IBM Storage

Storage needs for blockchain technology point of view

Document version 3.1
## Contents

- Introduction ........................................................................................................... 5
- 1 Blockchain storage calculations ........................................................................ 8  
  - 1.1 Blockchain assumptions ............................................................................... 8  
  - 1.2 Calculation .................................................................................................. 8  
- 2 Off-chain storage requirements ........................................................................... 9  
  - 2.1 Off-chain assumptions ............................................................................... 10  
  - 2.2 Calculation ................................................................................................ 10  
    - 2.2.1 Storage required for documents ......................................................... 10  
- 3 Performance ....................................................................................................... 12  
  - 3.1 Service-level agreements ......................................................................... 13  
- 4 Storage specification ......................................................................................... 13  
- 5 Processing requirements for off-chain .............................................................. 14  
- 6 Backup, recovery, and disaster recovery of off-chain ........................................ 15  
- 7 Does the source blockchain matter? ................................................................. 16  
- 8 Summary and recommendations ...................................................................... 17  

## References ............................................................................................................ 18
List of figures

Figure 1: What is a blockchain? ................................................................. 5
Figure 2: Hyperledger structure ............................................................... 6
Figure 3: IBM Blockchain Architecture .................................................... 7
Figure 4: World-wide blockchain projected spending .................................. 7
Figure 5: Graph of storage required per TPS per year for blockchain (IBM calculation) ........................................ 9
Figure 6: Required storage for blockchain based on transactions per second ................. 11
Figure 7: Blockchain runs on nodes at each peer ....................................... 12
Figure 8: Example NVMe-based storage system ......................................... 13
Figure 9: POWER9 versus x86 performance on database loads (copyright IBM) ........ 14
Figure 10: Cryptokitties was the first success for Ethereum ERC721 blockchain .......... 16
INTRODUCTION

What is a blockchain? Pioneered by cryptocurrencies such as bitcoin and Ethereum, blockchain is a model for a distributed, trusted, shared, ledger in which you can store transactions. Each transaction is encrypted and identified by a cryptographic signature that is chained to the previous block through additional cryptographic keys. This allows for the blockchain to be a shared, immutable source of truth as each block stores a hash or signature of the previous block. Thus, any change to a block would require recalculating all subsequent blocks and updating the entire chain. Figure 1 shows this concept.

What is a Blockchain?

The cryptocurrencies use either proof of work (PoW) or proof of stake (PoS) to be a member of the chain. PoW is a set of complex calculations that result in the creation of a new bitcoin and some estimates suggest that the computations require an equivalent of 5 to 7 kilowatt (kW) of energy be used per bitcoin. Obviously, PoW blockchains are not a high-performance option. PoS blockchains allow you to purchase into a blockchain, slightly more performant but still not a good way to perform thousands of transactions per second (TPS). A PoW blockchain can currently perform about 10 TPS under test and around 3 in reality, whereas a PoS can perform about 20 TPS under test and 6 to 8 TPS in reality. Both of these are non-permissioned blockchains where no one knows the other participants other than their hashed, encrypted identifiers.

Bitcoin is a PoW and Ethereum is a PoS. In PoW, you must utilize a cryptocurrency that you have mined to be a member, and in PoS, each blockchain transaction requires that you have cryptocurrency you have purchased. Each Ethereum transaction requires that you provide gas, which is a subset of an Ether, the cryptocurrency of Ethereum. Currently, Ethereum is one of the only cryptocurrency-based blockchains that provide (through their ERC721 specification for non-
frangible tokens) non-cryptocurrency assets to be traded. A frangible token is a single ether or single bitcoin that can be subdivided. A non-frangible token would be a car, house, diamond, or other asset that is normally sold as a complete unit.

The Hyperledger blockchain model is a permissioned, non-POW, non-POS model. Essentially you can become a member by being approved by the other members and can fully participate without onerous calculations or having to purchase each transaction. Because no POW or POS is required to use Hyperledger, it can support transaction rates that are limited only by the server computing power and speed of the underlying storage. The current performance is 3500 TPS for a Hyperledger-based, performance-optimized blockchain. It is projected that this could reach as high as 30,000 TPS soon. Hyperledger based blockchains can be utilized to deal with both frangible (fungible) and non-frangible items. Figure 2 shows the Hyperledger structure.

**Hyperledger-fabric model**

*Figure 2: Hyperledger structure*

Blockchain requires both on-chain storage of the core ledger data and off-chain storage of data required by smart contracts for verification and documentation. This is demonstrated in the IBM® Blockchain architecture shown in Figure 3.
Blockchain is becoming a disruptive technology in payments, logistics, medicine, and anywhere a trusted, provenanced, immutable ledger is required. Blockchain is projected to be a USD 9 billion industry by IDC by the year 2021. This is shown in Figure 4.

Recent studies have shown that permanent storage for blockchain data can cost as much as USD 100 per gigabyte (GB). Within the Hyperledger environment, it has been estimated that storage for
the blockchains alone, in medium to high-level transaction environments, could be as high as 197 terabytes (TB) or more per year. Figure 5 shows the estimated storage required per transaction per second, per year.

Attempting to find hard data for the storage required for Hyperledger blockchain, for either on-chain or off-chain data is difficult due to the newness of the technology and lack of hard documentation by users who are using it in their daily operations. In addition, Hyperledger is in a mainframe storage on the cloud and it can become problematic to get space volume calculations at all.

These calculations show that the primary storage may not be as trivial as everyone assumes. While pruning may come into play for non-financial data, for financial, pharmaceutical, medical, and other types of data, there are proscribed retention requirements (some for 50 years). So, even if pruned from the primary chain, it will still have to be maintained in an archive storage somewhere either in the cloud or on premises.

1 Blockchain storage calculations

Given a basic understanding of storage and some basic understanding of how blockchain stores data, you can derive a back-of-the-envelope calculation on how much storage is required for Hyperledger blockchain.

1.1 Blockchain assumptions

The following assumptions are made in the blockchain storage calculations:

- All calculations will be in actual bytes, that is 1024 bytes is 1 KB.
- All Hyperledger blocks are 1 megabyte (MB).
- Only hash, signature, or key data is stored in the blockchain.
- The company works 8 hours per day. The company has roughly 240 processing days per year and the number of transactions per second are averaged over those days only (allows for holidays and weekends.)
- Currently bitcoin is storing about 1400 basic transactions per MB block. So, Hyperledger blockchains have larger headers and a bit more robust transaction size so 1000 transactions per block was used as a mark in the sand.

1.2 Calculation

Using the assumptions in the previous section, the calculation to find out the amount of storage required per TPS becomes (example for 1000 TPB):

\[
(1 \text { TPS}/1000 \text { transactions per block}) \times 1024 \text { KB/block} \times 3600 \text { sec/hr} \times 8 \text { hr/day} \times 240 \text { days/year} = 7,077,888 \text { KB of data per transaction per year} = 6,912 \text { MB} = 6.75 \text { GB} = 0.00659 \text { TiB/transaction/yr}
\]
Figure 6 shows the application of this value at various transaction levels.

So even at modest transaction rates, storage for Hyperledger blockchain is in the terabyte or multi-terabyte size. Using the most conservative estimate of 1000 transactions per block for the 100 TPS level of blockchain activity, 0.659 TiB of storage per year is required. Going with the estimate of 5 KB per transaction, which is based on the actual test values from the Hyperledger team, only 205 transactions per block has been achieved. At 205 transactions per block, the same 100 TPS would require 3.215 TiB of storage per year.

To put this all in perspective, based on the total size of the ledger and total number of transactions stored, bitcoin is averaging close to 555 bytes per transaction or 1,889 transactions per block and Ethereum is close to 2 KB per transaction or 512 transactions per block.

2 Off-chain storage requirements

Since non-transaction data, such as pictures, contracts, PDF, and personal information should not be stored in the actual blockchain, some form of off-chain or sideDB storage is required. Generally, off-chain data will be unstructured. A hash or signature for the off-chain item will be generated and that is what is stored in the blockchain. The actual item is either stored in the cloud or in a near-cloud storage. It is expected that the required storage for off-chain data will exceed the needs of blockchain storage.

The General Data Protection Regulation (GDPR) specifications for the European Union will also affect how data is stored within a blockchain. Quoting Bertrand Portier - IBM Distinguished Engineer, Blockchain in Financial Services:
“One of the GDPR requirements is the right to erasure which is when an individual asks an organization that has their personal data to completely remove that data. The organization then has a limited time to comply. Well, if you know blockchain, you know that the blockchain ledger is *append-only and immutable* — there is no “undo” button after a write, and the chain of blocks contains historical transaction information that goes all the way back to when the blockchain was created. That can be a challenge for applying blockchain to GDPR. To comply with GDPR, **no personal data should be put on the blockchain directly.** Techniques exist to deal with this, which consist of putting a *cryptographic hash* on the chain or the “evidence” instead of the actual data. More guidance and expertise needs to be collected in this space. And, as my Promontory colleagues would say, “Be sure to check with your legal counsel!”

### 2.1 Off-chain assumptions

The following assumptions are made in the off-chain storage calculations:

- Each transaction does not produce a document. For calculation, a ratio of three transactions for each document is used so a figure of 0.3 is used.
- 8 hours per day is the workday.
- 240 days per year are actual processing days.
- Indexing and other storage requirements are not included.

### 2.2 Calculation

Using the assumptions in the previous section, the calculation becomes:

\[
1 \text{ TPS} \times \frac{\text{docs per transaction} \times 3600 \text{ sec/hr} \times 8 \text{ hr/day} \times 240 \text{ day/year}}{240 \text{ day/year}} = \text{Documents per year}
\]

\[
= 3 \times 3600 \times 8 \times 240 = 814,301 \text{ Documents per year for 1 TPS}
\]

#### 2.2.1 Storage required for documents

According to current references, 1,000,000 documents, of mixed formats, requires 333 GB of storage. This means, 814,301 documents will require:

\[
1000000X / (333 \times 814301) = \text{GB/year/TPS}
\]

\[
X = (333 \times 814301) / 1,000,000
\]

\[
= 271 \text{ GB/TPS/year}
\]

\[
= 0.264 \text{ TiB/Year/TPS}
\]

Figure 6 shows how this storage required per TPS will result in increased storage requirements as TPS increases.
So, as expected you can see if the transactions produce 1 document for every three transactions recorded, the storage required will soon exceed those required for the primary blockchain by an order of magnitude.

Most blockchain projects use already-stored support information that is kept in on-premises data sources. This leads to an unrealistic expectation that no secondary data store will be required for blockchains. As the technology matures, more and more of this off-chain data will be generated and, for performance reasons, will be stored in dedicated data stores designed to provide optimal access to this data for all network peers. The delays from using adapters into existing, non-optimized data sources will become unacceptable. In addition, these existing data storages are tied in with systems designed around obsolete applications that will be replaced by the blockchain application and so, must be redesigned.

Each peer that participates fully in the blockchain will own a node and will require off-chain storage. The amount of storage specified in these sections on on-chain and off-chain storage are per node. Figure 7 demonstrates this concept.
One final point is that many blockchain projects are driven by a consortium. These consortium driven projects specify that a new, secure infrastructure be used. Each member is required to have off-chain storage and processing that is equivalent in capacity and performance.

### 3 Performance

After the initial proof of concept activities are complete, performance takes the primary focus for on-or off-premises storage of off-chain data. Having to cobble together access links to existing data stores might cause unacceptable performance. The off-chain data must be stored in near-cloud storage in dedicated data stores. This is known as cloud-edge storage. In file systems, such as Internet Protocol (IP) file system or the InterPlanetary File System (IPFS), each member is responsible for storing and sharing their secondary data with all other members in the blockchain network. In such a file share system, the weakest link will be the member with the slowest off-chain storage, assuming that the consortium is using a central shared-storage for the blockchain data itself.

While much of the focus for Ethereum, and other, blockchain development efforts have been in the realm of open source solutions such as BigDB and IPDB, based no doubt on their non-establishment bias, enterprise-level blockchain users will be looking for proven enterprise-level databases such as Microsoft® SQL, Oracle, and IBM DB2® as well as Postgres. Instead of reinventing the wheel and having to take significant reliability and performance hits as the technology matures, enterprise developers utilize existing, proven technologies. For enterprise-level blockchain users, the focus for secondary data stores should be on utilizing the best existing, tested, and proved database technology for the type of off-chain data being stored: structured, unstructured, or both.
Newer storage technologies such as NVME will reduce processor cycle requirements for storage thus increasing the cycles available for cryptosecurity-related calculations. IBM designed hash/signature engines designed for blockchain will also offload processing cycles. Figure 8 shows a Non-Volatile Memory Express (NVMe) or NVMe-like storage system.

A historical reference may serve to demonstrate the need for performance. When Hanna was first introduced, it was portrayed as a memory-only database and storage was not that important. It was later found that utilizing the proper, low-latency, high-speed storage under the Hanna database improved performance by at least 30%. If performance had been a key concern from the beginning, many projects would have been more successful.

3.1 Service-level agreements

All members of a blockchain network, Hyperledger, Ethereum, or Corda, will have to commit to a service level agreement (SLA) specifying minimal latency and bandwidth requirements for both on- and off-blockchain storage. In the IBM model using Hyperledger, the on-chain storage and processing is accomplished with a cloud-based containerized virtual machine (VM) sharing a centralized storage. Processing will be done in memory thus providing the best processing and storage latencies. Network consideration will have to be given about transactional logic and efficiency to ensure optimal benefit is acquired from processor and memory resources. However, the off-chain, cloud-edge storage would be at the discretion of each member, and thus the need for an agreement to performance-based SLA between members.

4 Storage specification

Ideally, the off-chain storage is a self-contained processing and storage system capable of tiering non-critical data and providing optimal speed for current or critical data. Co-storage with existing application data would result in sub-optimal performance and might lead to SLA violations and ejection from the network. Any storage must also be scalable, as far as storage volume, with invisible addition of storage capabilities. What is meant by invisible is that adding additional storage should be completely non-impactful to existing operations and transactions. Use of a virtual machine environment such as VMWare or Oracle VM would allow deploying identical systems to each
member of a blockchain network, and, as long as identical hardware was deployed to host the VM environment, similar if not identical performance would be obtained.

IBM proposes that the storage for off-chain data be architected accounting for the needs of the data, whether it is structured, unstructured, or both. This means there is no one-size-fits-all solution, but instead a portfolio of storage and compute options must be supplied, allowing the blockchain developer or user to choose the best fit for their environment. It is beneficial to performance if the off-chain storage uses NVMe or NVMe-like processing to offload processor cycles.

5 Processing requirements for off-chain

Unlike the blockchain environment itself where the processing and storage requirement will be met by the resources in the cloud, the off-chain processing required by the off-chain storage (whether it is enterprise or open source) will have to be met by each participant in the blockchain network. The IBM POWER® series of processors, the latest being the IBM POWER9™, utilizing IBM architecture, has shown superior performance, reliability, and security to the x86 processor-based commodity servers. However, the VersaStack combination of UCS and storage has also shown performance, reliability, and security. Each participant should have identical processing assets to ensure that the performance of the overall blockchain is not compromised. Therefore, the processing requirements of off-chain or sideDBs is a critical factor for the overall performance of the blockchain environment. Figure 9 shows the relative performance of the IBM POWER9 processor against the equivalent x86 environment for database processing using DB2. Other database tests show parallel performance results.

![Power L922 vs tested x86 system - Db2 Warehouse](image)

Figure 9: POWER9 versus x86 performance on database loads (copyright IBM)
6 Backup, recovery, and disaster recovery of off-chain

Given the critical nature of off-chain data, trusted and secure means of backup, recovery, and replication must be provided. Solutions such as IBM Spectrum® products should be utilized to provide enterprise-level backup, recovery, and replication services. Figure 6 shows an IBM proposed architecture that includes all needed features of a backup and recovery scenario including disaster recovery.

Within the on-premises storage, backup is accomplished by use of the IBM Spectrum Copy Data Management suite of applications. This provides for the backup and recovery due to data corruption or local failure. Through use of replication services to the cloud, whether it is IBM Cloud™, Amazon Web Services (AWS), or Microsoft Azure, disaster recovery is easily enabled.

For block and file transfer to cloud, IBM Spectrum Virtualize™ on IBM Cloud enables hybrid cloud solutions, offering the ability to transfer data between on-premises data centers and any IBM Spectrum Virtualize base appliance (IBM SAN Volume Controller (SVC), IBM Storwize®, IBM FlashSystem® V9000 and VersaStack or IBM Spectrum Virtualize only and IBM Cloud).

For unstructured data, IBM Cloud Object Storage provides an innovative, secure, and cost-effective way to store and manage data without creating multiple copies. IBM’s groundbreaking SecureSlice technology distributes data slices across storage systems for security and protection. This unique approach combines encryption, erasure coding, and information dispersal of data to multiple locations for protection without complex or expensive copies. The service is continuously available; it can tolerate even catastrophic regional outages without downtime or the need for customer intervention.

To achieve similar dispersed storage on other leading clouds, customers would have to invoke a replication technique to create a second copy of the data in a separate region, which they would have to manage. IBM Cloud Object Storage does not require replication techniques or complex configurations to make it fast and efficient to meet cloud data storage needs.

Some users might want to use some sort of stand-alone utility to interact with their storage. As the Cloud Object Storage API supports the most common set of S3 API operations, many S3-compatible tools can also connect to Cloud Object Storage using HMAC credentials.

Some examples include file explorers such as Cyberduck or Transmit, backup utilities such as CloudBerry or Duplicati, command line utilities such as s3cmd or Minio Client, and many others.
7 Does the source blockchain matter?

All blockchains that will be used for tokenized, non-frangible data, will require off-chain storage. When the ERC721 standard was released in November 2017, one of the first uses was for Cryptokitties. Cryptokitties are stylized cat pictures that contain a DNA code for their features. Cryptokitties can be mated to produce a unique offspring based on the DNA of the parents and a proprietary mixing algorithm. After the introduction, the traffic for Cryptokitties crashed the Ethereum network. If more robust storage and planning for off-chain storage and server assets had been used, they would have not had this issue. Within a few months, the Cryptokitties were generating transactions equivalent to USD16 million dollars and had grown to over 600,000 distinct Cryptokitties. While Cryptokitties itself was a great success, the underlying infrastructure failed. While the Cryptokitties example seems frivolous, it does show that you must always plan for success.

![Cryptokitties was the first success for Ethereum ERC721 blockchain](image)

Whether it is ERC721 data in Ethereum, pictures of diamonds in Hyperledger or whatever comes down the pike for other blockchain specifications, off-chain storage of some kind will be required. Therefore, this specification is good, no matter the source of the off-chain data.
Summary and recommendations

In view of this need for tiered, high performance, self-contained storage, IBM offers a variety of storage products (both hardware- and software-defined storage) that can meet the on-chain and off-chain needs for blockchain. The IBM FlashSystem 9100 product delivers performance (NVMe), security (encryption), and controls (SVC) to meet the various blockchain peer and node requirements. In addition, the VersaStack solution is an ideal candidate for tiered storage needs.

High-performance processors to calculate and confirm the needed crypto-hash and signature verifications as well as handling off-chain database processing requirements will necessitate the use of IBM System Z® (LinuxONE or POWER9 processor-based computing assets).

Backup, recovery, and replication services must be robust, tested, and trusted and must provide enterprise-level performance and reliability, to that end, the Spectrum suite of products is suggested. Utilization of containerized, virtual environments will ensure performance as long as they are deployed on identical hardware platforms as defined. Obviously, deploying a container into a low-performance x86 processor-based environment will not be as performant as deploying it in a high-performance IBM System Z (LinuxONE) system.

Regardless of the perceived size needs, the performance of the storage assets for off-chain data will be critical, or the entire blockchain environment, may be Hyperledger fabric, Ethereum, or Corda based, will grind to a halt.
REFERENCES

Figure 2 source: IDC’s Worldwide Semiannual Blockchain Spending Guide, 1H17.

Figure 5: Based on IBM internal testing of Db2 Warehouse executing a sample analytic workload of 30 distinct queries of varying complexity (intermediate & complex). Results valid as of 3/14/18 and conducted under laboratory condition with speculative execution controls to mitigate user-to-kernel and user-to-user side-channel attacks on both systems, individual results can vary based on workload size, use of storage subsystems, and other conditions.

Three nodes of IBM Power® System L922 (2×10-core/2.9 GHz/512 GB memory) using 2 x 300 GB SATA 7.2 k rpm LFF HDD, 1 GbE two-port, 10 GbE two-port, 1 x 16 Gbps FCA running DB2 Warehouse 2.5 and IBM Spectrum Scale™ 4.2 with RHEL 7.4.

Competitive stack: Three nodes of 2-socket Intel® Xeon® SP (Skylake) Platinum 8168 (2×24-core/2.4 GHz/512 GB memory) using 2 x 300 GB SATA 7.2 k rpm LFF HDD, 1 GbE two-port, 10 GbE two-port, 1 x 16 Gbps FCA, running DB2 Warehouse 2.5 and Spectrum Scale 4.2 with RHEL 7.4. Pricing is based on Power L922 (http://www-03.ibm.com/systems/power/hardware/linux-lc.html) and typical industry standard x86 pricing (https://h22174.www2.hpe.com/SimplifiedConfig/Index) Db2 Warehouse pricing is based upon USD regional perpetual license costs where certain discounts can apply.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.