

Tackling Data Inefficiency: Compressing the Bitcoin Blockchain

Alexander Marsalek | amarsalek@iaik.tugraz.at

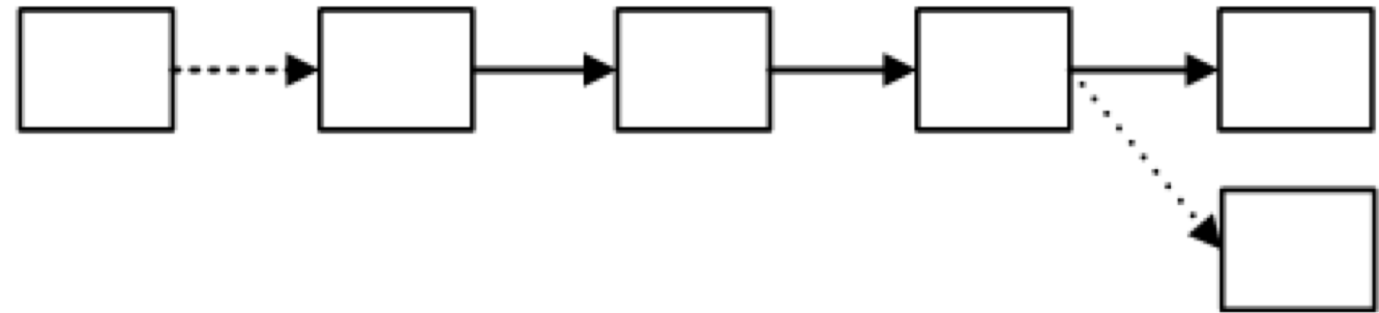
Thomas Zefferer, Edona Fasllija, Dominik Ziegler

Institute of Applied Information Processing and Communications
Graz University of Technology, Austria

06.08.2019

Background - Bitcoin

- What are:
 - Miners
 - Transactions
 - Blocks
 - Proof-of-Work
 - Block rewards
 - Consensus algorithms
 - UTXO set

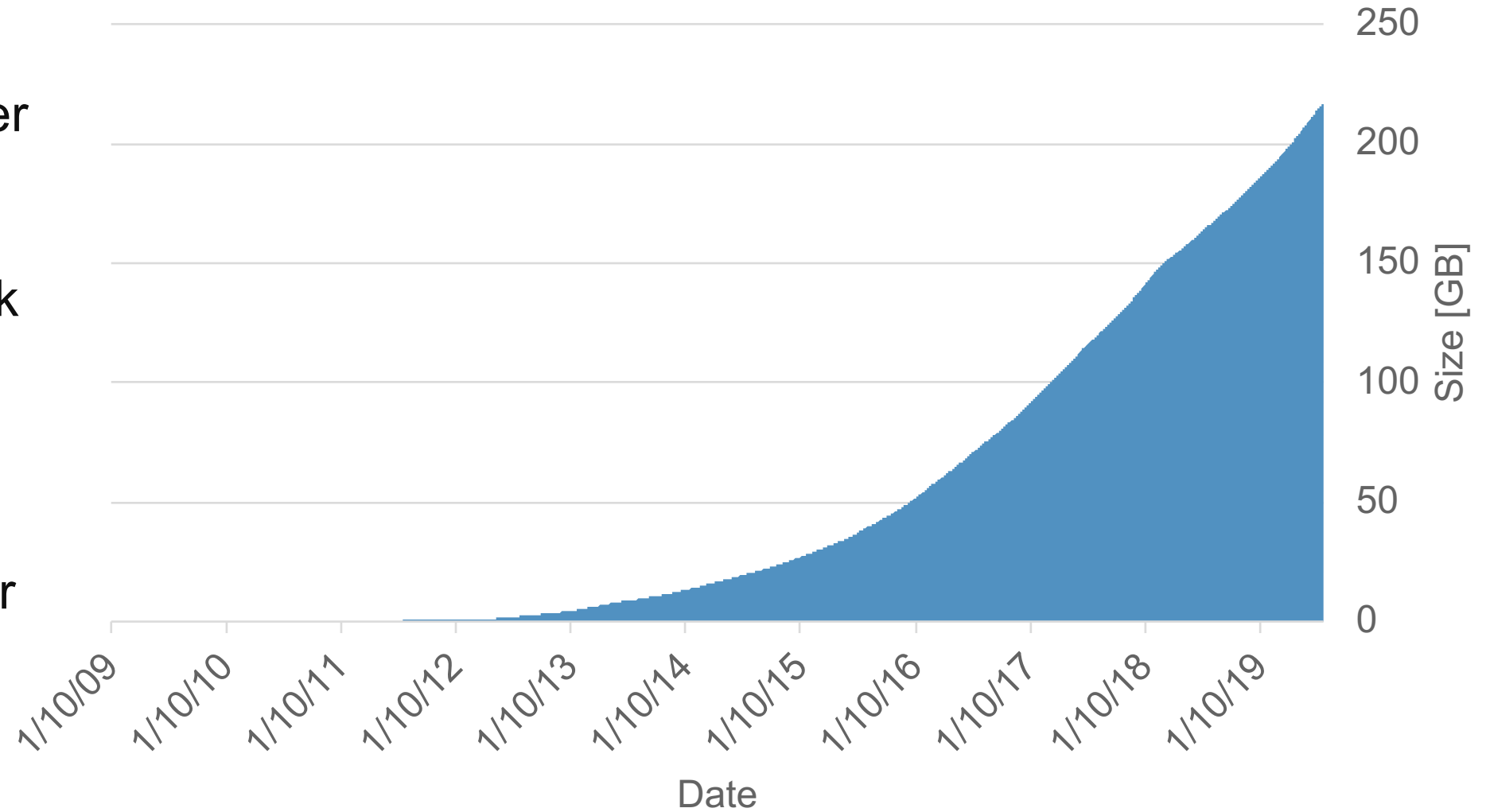


Bitcoin Nodes

- Full Nodes
 - Check every transaction and block
 - Need full copy of blockchain
 - Build & maintain UTXO set
 - Needs a lot of local storage
- Lightweight Nodes
 - Can check if a transaction is included in a block
 - Need only block headers
 - Can only perform block validity checks
 - Queries full node
 - Trust full node
 - Limited privacy

Issue

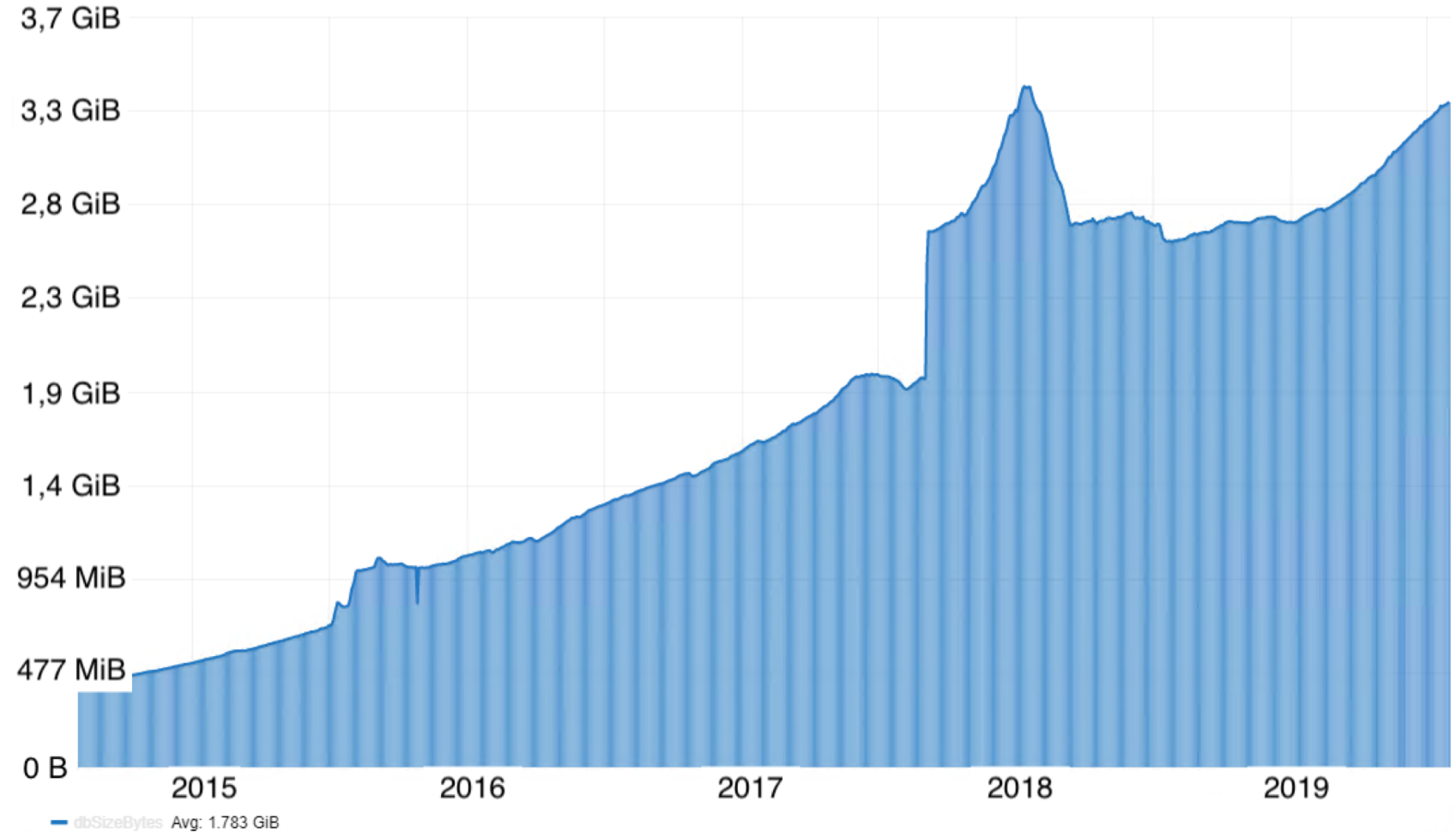
- Append only ledger
 - Size increases with every block
 - 2011: 822 MB
 - Now: 217 GB
 - ~ +52 GB / year



Source: <https://charts.bitcoin.com/btc/chart/blockchain-size>

UTXO Set

- Contains only relevant information
- Grows & shrinks
- ATH: 3,6 GB



Source: <https://statoshi.info/dashboard/db/unspent-transaction-output-set>

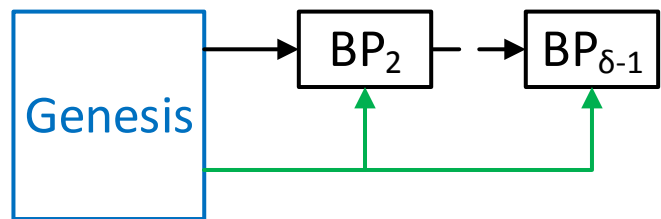
Goals

- Node
 - Full node like security & privacy
 - Runs on resource constrained device

Approach

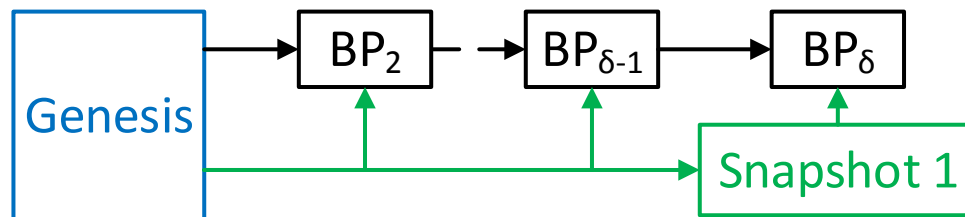
Idea

- Enforced by new rule:
 - Periodically create snapshot blocks



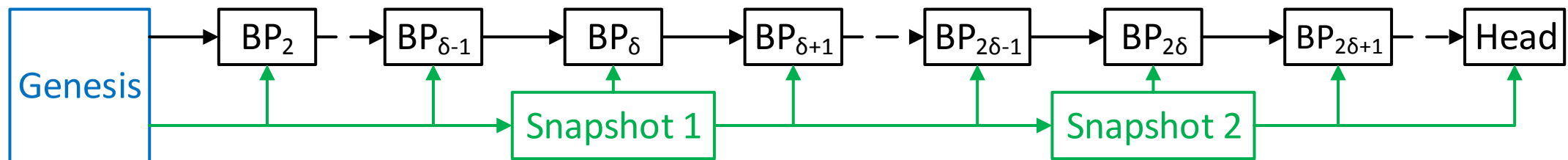
Idea

- Enforced by new rule:
 - Periodically create snapshot blocks



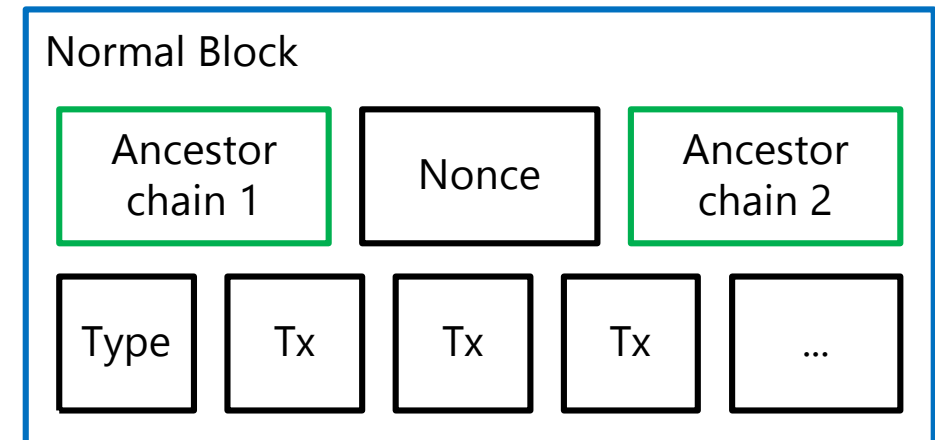
Idea

- Enforced by new rule:
 - Periodically create snapshot blocks



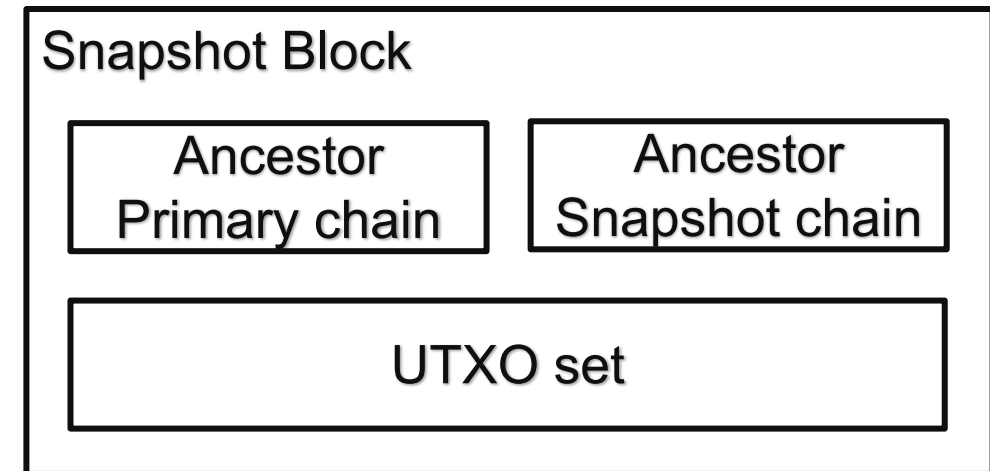
Normal Block

- Add new field
 - References the last snapshot block



Snapshot Block

- Contains:
 - UTXO set
 - Reference the previous snapshot block
 - Reference to last block considered for snapshot



Thin-Client Synchronization

Input: confidence factor α

1. Load head block
2. Load referenced snapshot block
3. Load all blocks between
4. Check if snapshot block is confirmed by at least α blocks
 - If yes: load all block headers & verify chain
 - If no: load previous snapshot block and continue with step 3.

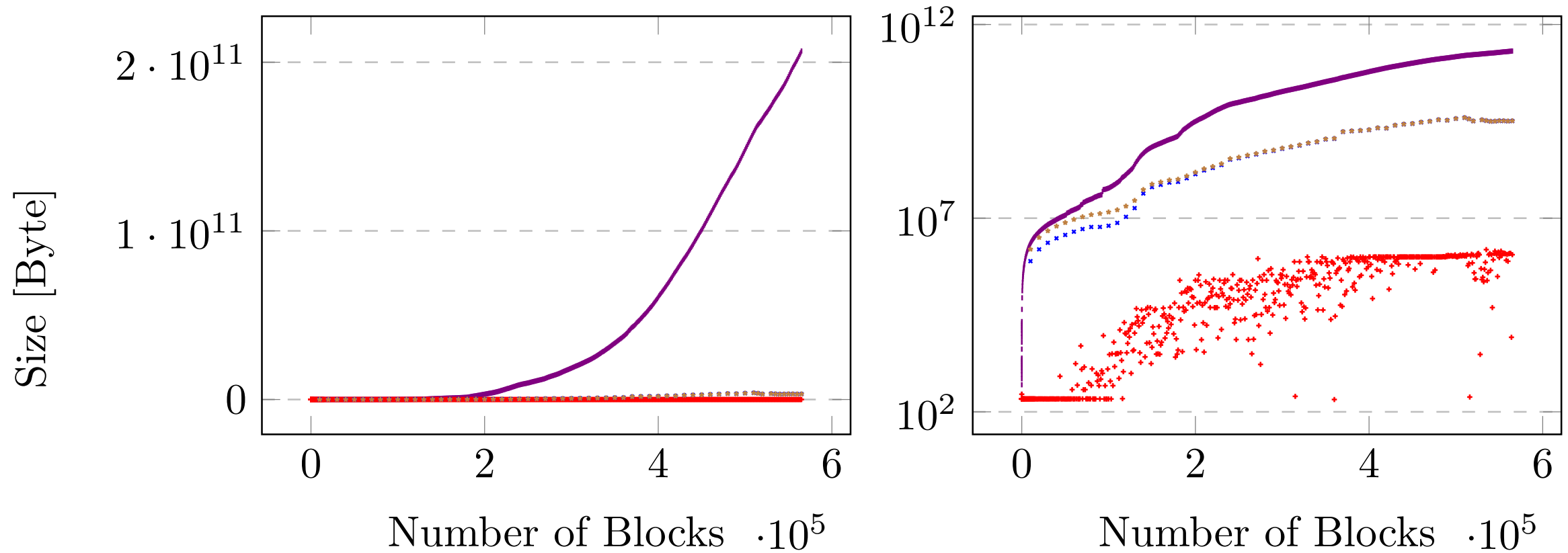
Evaluation

Evaluation

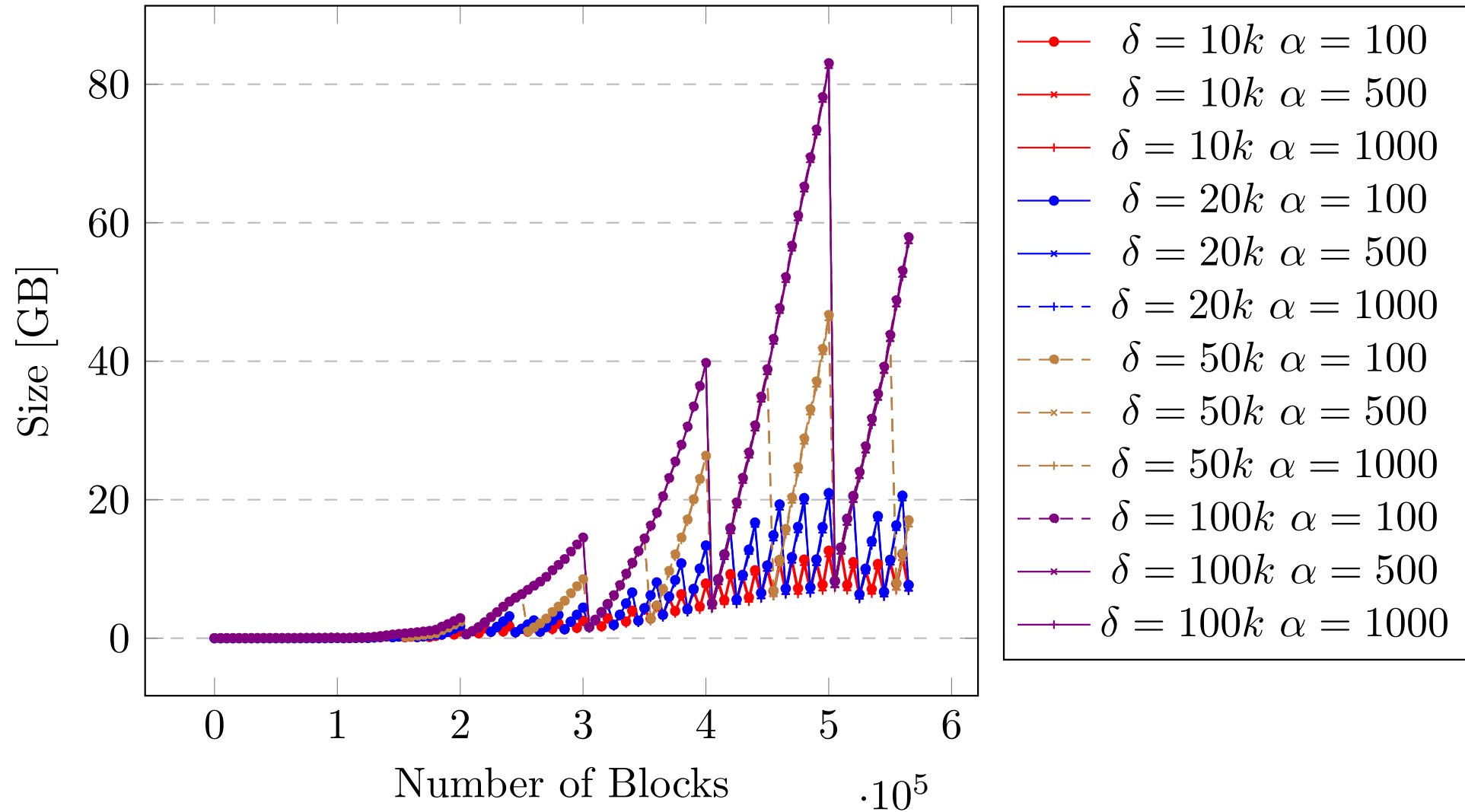
- 2 parameters:
 - Snapshot interval: 10k, 20k, 50k and 100k
 - Confidence factor: 100, 500, 1000

Blockchain -, Block -, UTXO - Size

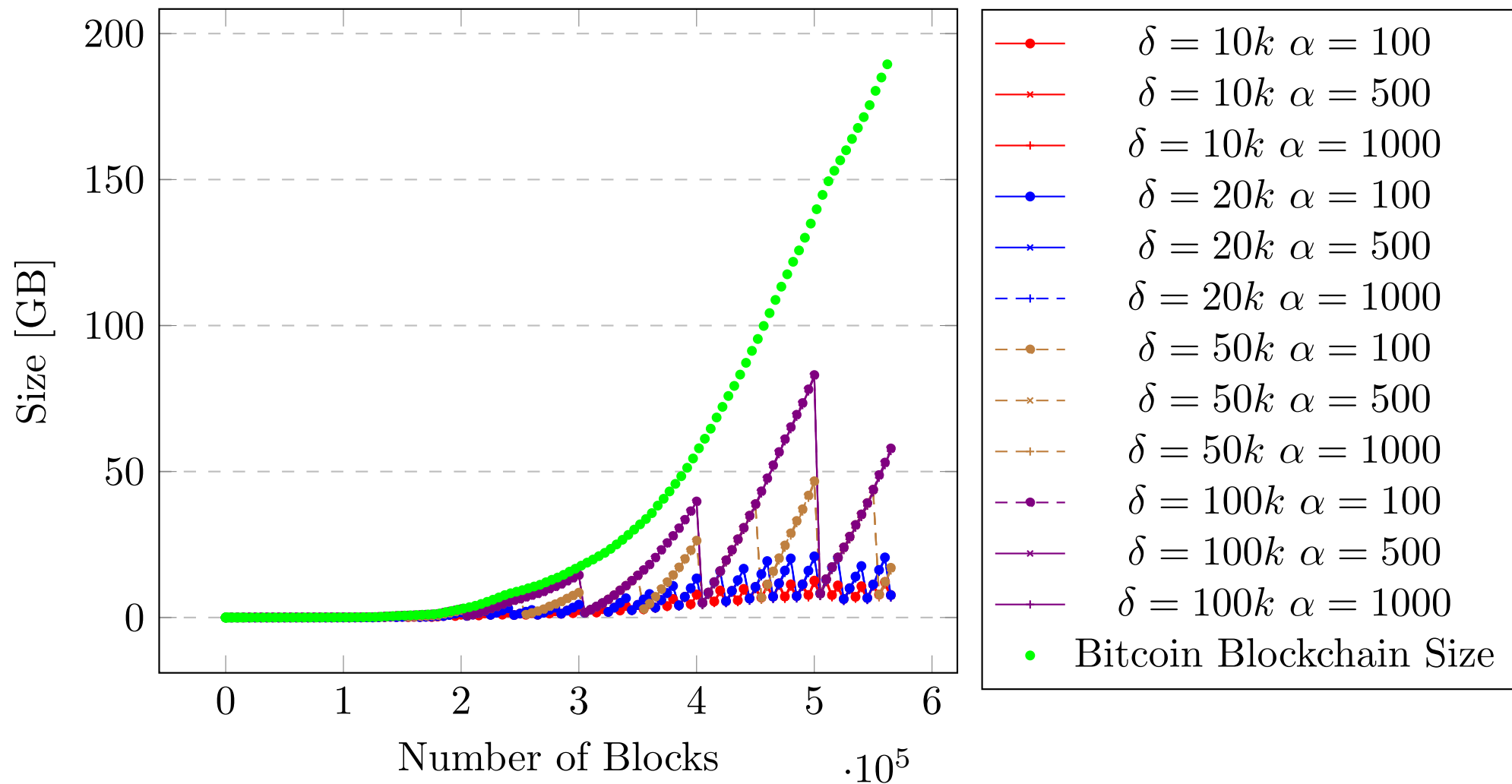
| Blockchain Size + Block Size × UTXO Size * UTXO Size + Block Headers



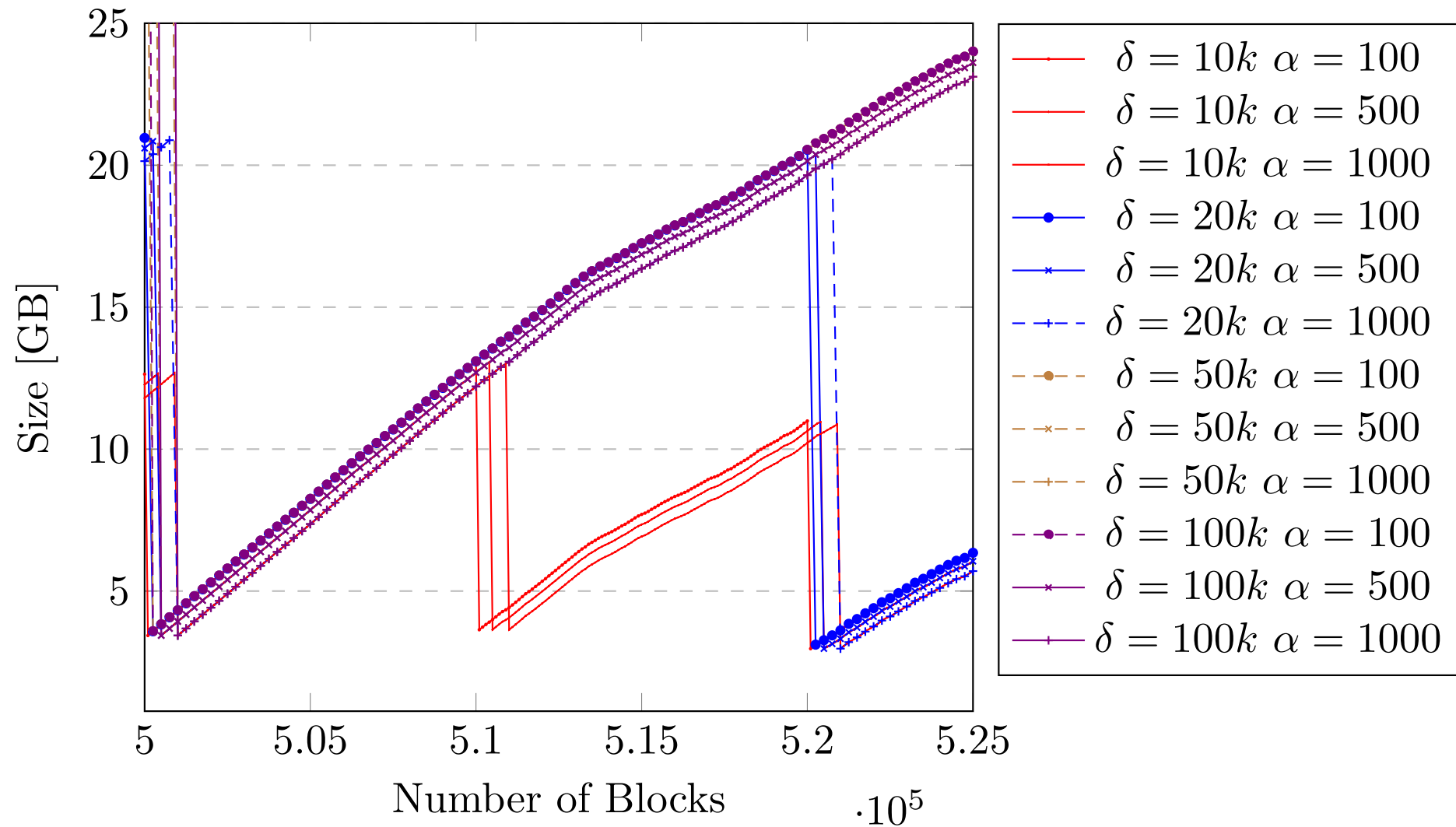
Impact of Snapshot Interval



Comparison: Synchronization Amount



Impact of Confidence Factor



Conclusions

- Proposed approach creates periodically snapshots
- No change in trust assumption, no central or trusted authority
- With $\alpha=10000$, the size can be reduced by 93%
- Confidence factor has almost no impact