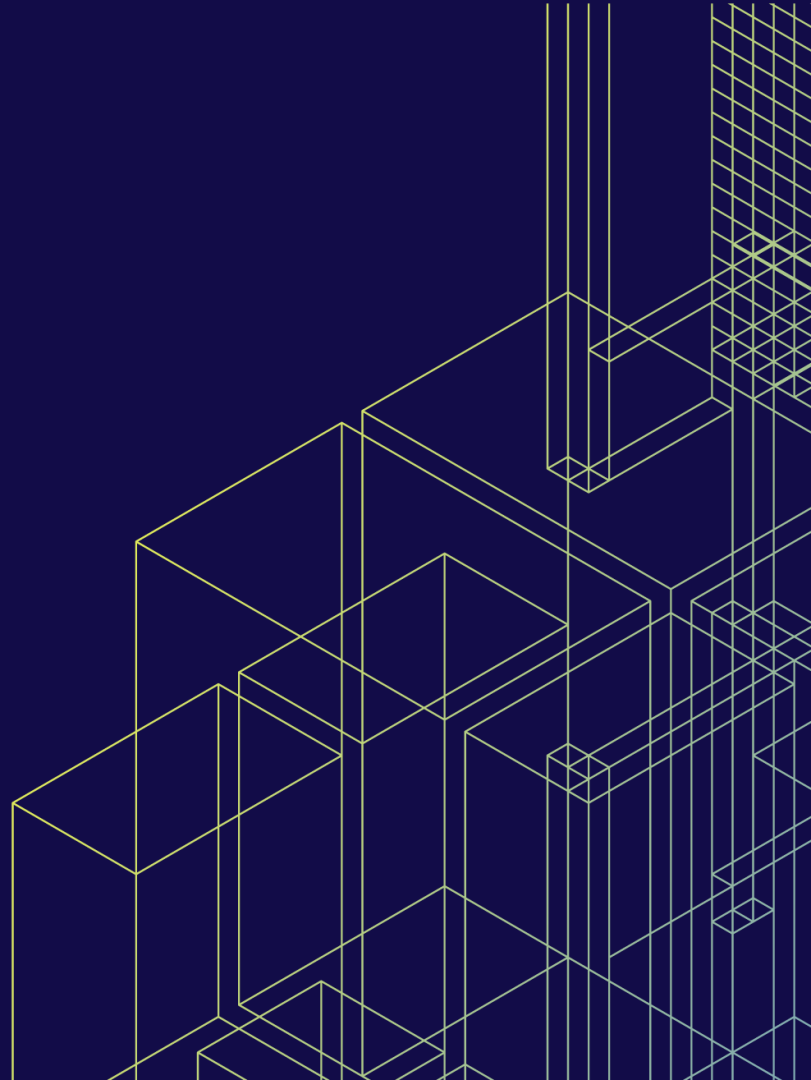




September 23-26, 2019  
Santa Clara, CA

# Storage Applications in Blockchain

**Olga Buchonina - ActionSpot**  
**Daniel Jones – Open Source**  
**Burst Apps Developer**



# What is Blockchain?

- Blockchain is a distributed database of records stored in blocks.
- Blockchain is secured using peer validation in cryptography.
- Blockchain as a technology has several facets that directly or indirectly can impact user depending on implementation.

# Current State of Blockchain Technology

- Ethereum blockchain has made it easy for everyday individuals to create dApps.
- There are current reports that as of 2017 and 2018, at least 50% of all Initial Coin Offerings had failed to raise funds and approximately 800 others had failed altogether.
- New projects are constantly created seeking to bring solutions, sometimes these solutions are not needed.
- Blockchain vs. Database

# Current State of Blockchain Technology

- Many larger corporations are becoming more interested in the use of blockchain, however it is important to be mindful, not everything that appears to be blockchain, is blockchain.
- With over 50% of ICOs failing to raise funds and others just completely failing, the US government is having to become involved.
- Blockchains that are mined and supported by public peers are not considered securities by the SEC, unlike those that are ran by businesses or ICOs, STOs, IEOs.



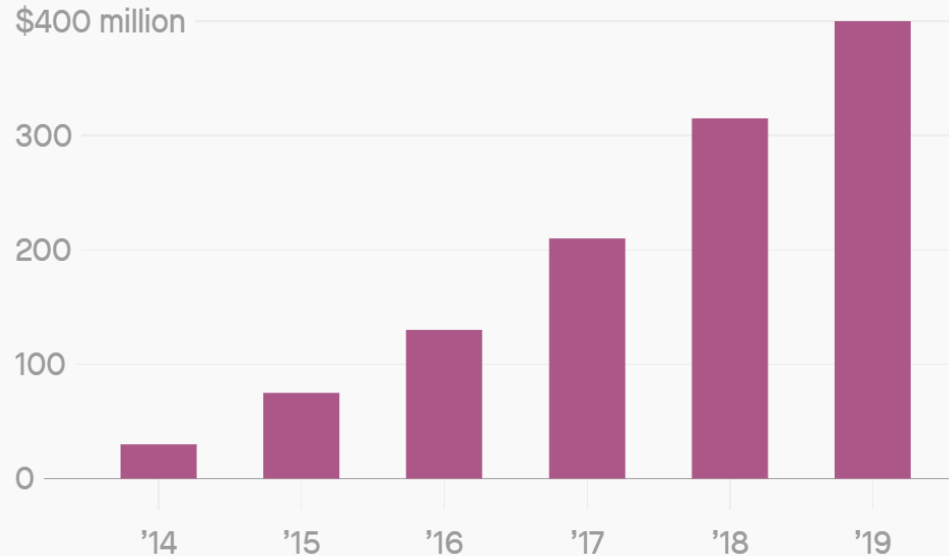
# Current State of Blockchain Technology

- Individual state and city governments are looking into blockchain implementation, real estate deed management, tax payments, smart cities.
- Pharmaceutical companies are looking into tracking medications from start to finish in order to ensure the quality of the products they provide.
- Others in the farming, wine and even cannabis business are looking for similar solutions.
- Since it has become less challenging for people to create decentralized applications, they are also coming up with much needed solutions.

# Who is adopting Blockchain?

- Companies racing to adapt blockchain include Amazon, Walmart, UBS, Microsoft, IBM and PwC. The Bank of Canada is also experimenting with the technology.

Estimated bank spending on blockchain tech



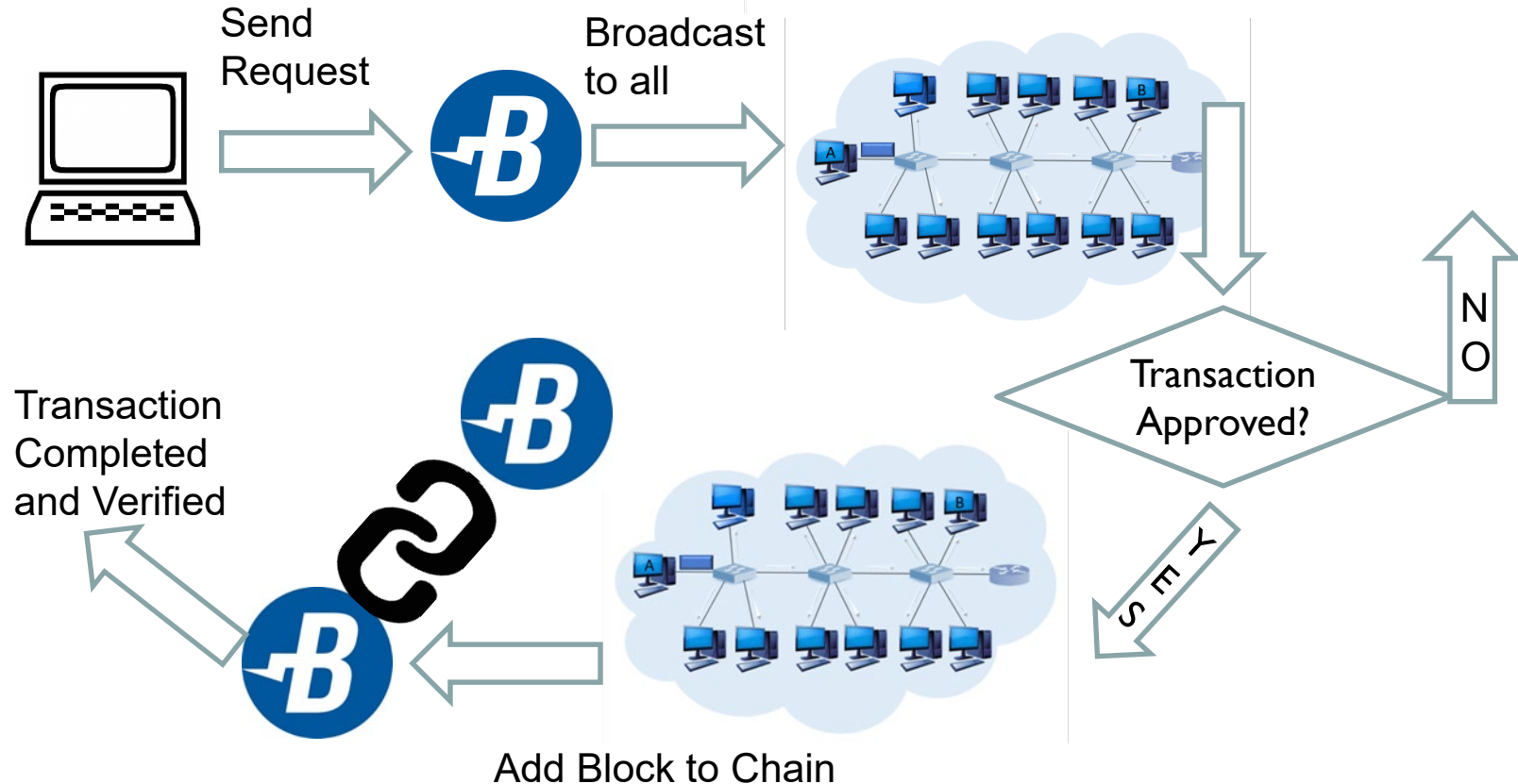
# Current State of Blockchain Technology

## Limitations

- Blockchain today ( according to Deloitte Insights) are relatively slow. Example: Bitcoin transactions are 4.6 per second, VISA 1,700 transactions per second

VISA	BITCOIN	BURST
1,756 per second	4.6/sec	Theoretical infinite – using Dymaxion
~150 MLN/24 hours	2,759/24 hours	n/a

# How does Blockchain Work?



# Relevant Consensus Protocols

- Proof of Work
- Proof of Stake
- Delegated Proof of Stake
- Proof of Capacity
- Proof of Space

# Proof of Work

- Proof of work is the first trustless consensus.
- This algorithm is utilized to confirm transactions between individuals in a trustless fashion.
- In this consensus, the process of performing the Sha-256 and submitting the output is called “mining”.
- The individuals verifying the transactions are called “miners”.
- As they verify transactions, they are trying to solve a puzzle to earn the block reward.

# Proof of Work

- A block reward varies by chain, however it will also include all transaction fees paid in that block.
- Proof of work can be optimized with use of ASICS (Application Specific Integrated Circuit).
- While Bitcoin was the first to implement the proof of work consensus, Ethereum, Monero and Litecoin use it as well.

# Proof of Stake

- Unlike proof of work, individual users aren't able to validate, your validation capability is based on your stake on said consensus.
- New blocks are created pseudo-randomly based on your stake on the consensus, either through randomized block or coin age based selection.
- The process of creating a new block is called minting or forging;
- The individuals verifying the transactions and creating new blocks are called "forgers".



# Proof of Stake

- Randomized is the most commonly used and easier to predict as it looks at the user with the lowest hash value and size of their stake. This helps others determine who might become the forger.
- Coin age based selection happens by looking at the individual with the most amount of coins staked for the longest period of time. At least 30 days.
- In proof of stake, most of its currency is fixed, therefore the rewards consist of transaction fees.
- However, this currency can be inflated in order to create additional supply when needed.

# Proof of Stake

- Ethereum will be moving into a Proof of Stake consensus protocol, DASH, Stellar and NEO are other blockchains using this consensus.

# Delegated Proof of Stake

- Or DPoS Is a variation of proof of stake, which seeks to reach consensus more efficiently.
- Voters, select witnesses, or other users they would like to validate transactions.
- Voters can also give their voting power to others.
- The number of witnesses is capped and it is their responsibility to validate transactions and create new blocks, they in return receive any transaction fees.
- Top tiered witnesses can prevent transactions from being included, however they cannot change the details of said transaction.

# Delegated Proof of Stake

- Additionally, users in DPoS Systems vote for a group of “delegates” or individuals responsible for maintaining the network.
- While they oversee the performance and governance of the blockchain, such as changing block sizes, they are not responsible for validating transaction or creating new blocks.
- Blockchains such as EOS, Cardano and TRON use this consensus.

# Proof of Space

- There are current concept currencies that are looking into implementing Proof of Space, some of these concepts are Chia and Spacemint.
- Often times PoC Blockchains are confused for Proof of Space.
- It is a cryptographic technique in which individuals or “provers” demonstrate they have available hard drive space.
- Such verification must be efficient as not to take up additional space.
- It would be virtually impossible for a prover to pass the verification process if they do not have the space they claim to have available.

# Proof of Capacity

- Proof of Capacity or PoC, like Proof of Work, allows individuals to mine crypto currency.
- PoC Mining requires utilizes individual's empty hard drive space in order to plot.
- It is done by utilizing the outputs of the shabal-256 cryptographic function to validate capacity to be used in mining.
- The bigger the plot, the more likelihood to win a block due to probability.

# Proof of Capacity

- Shabal-256 currently is ASIC-resistant due to the IO requirements (as it requires writes).
- One time hashing process(plotting) versus continuous hashing.
- Mining process only involves reading the plots every new block, (time per block vary by blockchain) and submitting the answers plus deadline (time to read to actual nonce).
- Power requirements for reading the plots greatly reduce overall energy consumed.
- Burstcoin, BHD and BSN are some of the blockchains currently using PoC Consensus.

# Burstcoin

- Burstcoin is an open-source decentralized blockchain that connects individuals, businesses, and financial institutions.
- Burstcoin allows everyday individuals to begin plotting and mining in their empty hard drive space.



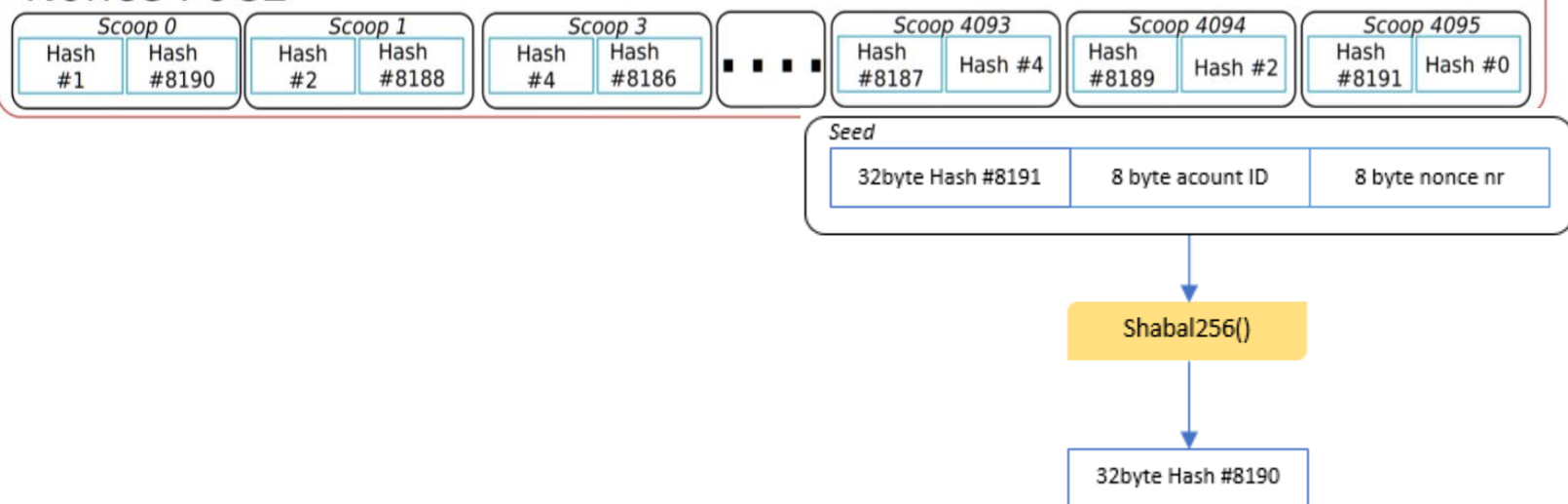
# Burstcoin

- Burstcoin was the first cryptocurrency to use the proof-of-capacity algorithm. (2014)
- Burstcoin was the first cryptocurrency to implement working, "Turing complete" [smart contracts](#) in a live environment in the form of *Automated Transactions* (AT), this occurred before both [Ethereum](#) and [Counterparty](#).
- Burstcoin's ATs include decentralized crowdfunding.
- Atomic cross-chain transactions (ACCT), a more recent innovation by Burstcoin and Qora allows for full decentralized trading between two cryptocurrencies without the need for any third-parties such as online exchanges.

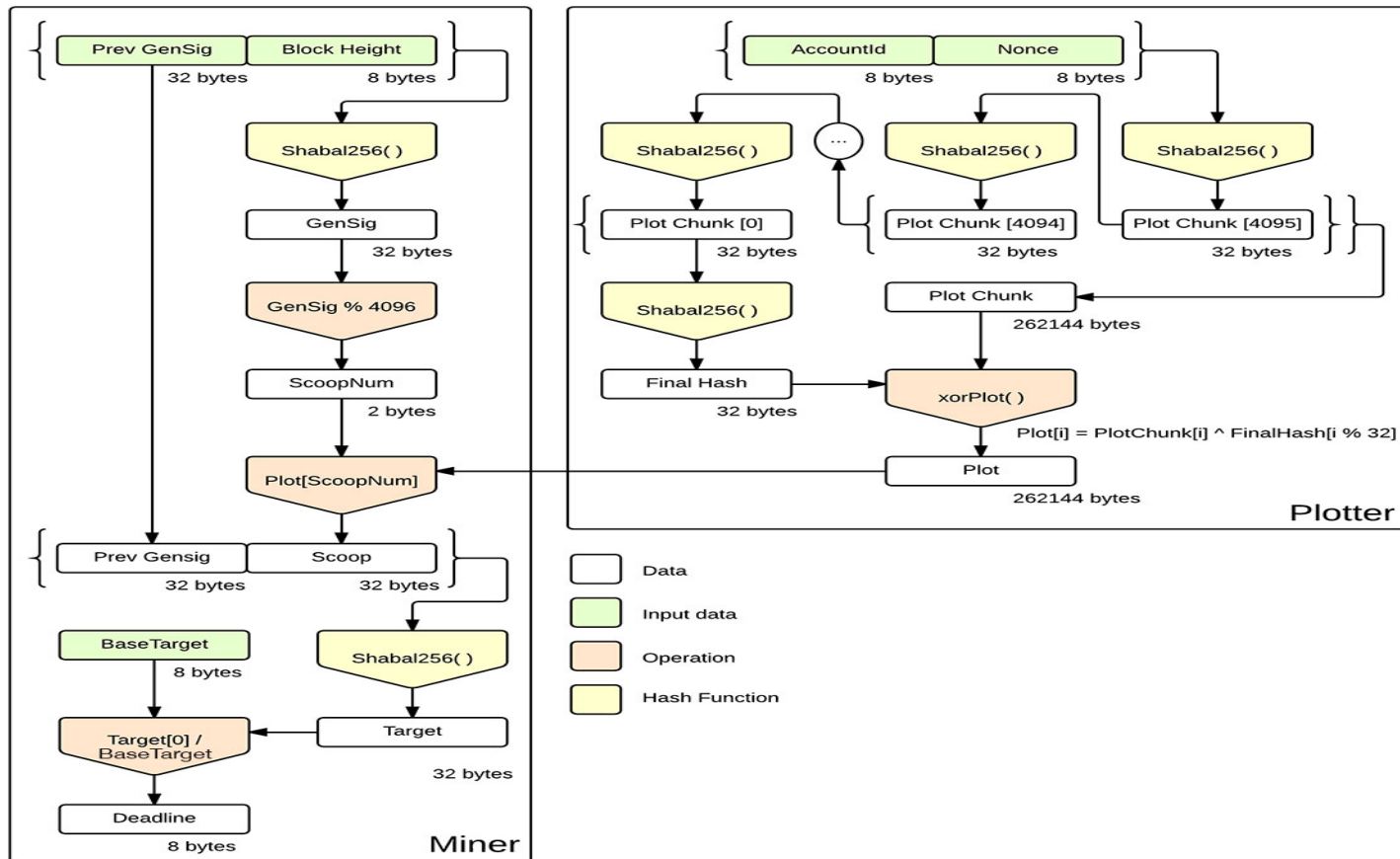
# Blockchain and Proof of Capacity

- Plotting is the process of generating plot files, which are just files storing a large number of pre-computed hashes. Each *plot* file contains one of more groups of 8192 hashes, these groups are called *nonces*. A nonce is exactly 256KiB in size (8192 x 32 bytes per hash). Additionally, each nonce is divided into 4096 pairs of hashes, the pairs are referred to as *scoops*. Each nonce can also be identified by its index number, ranging from 0 to  $2^{64}$ .

## Nonce PoC2

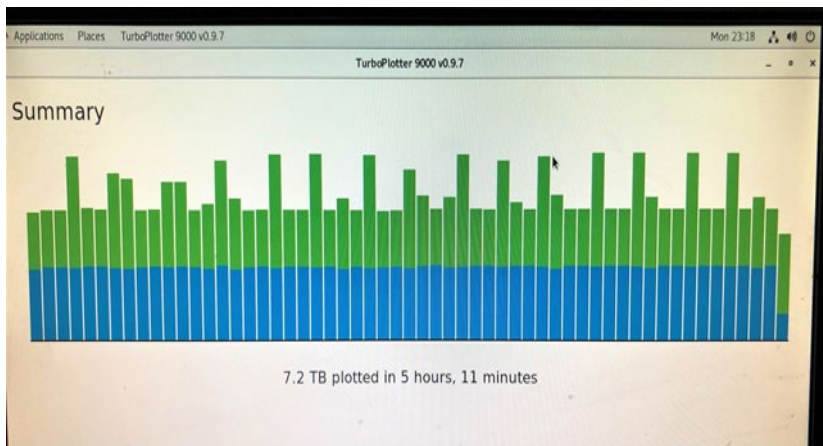


# Burst Coin Mining and Plotting



# Examples of Plotting and Mining with Western Digital

## Plotting



# Burstcoin

- Burstcoin is an open-source decentralized blockchain that connects individuals, businesses, and financial institutions.
- Burstcoin allows everyday individuals to begin plotting and mining in their empty hard drive space.
- Due to the ease of mining there are currently individuals mining in various parts of the world.
- We have a wide range of businesses currently interacting with the Burstcoin Blockchain in many capacities, payments, renting out solar mining space, building mining systems or solutions to provide extra transparency for their day to day operations.

# Burstcoin

- Users are able to mine Solo (standalone) or in Pools (with other miners).
- A solo miner submits to the network directly through their node without going into a pool.
- There are different types of pools based on what the pool operator wishes to run, miners then choose the pools that are more appealing to them.
- Some of these pools use a portion of their proceeds for additional projects or fundraising.

# Examples of Mining Applications





# Burstcoin

- Due to its decentralized nature, there are several development teams working in different projects that support the Burstcoin Blockchain all over the world.
- We are constantly finding new innovative ways of adoption and bringing solutions to businesses and individuals alike.
- Due to its low energy consumption, it is eco-friendly and wonderful for the environment.
- There are individuals which run and operate Burstcoin mining farms that only run on solar energy.



# Energy Efficient and Current State

**1000 kWh**

Electricity consumed per  
transaction (Bitcoin)

**0.0024 kWh**

Electricity consumed per  
transaction (Burst)

**8,112,058**

TOTAL TRANSACTIONS

**176,856**

BURST WALLETS

**489**

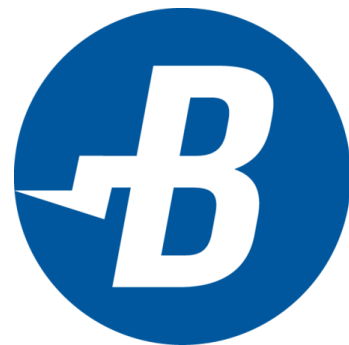
FULL NODES

**429,105**

TERABYTES CURRENTLY MINING

# How does NVMe and NVMe-oF plays into the current landscape of PoC

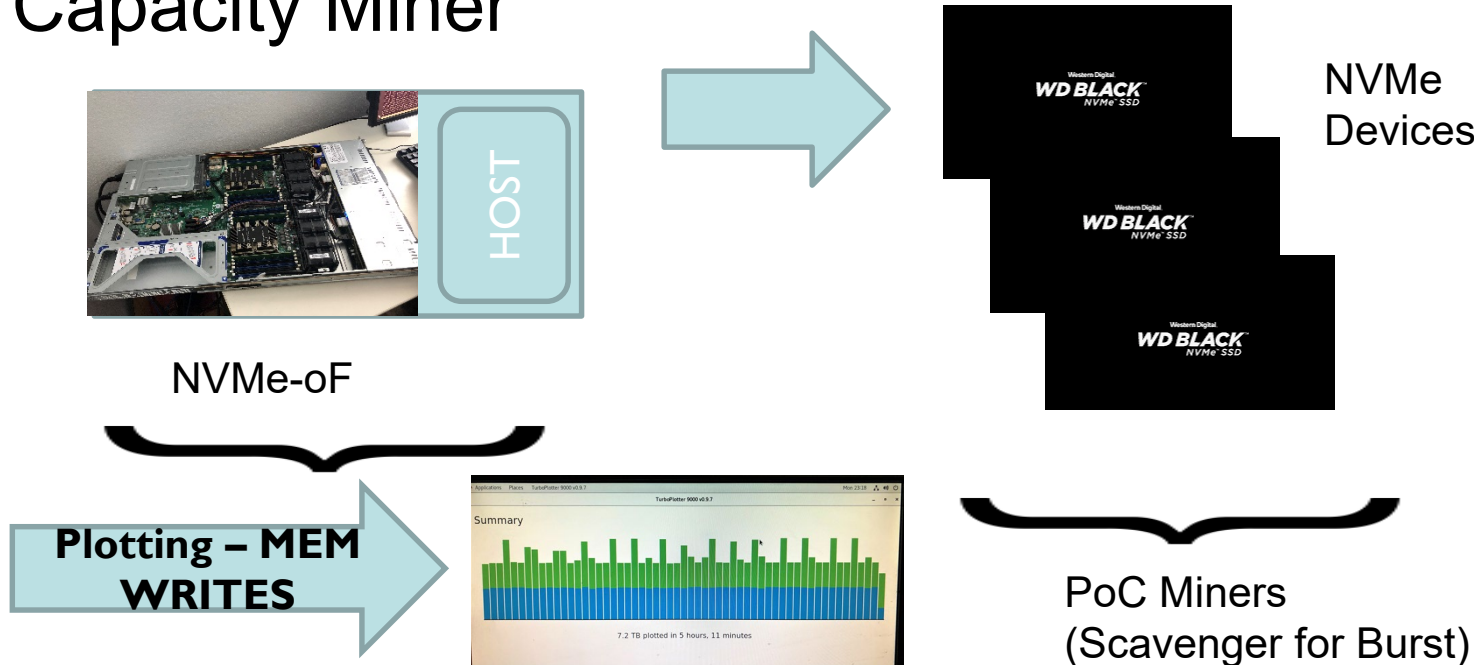
SDC<sup>19</sup>



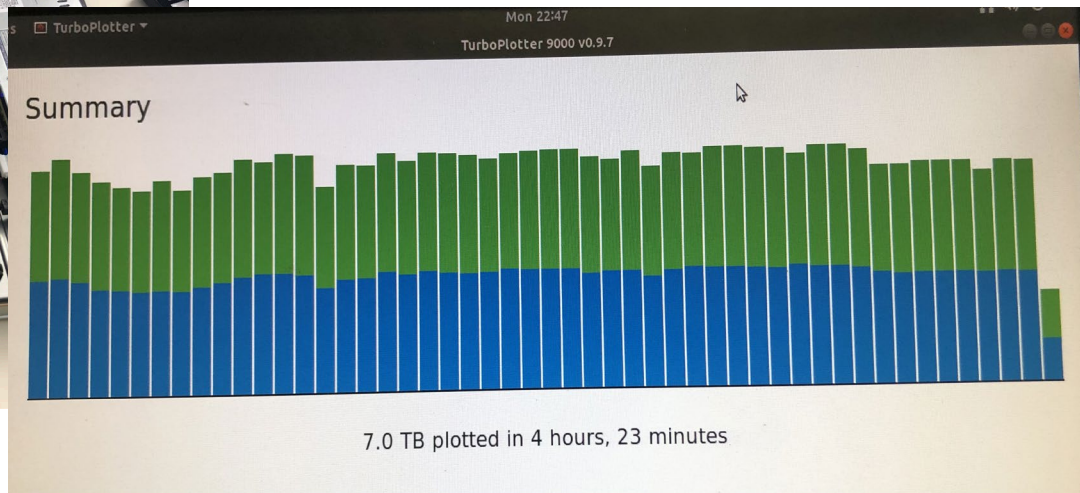
**Western Digital®**

# Building Blockchain using NVMe and NVMe-oF end to end solutions

## The architecture and setup for Blockchain Proof of Capacity Miner



# Examples of Plotting and Mining with Supermicro



# Why decentralized concept can be effectively utilized in NVMe

Architectural decentralization  
Political decentralization  
Logical Decentralization

Advantages	Disadvanges
Fault tolerance	Lack of Focus – too many decision makers
Attack resistance	Speed of Action
Collusion Resistance	Duplication of Work

# Network limitations for Data processing

Blockchain technology is a chain of “blocks” that contain data. It is a distributed database system that accommodates a continuously growing list of immutable blocks. Blockchain allows consumers and suppliers to have a transparent mode of communication and transaction to connect directly without the need of middlemen.

- **KEY ELEMENTS :**
  - **Signature verification**
  - **Redundancy.**
  - **Attaining consensus**
  - **Complexity**
  - **Energy and resource consumption**
  - **Security flaws**



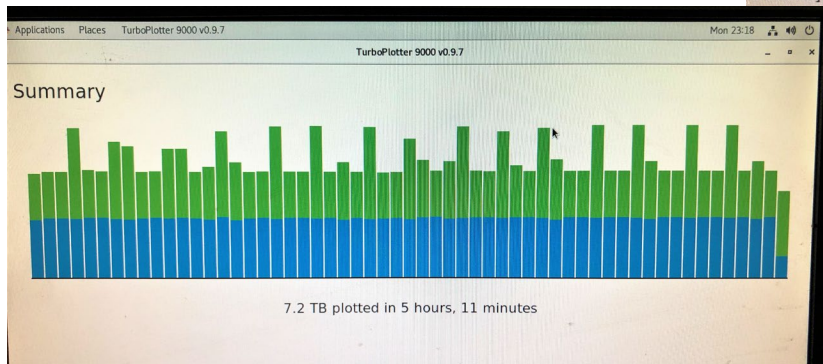
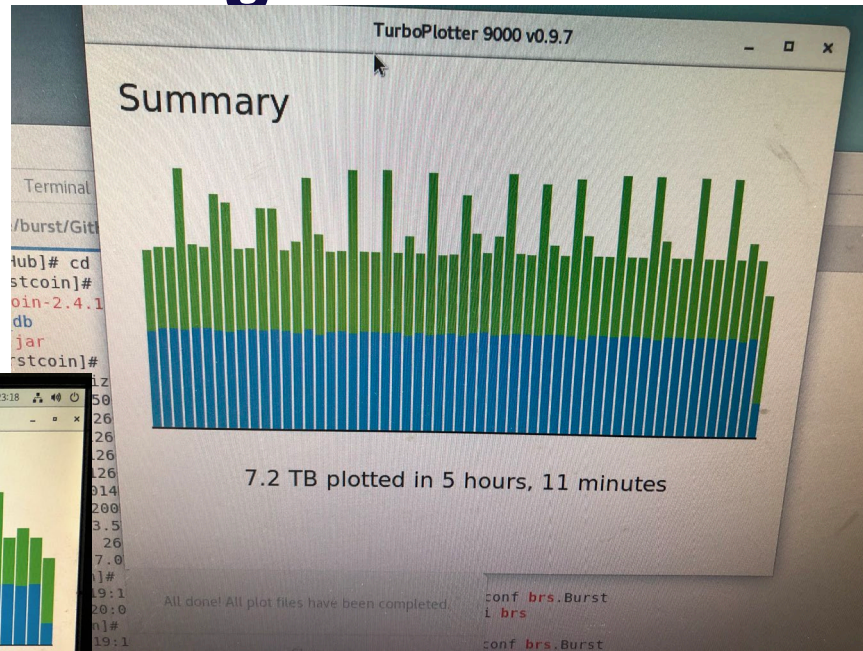
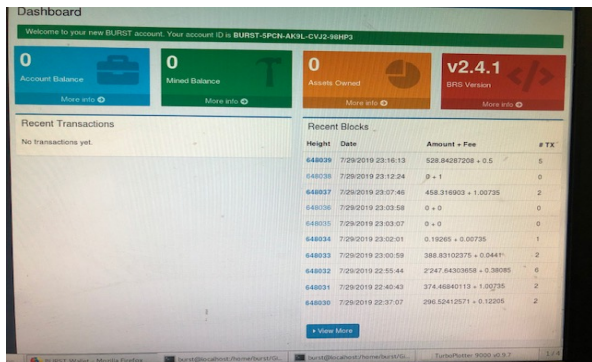
# Blockchain and NVMe – Plotting and

September 23-26, 2019

San Jose, CA

## Mining

SDC<sup>19</sup>



# NVMe/NVMe-oF

## Performance benchmarks for NVMe and Blockchain today



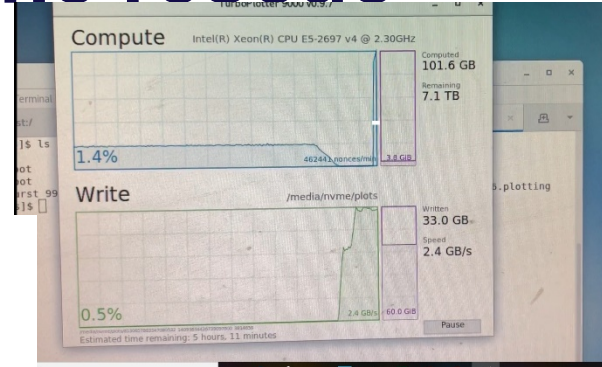
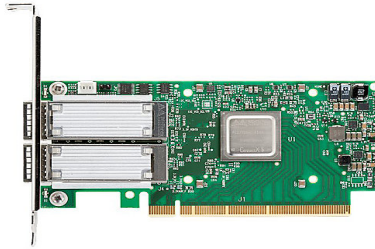
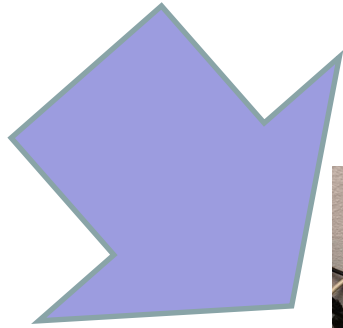


# Advantages of using NVMe/NVMe-oF by mining Proof of Capacity

- Better read performance for mining.
- Significant write performance increase for plotting.
- Improvements in NVMe and NVMe-oF allow further optimization of drive resources
- POC mining allows for usage of under or unutilized resources within storage systems.

# NVM Technology to the rescue

“it took 16 hours on a 4TB 7200rpm Toshiba on my 16c32t machine. I was getting 32K nonces/min “ ( Burst



HPE Proliant Server  
+ Mellanox NIC 100Gpbs  
+ WDC NVMe/NVMe-oF  
=> 5 hours, 11 minutes 7.2 TB

# NVMe and Exchange? Reality of Myth?

- What powers the Crypto Exchange?
  1. Flexibility to customization and scaling
  2. Security
  3. Easy management
  4. The incredibly low delay time for the user
- Imagine we apply recent development and advances in NVMe and NVMe-oF to address this .....
- .....and so much more

# What is a Digital Exchange

- A digital exchange is a privately owned marketplace for individuals to buy and sell crypto currencies at real time.
- Often times, exchanges require crypto currencies to provide them with large volumes of said coins to be made available for sale, in addition to listing fees.
- Some of these exchanges require something called KYC or Know Your Customer which requires users to provide identifying information to these exchanges.
- They make it convenient for everyday individuals to purchase crypto currencies.

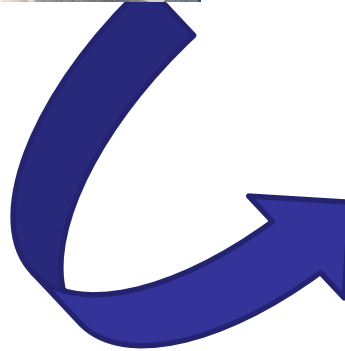
# What is a Crypto Currency ATM

- Crypto currency ATM machines are very similar to ATM machines financial institutions own.
- However, most of these machines are independently owned and require the owner(s) to have a MSB license.
- ATM Operators are also required to have crypto currency to replenish each machine to make it available for purchase.
- Cost of crypto currency isn't always updated real time, sometimes costing users and the owners more money.

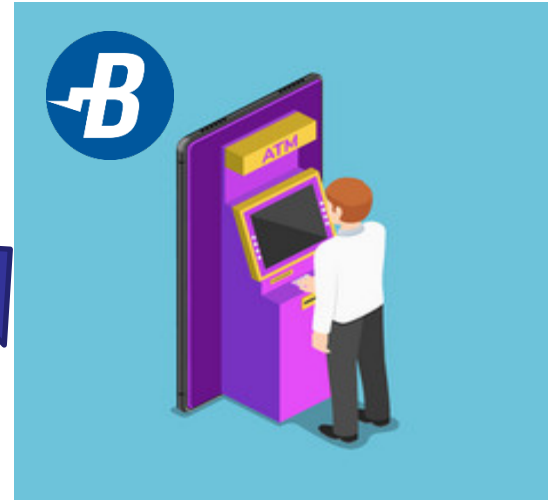
# NVMe powered ATM machines



ATM machines powered  
by NVMe drives (WDC image)



Crypto ATM machines  
powered by NVMe drives



# What are dApps

- dApps or Decentralized Applications are a new solution that has been brought about through the introduction of blockchain;
- Individuals are becoming more aware of privacy, manipulation or censorship issues that arise from the use of centralized services.
- dApps enable individuals to interact with products and services in a more transparent, censorship free manner.
- Ethereum blockchain has made it easy for everyday individuals to create dApps.

# Some comparison notes between Apps and dApps

Apps	dApps
Proprietary code – software applications	Open Source
Software runs on Android or iOS	Decentralized
Free or pay to use	Incentivized
Security can be an issue	Protocol Centric



# Burstcoin dApps

- Burst DNS – Burstcoin DNS system that allows aliases.
- Cloudburst – Enables the user to store files on the blockchain, it is currently capped at 1 MB.
- Burtcoupons – Contractless, smart contract which you can use to create or claim password protected transactions.
- Blockplay – Online auctions utilizing the Burstcoin Blockchain.
- P-Chains – Private Blockchains that reconcile the Burstcoin Blockchain.

# Interested in Learning More?

- You can use the following websites:

<https://myactionspot.com/myactionspot/blockchain-services/>

Donate and get involved ->

<https://www.burst-coin.org/>

Need more information ? Details?

- Schedule a meeting with us :

[info@myactionspot.com](mailto:info@myactionspot.com) or [nixops@protonmail.com](mailto:nixops@protonmail.com)

September 23-26, 2019  
Santa Clara, CA

# Q&A