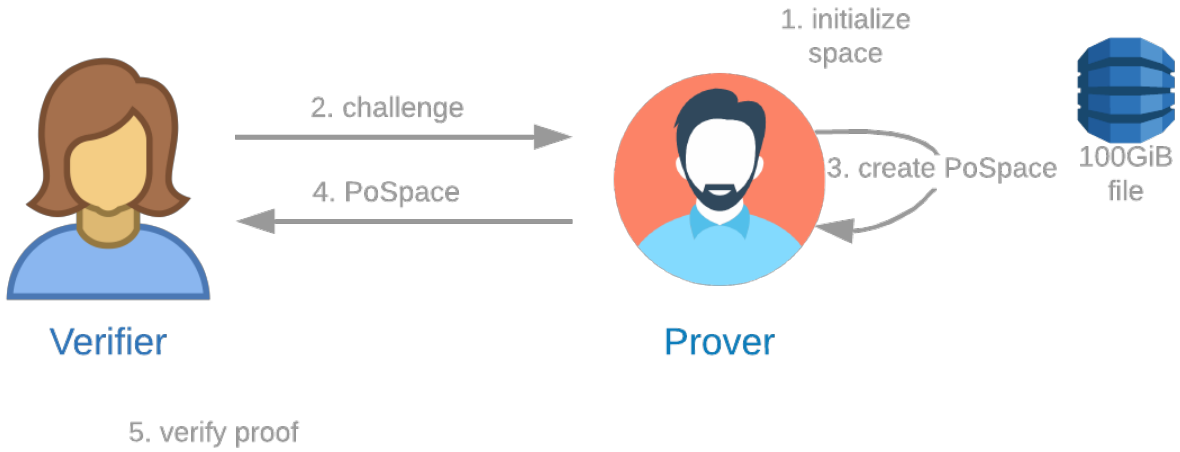
Challenges come in from the network and a farmer checks plots for winning proofs

If farmer finds a winning proof, they broadcast that to the network to form a “block” on the blockchain with transactions

Farmer is rewarded Chia (XCH)

Currently 2 XCH per block

Proofs of Space and Time for the Win!



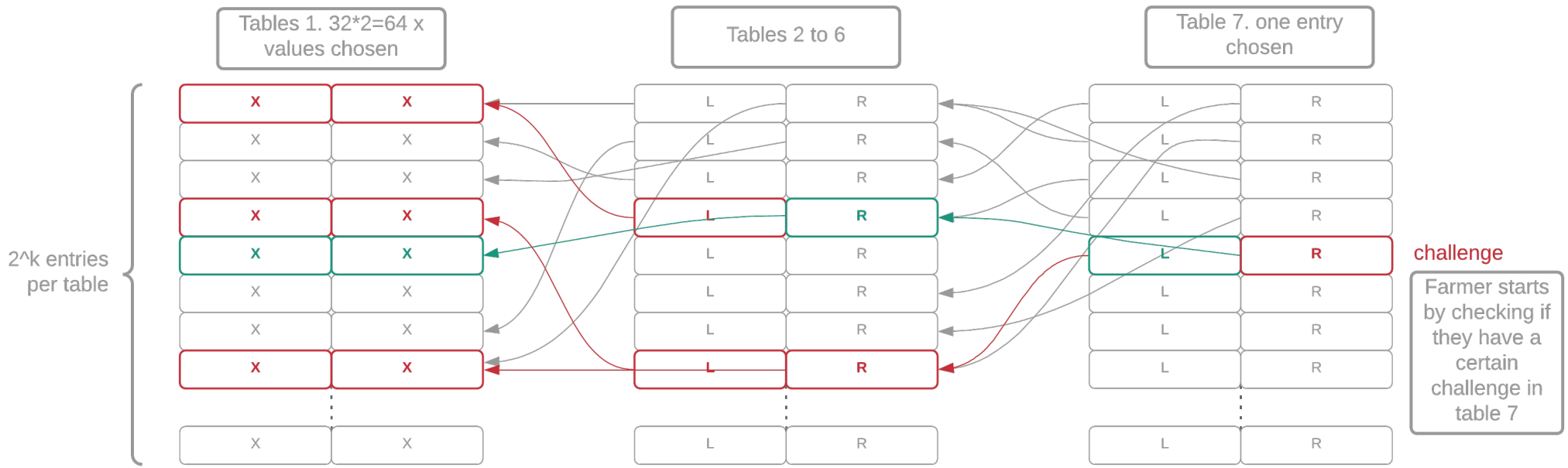
Proofs of Space

- Farmers need to prove to the network that they are storing the data.
- Need to be easily and quickly verifiable
- Needs to be resistant to attacks

Proofs of Time

- Verifiable Delay Function (VDF) that cannot be parallelized
- Easily verifiable that a real amount of time was spent with deterministic output
- Performs squaring computations within class groups of binary quadratic forms

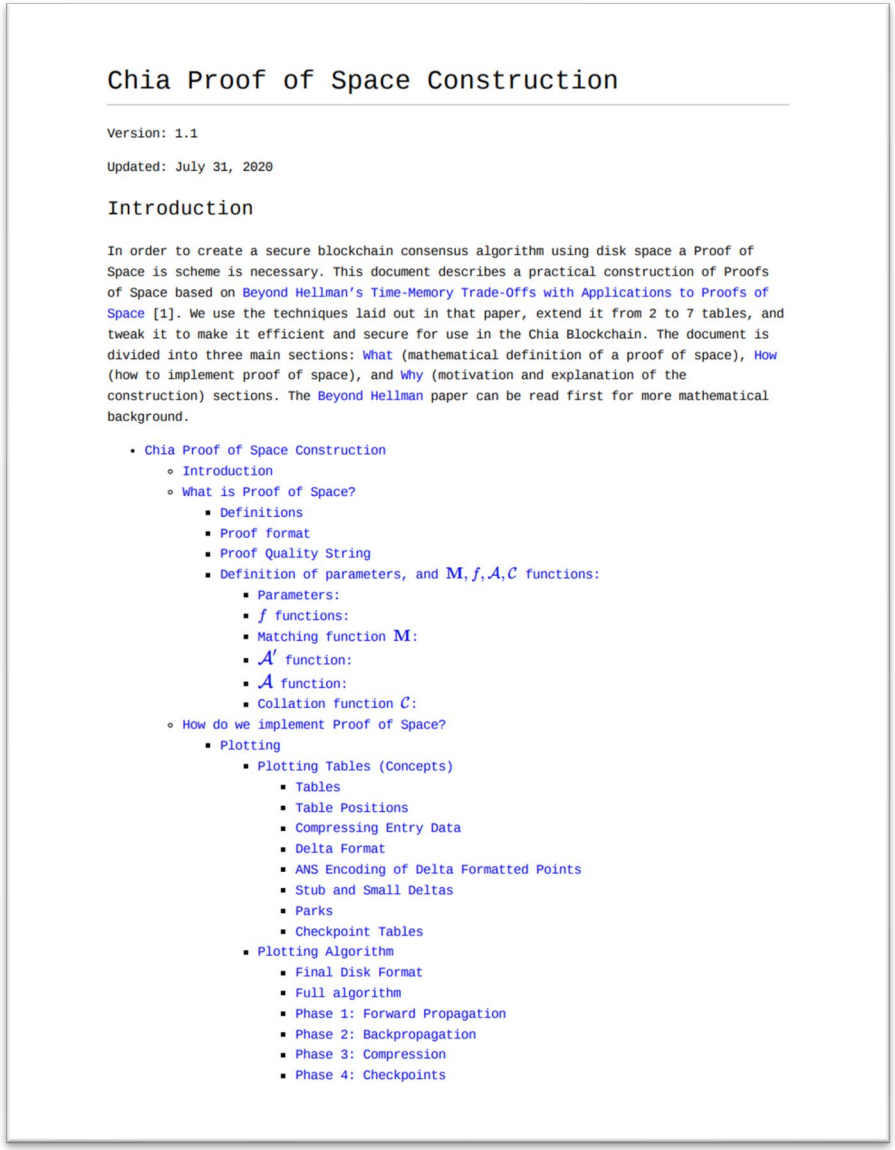
The Fix to Proofs of Space



- Proofs of space designed with 7 tables to prevent Hellman attacks
- Need to be able to quickly retrieve proof (make farming easy)
- Plot size determined by k parameter

Plotting is Write Intensive Workload

- Phases of plotting require a lot of sort on disk & algorithmic compression
- Each K=32 plot takes 1.43TB of disk writes
  - Can be reduced by 72% with 110GB of DRAM
  - Can be eliminated with 416GB DRAM (~300GB with space tradeoff)



Chia Proof of Space Construction

Version: 1.1

Updated: July 31, 2020

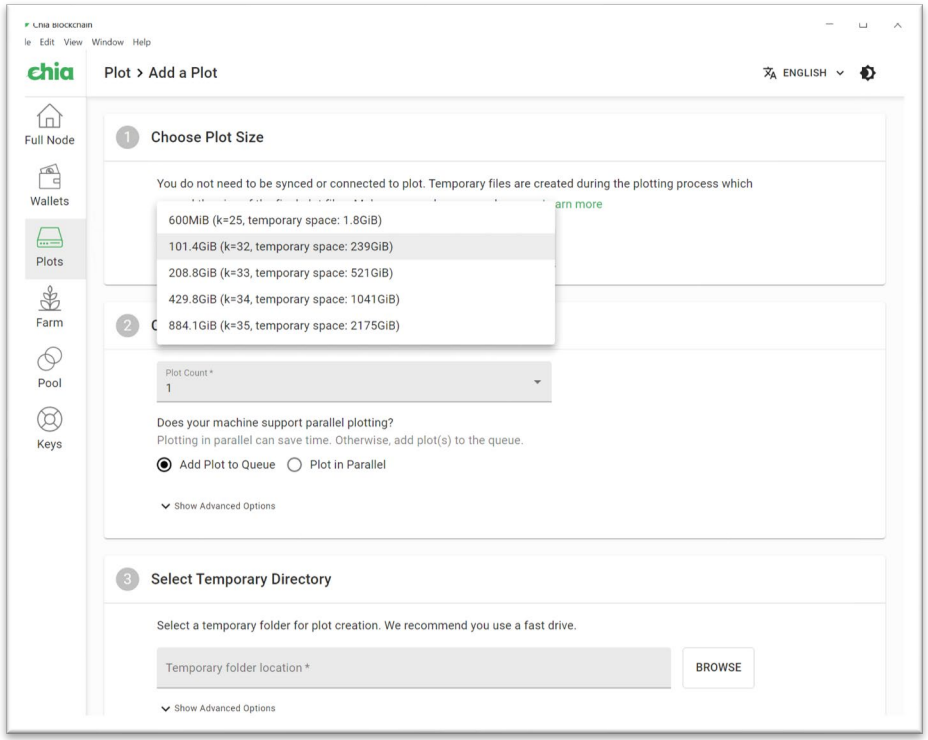
Introduction

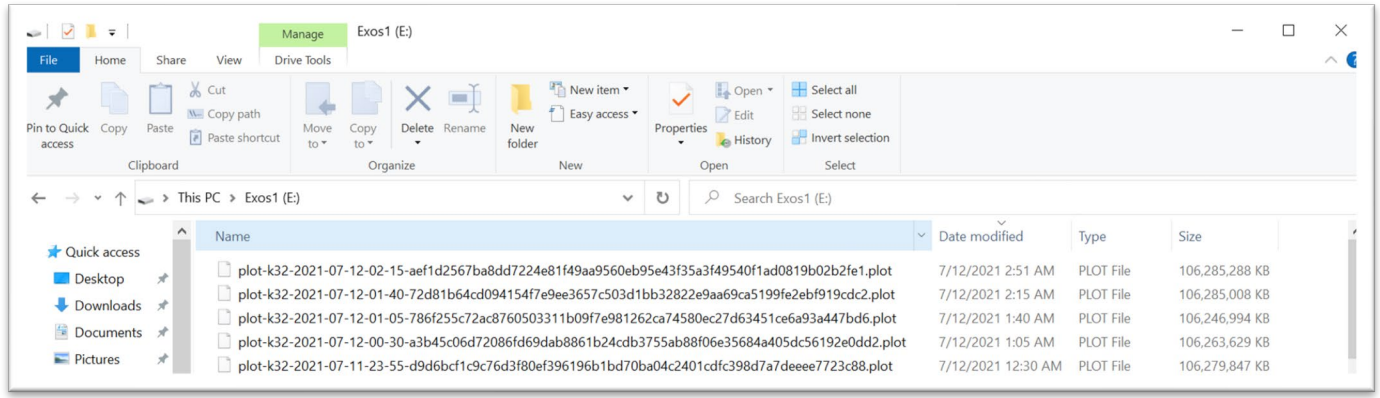
In order to create a secure blockchain consensus algorithm using disk space a Proof of Space is scheme is necessary. This document describes a practical construction of Proofs of Space based on Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space [1]. We use the techniques laid out in that paper, extend it from 2 to 7 tables, and tweak it to make it efficient and secure for use in the Chia Blockchain. The document is divided into three main sections: What (mathematical definition of a proof of space), How (how to implement proof of space), and Why (motivation and explanation of the construction) sections. The Beyond Hellman paper can be read first for more mathematical background.

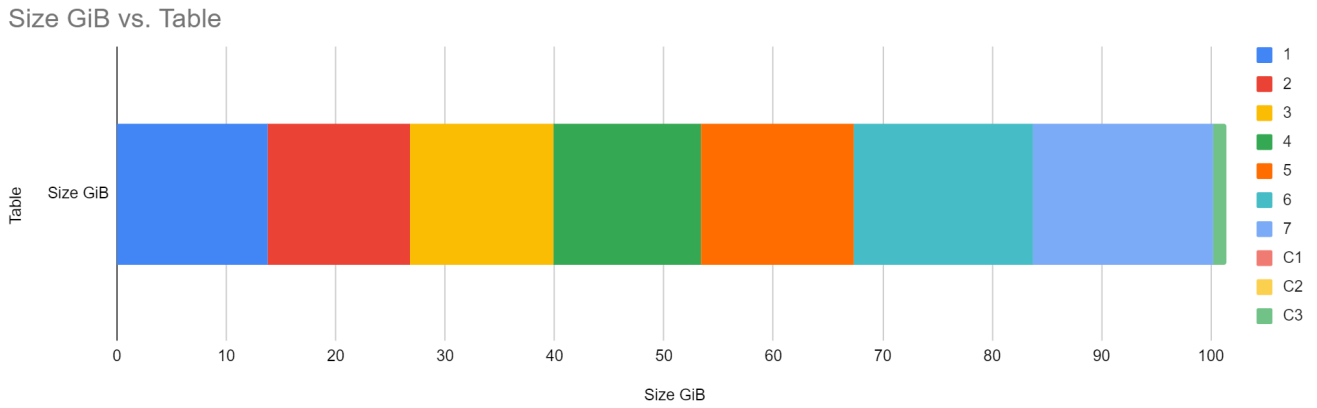
Plotting – All About Performance

Chia Plotting – Files Are Created and Then Transferred to Hard Drive

Use compute, memory and temporary storage to create plot files







How Can Computational Storage Help Speed Up Plotting?

- Compression is hard – new algorithms
- Lots of sort on disk – acceleration
- Need to beat cost of DRAM or performance of high performance NVMe for similar price
- Opportunities to reduce disk writes
- Opportunity for doing low power plotting with onboard compute

Plotting Hardware Required

Server **Workstation** **Desktop**

High endurance NVMe

Create plots as fast as possible. Requires use of hardware for duration of plotting (a few months)

Or…

Use plotting as a service

Plotting Cloud

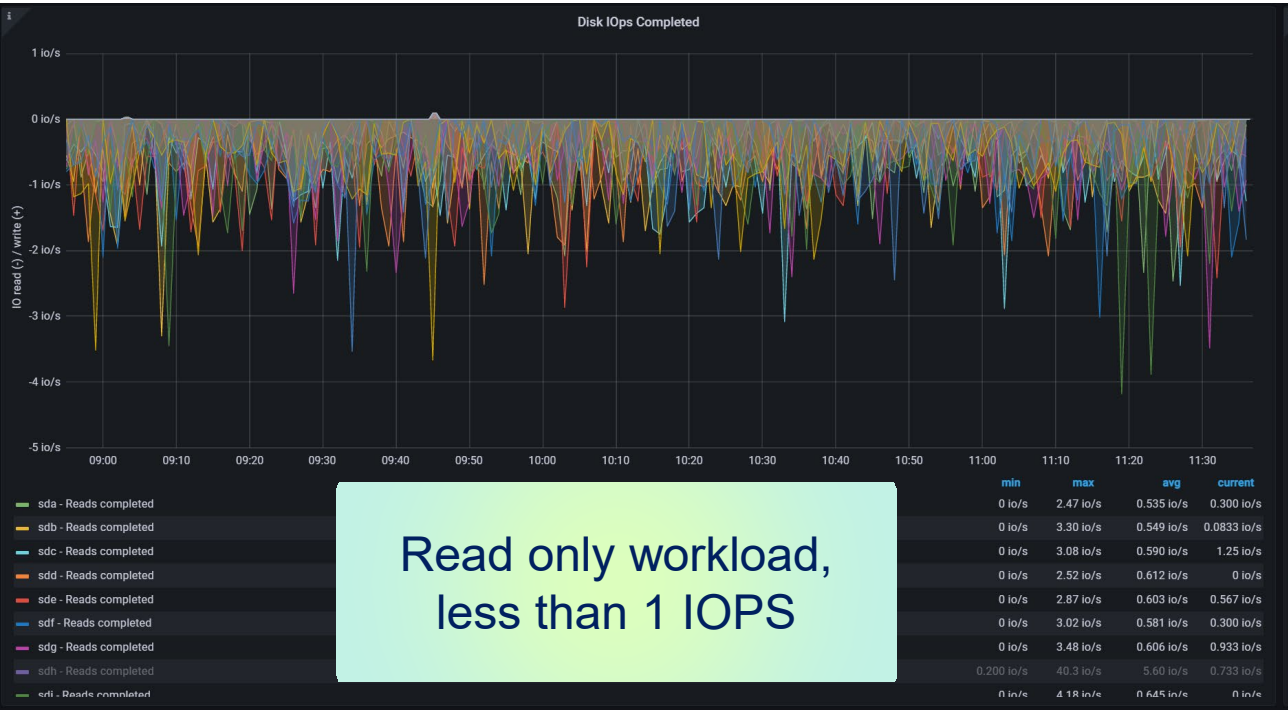
aws

akash

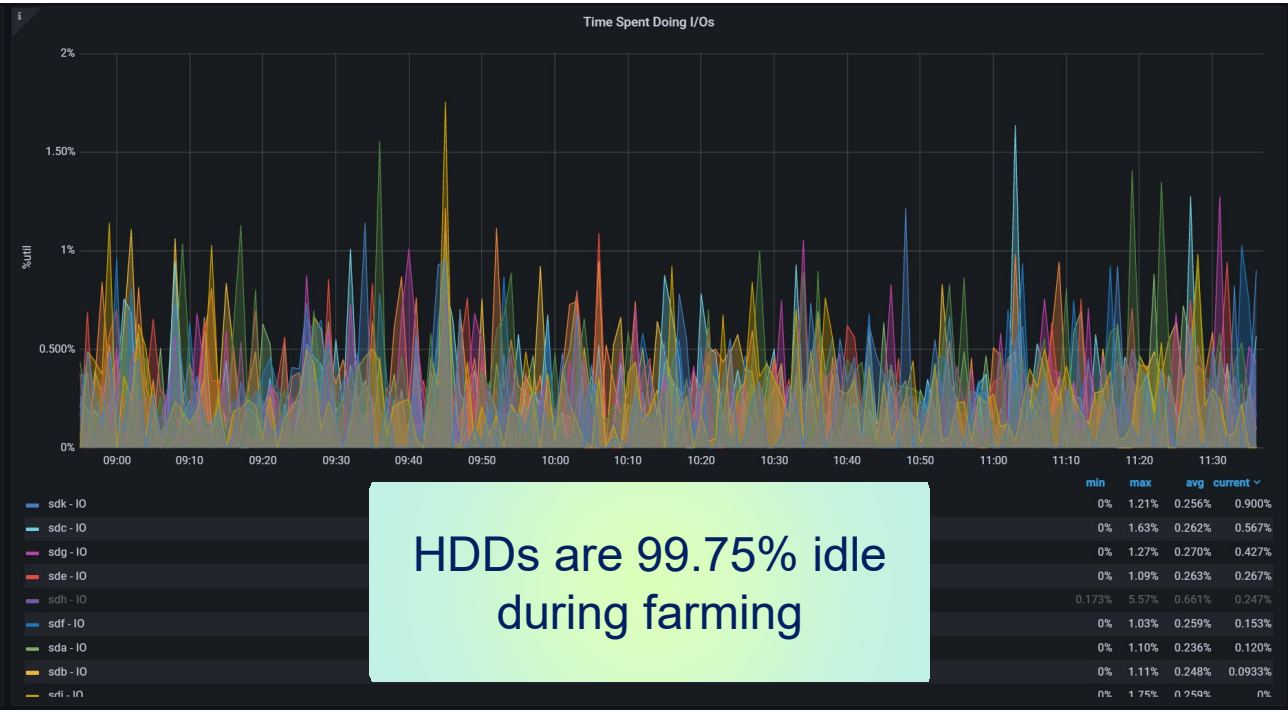
EQUINIX

Download plots from providers. Requires high speed internet connection

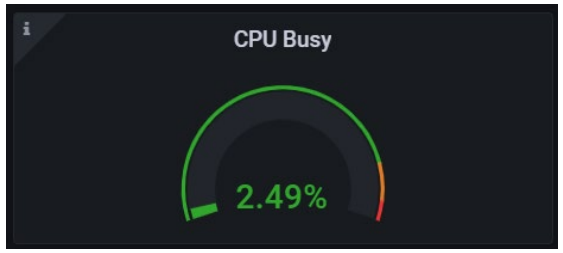
Farming – Efficient Protocol



Read only workload, less than 1 IOPS



HDDs are 99.75% idle during farming



Very lightweight process requires low CPU

Farming Hardware Required

JBOD **NAS** **Desktop** **DIY**



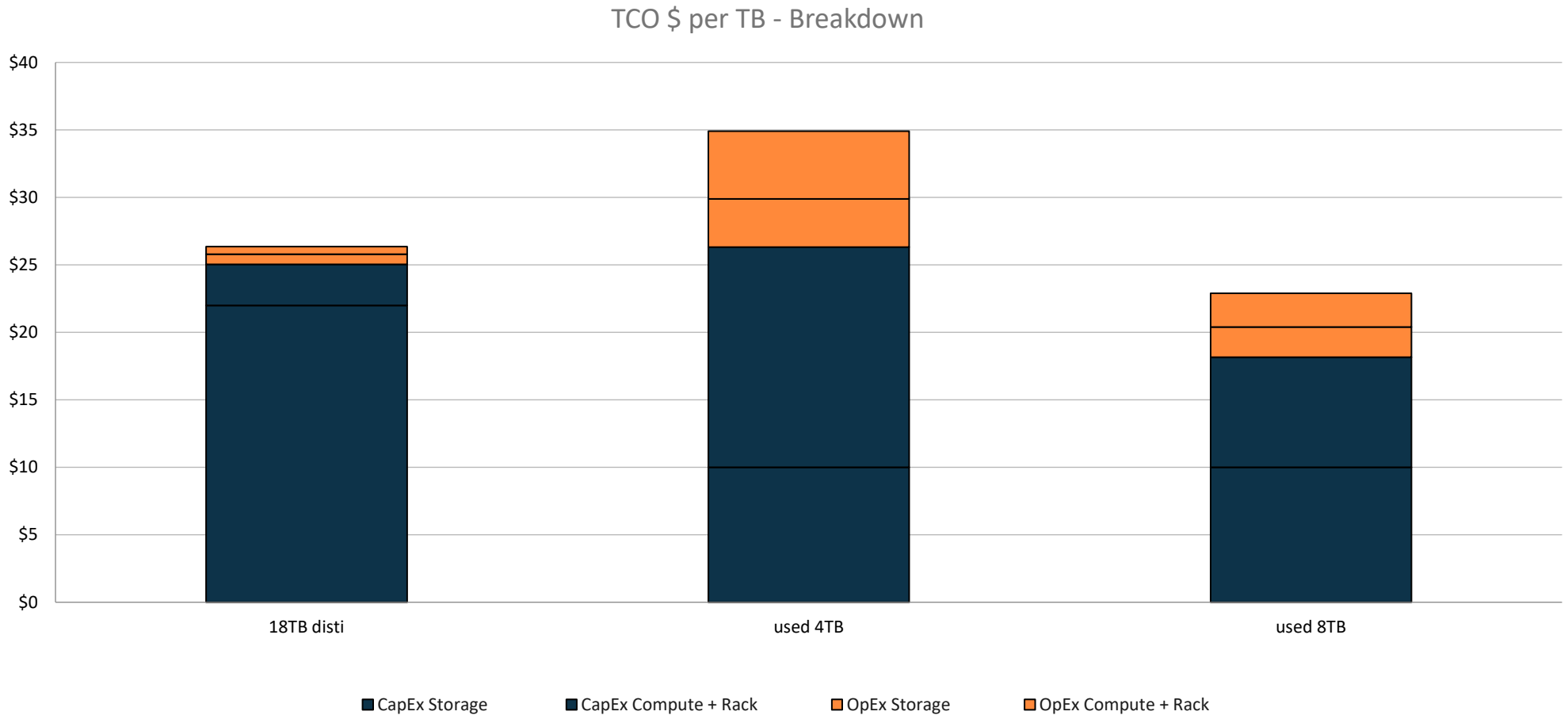

High capacity HDD

JBODs (Just a bunch of disk) houses many hard drives

Store the most data in the smallest amount of space at lowest power

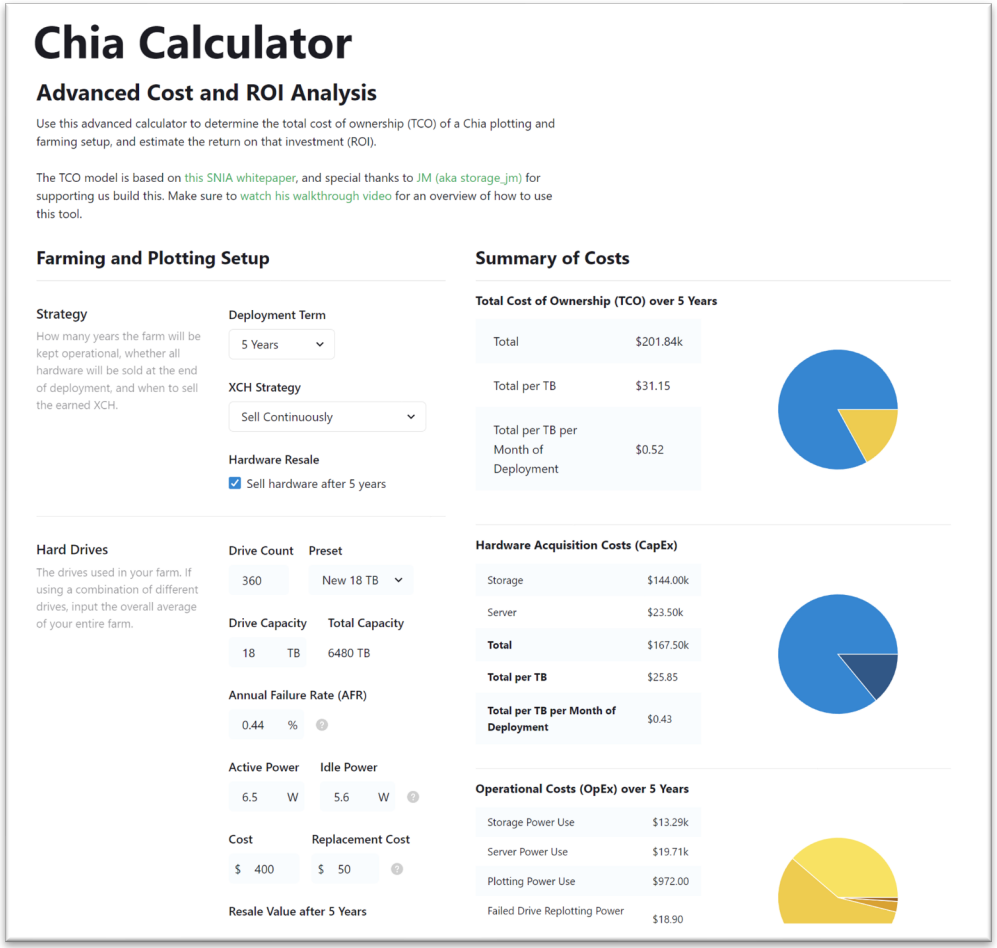
Use high-capacity HDDs for best power efficiency, or cheap used drives if rack space and power are more available

TCO Chia Farming



Chia Calculator Using SNIA TCO Model!

- Use Chia Calculator to estimate earnings and input variables to look at total cost of ownership and profitability for Chia farming!
- Uses SNIA TCO model as base for calculations
- Very user friendly
- https://chiacalculator.com/roi



Computational Storage

Need A New Way to Look at Storage

Pain Points

Physical Space

Available Power

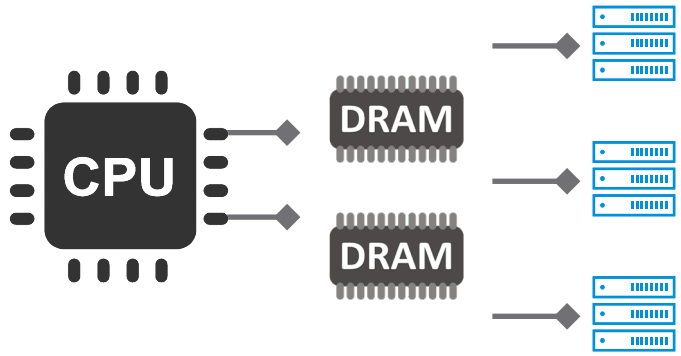
Scaling Mismatch

Bottleneck Shuffle

Scaling requirements are not met with existing solutions

One CPU to many storage devices creates bottlenecks

These bottlenecks exist, we currently just shift where they reside



Technologies that ‘compose’ these elements just exacerbate the bottleneck

A way to augment and support without wholesale change is needed

Using Computational Storage

Benefits

- ✓ Distributed Processing
- ✓ Faster Results
- ✓ Lower Power
- ✓ Smaller Footprint

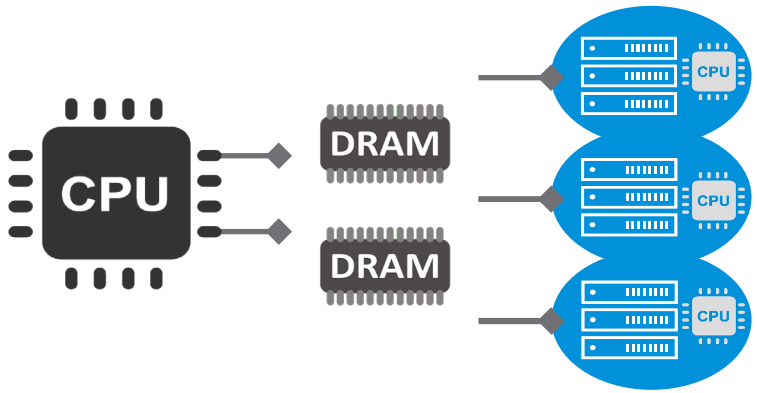
Reduced data transfers

Reduced fabric provisioning

Scaling compute resources with storage provides access to results faster

Computational Storage resources 'offload' work from the overtasked CPU

Seamless architectures create new 'servers' with each storage device added

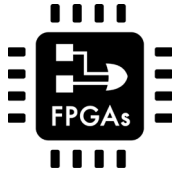


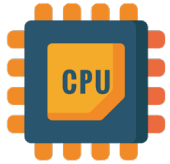
Additional CPU resources without added rack space

Why Cryptocurrency and Computational Storage?

Proof of Work (PoW)

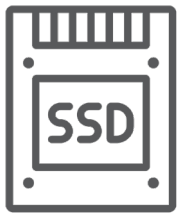
- Using **xPU to Mine**





Proof of Space and Time (PoST)

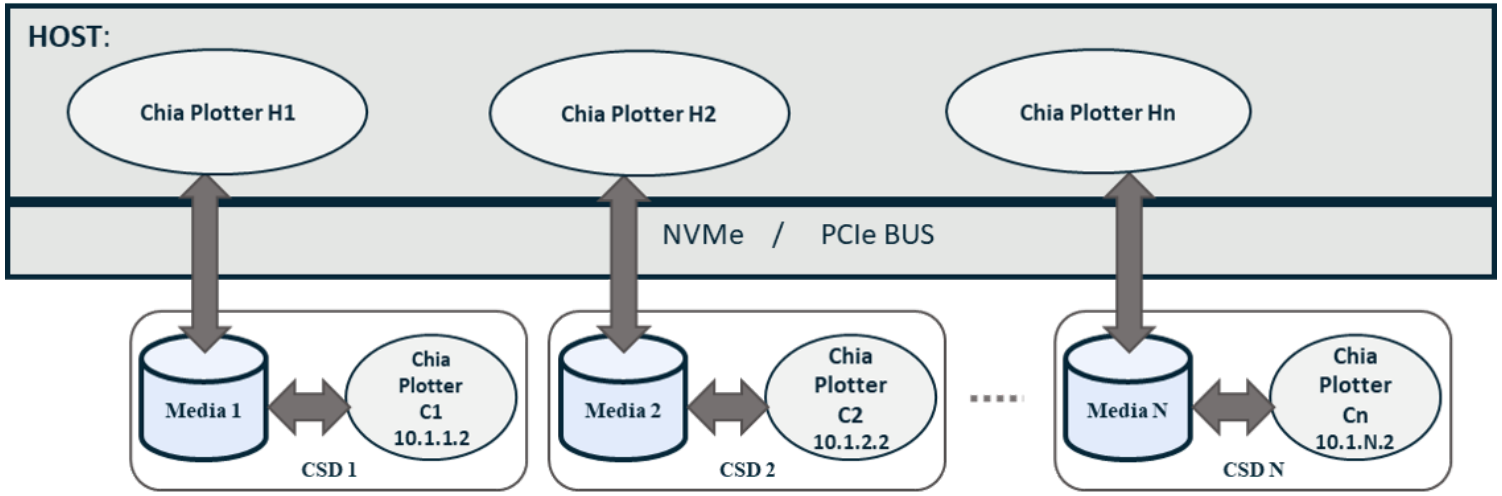
- Using **Storage to Plot/Farm**

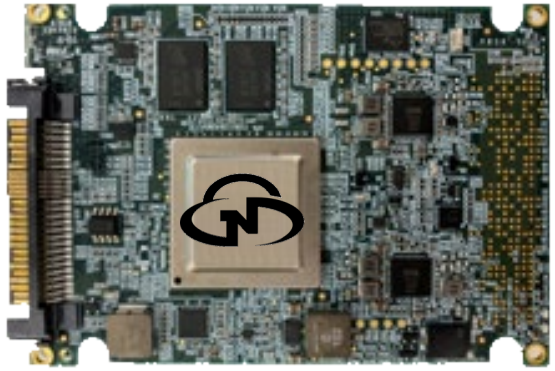


Auto-Plotting Cryptocurrency with Computational Storage

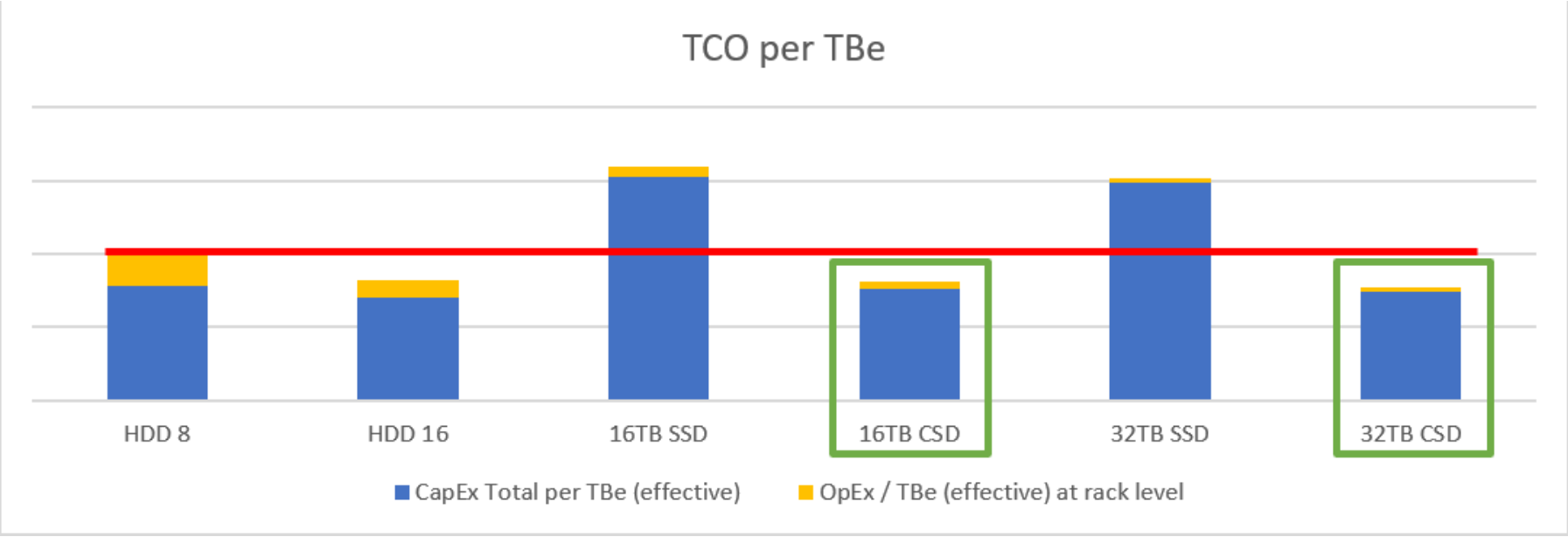
How does Computational Storage Support Proofs of Space?

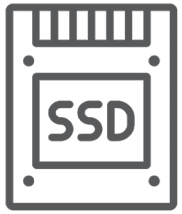
- **CSDs provide the Compute Necessary on Board**
- Reducing the TCO of Chia Plotting by using CSDs at Scale
- Reduce Host activity, increase Plots more quickly
  - **Faster time to Revenue, Reduced Acquisition Costs**





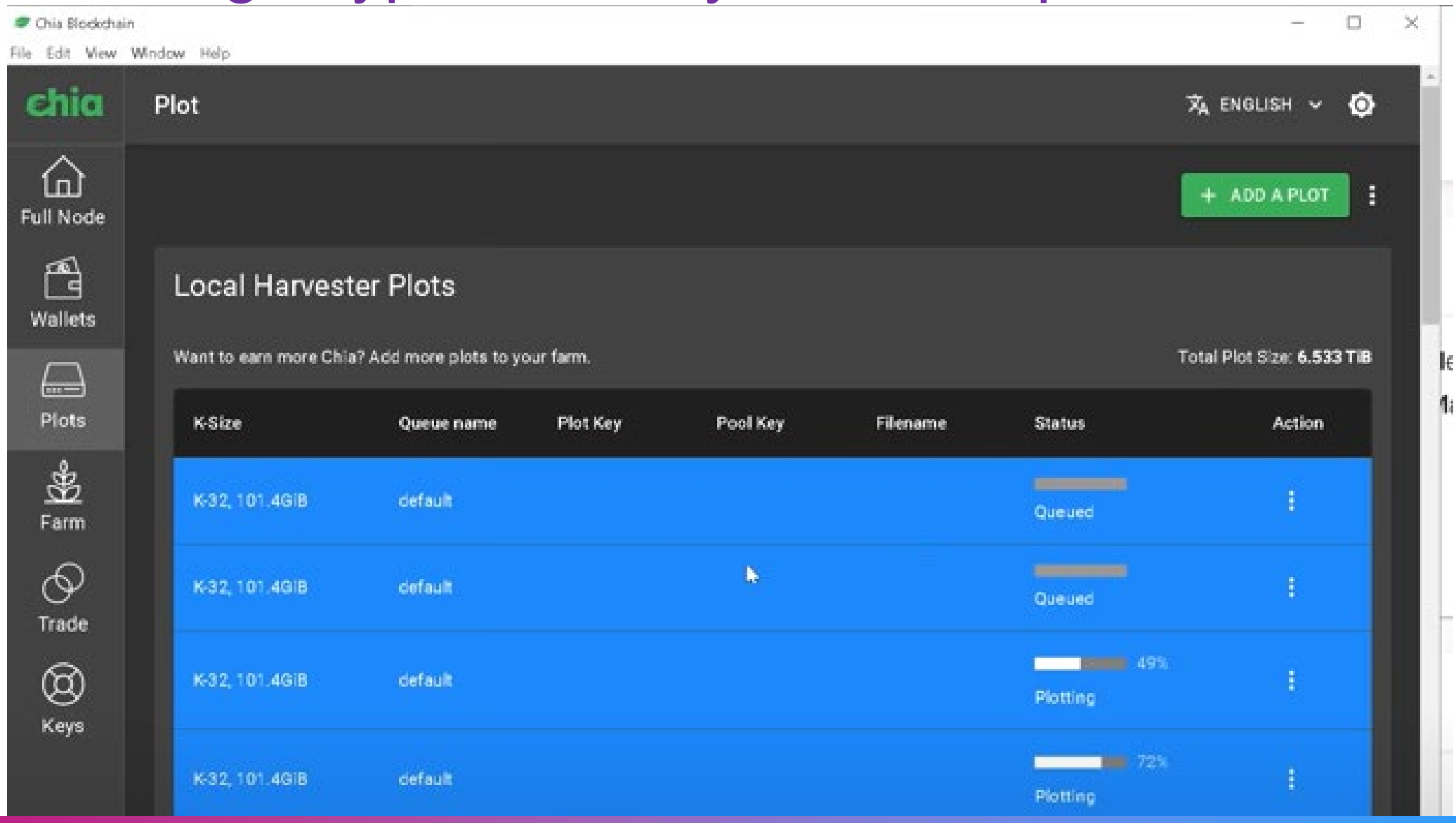
Why Cryptocurrency and Computational Storage?





Total Cost of Ownership (TCO) Model for Storage

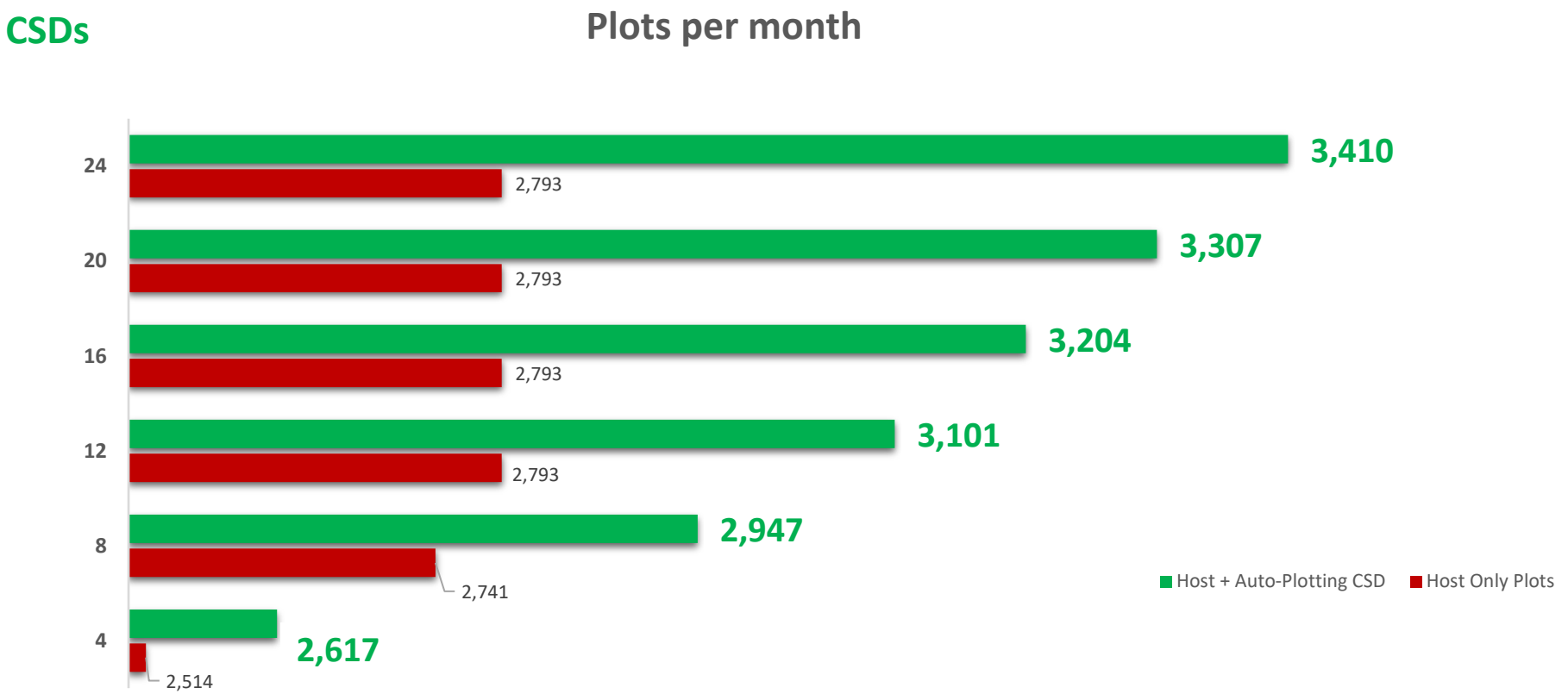
Auto-Plotting Cryptocurrency with Computational Storage



Auto-Plotting Cryptocurrency with Computational Storage

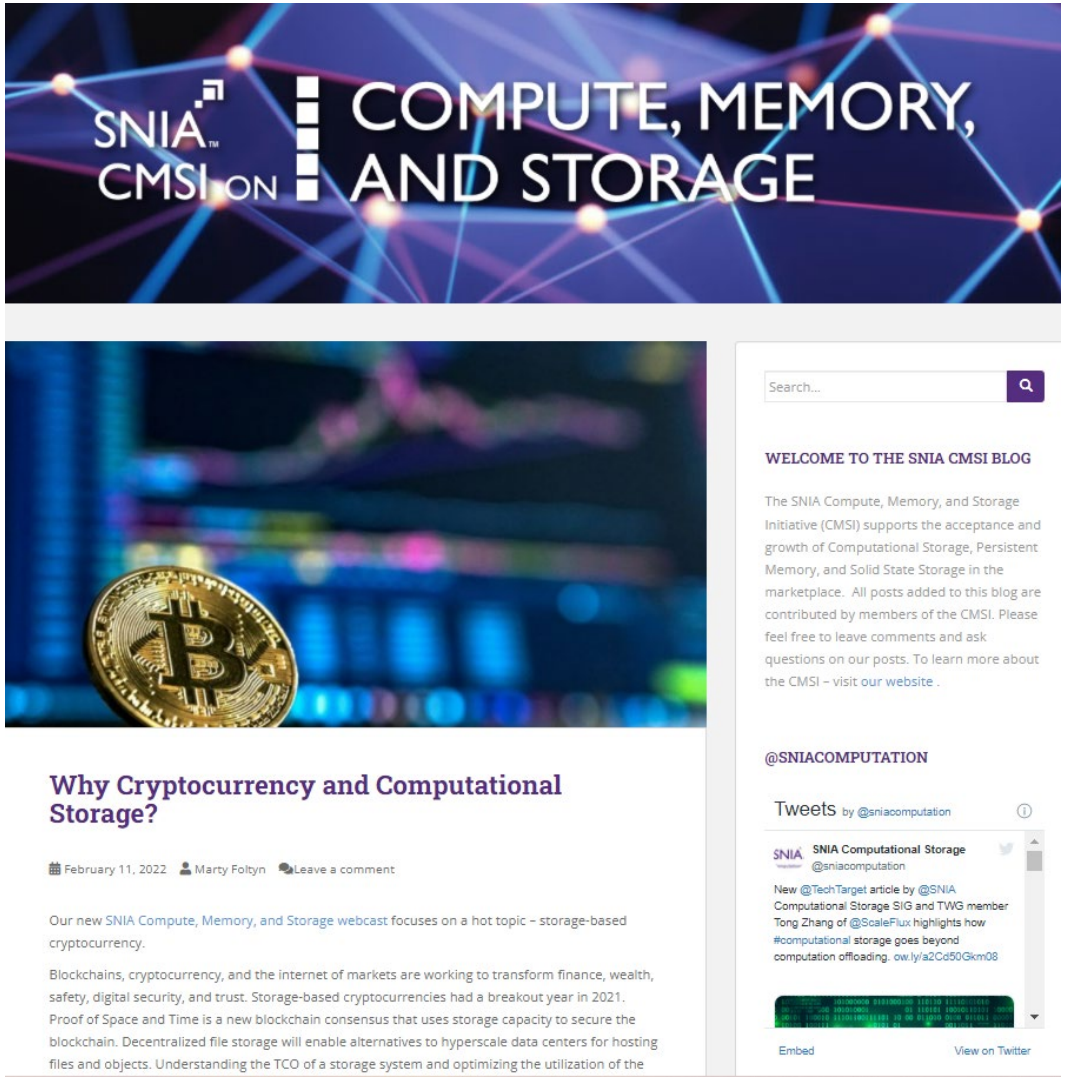
How does Computational Storage Support PoST?

- CSDs provide the Compute Necessary on Board



Thanks for Watching Our Webcast

- Please rate this webcast and provide us with feedback
- A link to this webcast and the PDF of the slides are posted to the SNIA Compute Memory and Storage Initiative website at https://www.snia.org/forums/cmsi/knowledge/articles-presentations
- You can also find this webcast and many other videos and presentations on today's topics in the SNIA Educational Library
- A Q&A from this webcast will be posted to the SNIA Compute, Memory, and Storage Blog
- Learn more about computational storage at www.snia.org/computational



Where To Find Out More About Cryptocurrency & Computational Storage

- Website resources
  - www.snia.org/CMSI
- Twitter
  - @sniacomputational
- Blog
  - SNIAComputeMemory&Storage
- Videos
  - https://www.youtube.com/user/SNIAVideo/playlists
- Educational materials
  - https://www.snia.org/educational-library
- Joining SNIA and the Compute, Memory, and Storage Initiative
  - https://www.snia.org/member_com/join-SNIA

Thank You for Watching!

Questions?

You can always reach us at askcmsi@snia.org

www.snia.org/cmsi

