

Sharder Whitepaper

Multi Chain Storage and Validation Network V3.0 2020



Website : <https://sharder.org>
Email : hi@sharder.org
Telegram : https://t.me/sharder_talk
Twitter : <https://twitter.com/sharderchain>
Github : <https://github.com/sharders>

1. Overview	3
2. Definitions	4
3. Design Philosophy	4
4. Sharder Storage	5
4.1 Definition of Roles	5
4.2 Network Topology	6
4.3 Data Security	7
4.3.1 Data Encryption	7
4.3.2 Data Sharding	7
4.3.3 Data Replication	8
5. Sharder Storage & Validation (SV) Network	9
5.1 Sharder Architecture	10
5.2 SV and Authentication Transaction Process	11
5.3 File Hash (Fingerprint)	11
5.4 SV Transactions	11
5.5 Authentication Transactions	12
5.6 Multi-chain	12
5.7 Blockchain as a Service	14
5.8 User Interaction	14
5.9 Document Validation & Authentication for Business	15
6. Sharder Account	17
7. Sharder Consensus	17
7.1 Sharder Nodes	17
7.2 Sharder Pool	19
7.3 CPoS weighted table	20
8. Tokenomics	22
8.1 Token Type:	22
8.2 Total Supply	23
8.3 Burning / Reduction of Supply	23
8.4 Storage Costs & Transaction Fees	23
8.5 Fee distribution	23
8.6 Sharder Pool Staking Limits	23
8.7. System / mining rewards	24
9. Applications	25
9.1 SignEase	25
9.2 ISLAND	25
10. Road Map	25

1. Overview

Vision: To build a global, peer to peer, secure, cross-chain, distributed storage network that is online 24/7. The Sharder Network will provide storage, storage validation and authentication capabilities that reimagines and redesigns the way people store, exchange and validate valuable data.

Sharder is a distributed storage and validation network under multi-chain architecture. The name, “Sharder” comes from the word, “shard” a widely used term within computer science. Sharder Client can be deployed together in conjunction with various public blockchains, storage networks and personal nodes.

Sharder Network can provide blockchain storage capabilities with unmatched data security. Sharder solves the problem of data breach that is prone amongst centralized storage solutions. Data stored on the network is encrypted, shard (broken into fragments) and distributed to nodes around the world ensuring data can not be accessed without authorization.

Sharder also offers authentication capabilities along with blockchain storage & validation. Sharder can store and validate documents, contracts and reports by utilizing a files digital fingerprint or file hash. This ensures that all documents are securely stored, traceable, not altered or tampered with and verifiably immutable.

Using Sharder, falsified documents can now become a thing of the past. This business opportunities for Sharder’s document validation are truly endless. Industries ranging from aerospace to education to government and everything in between are set to benefit from this technology.

After more than 2 years of research and development, component testing, network and commercial trials, Sharder is ready for commercial implementation. Sharder’s native token, SS, now has usage scenarios that will allow Sharder’s ecology to progressively improve.

In this white paper, we outline how Sharder constructs a decentralized storage network with storage validation and authentication capabilities. This document has been written for all users, including those without background knowledge in computer science, programming, mathematics.

2. Definitions

CPOS: Credit based Proof of Stake. The consensus used by Sharder to secure the network.

Sharder Chain: The sharder chain is a shared public ledger on which the entire sharder network relies. All confirmed transactions are included in the sharder chain.

Sharder Hub / Box: A hardware device with pre-installed software (Sharder Client) that can join the Sharder Network.

Sharder Network: The decentralized and distributed blockchain based storage network comprising various Sharder Nodes. Sharder Network will gradually reform the way people store, exchange and validate valuable data.

Sharder Node: The Sharder Hub, Box or computer that is participating in the Sharder Network.

Sharder Token (SS): The cryptocurrency embedded into the Sharder network. A total of 500 million SS are issued. The total supply will continually decrease as tokens will be burnt with transactions on mainnet. SS is a utility ERC-20 token. SS tokens are required by users to store and validate data on the network. They are also used to reward nodes for storing data, validating transactions and mining blocks.

SV: Storage & Validation

3. Design Philosophy

Business Focused: The design and development priority is based on real business scenarios.

Open for integration: Though sharder itself is one storage network, it's open to integrate other storage networks such as IPFS/Filecoin to provide additional storage services.

Imperfect Nodes Presumption: The network architecture allows single node failure and occasional downtime while the whole network remains robust and secure

Ownership & Privacy: Data is encrypted and private. A data owner has complete ownership and access to their data. No one without authorization can access data.

Quantified Contribution: All contributions to the network are quantified and observable based on measuring methods such as PoR (Proof of Replica).

Eventual Consistency: Data objects are allowed to have different states at different nodes and can rapidly converge to the entire network consistently.

Monitoring & Recovery: The entire network availability and data object states are closely monitored and could be spontaneously recovered.

Audit & Supervision: Data can be monitored and audited in specific situations with the consent of data owners.

Extendable API: User-friendly API with high extensibility.

4. Sharder Storage

Sharder has constructed a distributed storage network which provides cost-effective storage space, reliable data storage and transparent on-chain information. The Sharder Network is accessible to global public chains (such as Qtum, Ethereum), storage networks (such as IPFS, Aliyun, Baidu Cloud), and personal storage devices (such as hard disks and cloud disks). DApp's can be developed based on Sharder Network.

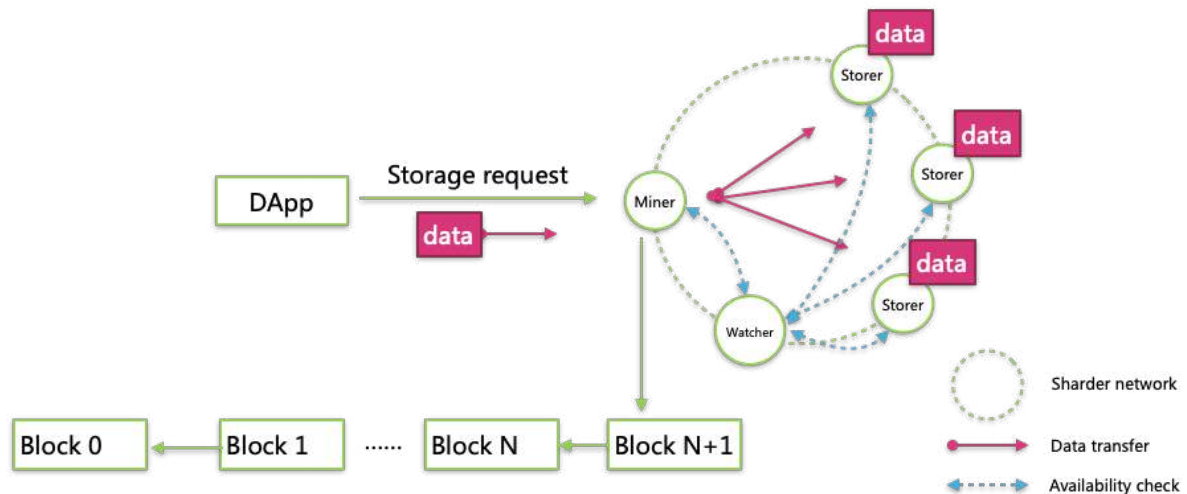
4.1 Definition of Roles

Storer: Provides disk capacity for data storage and gets rewarded in SS tokens. Storers are also subject to inspection from data owners or Watchers and provide proof of storage.

Watcher: Observes the entire network state, checks the security state according to the security strategy, and fixes existing or potential loopholes. Watchers must be constantly online. They are essential for the rapid convergence of the whole network, and perfect for data indexing.

Miner: Similar to miners in blockchain networks, miners need to run a client (terminal or GUI) to store block information and process and bundle transactions. The network's stability, connectivity and throughput rate highly rely on Miners.

The above three roles work together to fulfill storage requests on the Sharder network. See Diagram below:



The Watcher observes the entire network and maintains the status of the Storer. When storage requests are sent to a Miner, the Miner checks the status of Storer via a Watcher and assigns the data storage tasks to Storer to store the data. At the same time, a new block containing the storage request transaction is generated by Miner.

4.2 Network Topology

We have built a peer-to-peer network with a large number of nodes that can join and exit at any time. Therefore, it is critical to have a good routing table maintenance and lookup algorithm. We choose the Kademia protocol¹ (hereinafter referred to as Kad) as the basis to build a P2P peer-to-peer network. Kademia uses a "distance" calculation based on XOR between two nodes and then maintains a Distributed Hash Table based on such "distance". Such design greatly speeds up the routing search process, which is critical for the Sharder Network with numerous storage nodes.

The node list of K bucket in Kad describes the online state of nodes. The Watchers select the proper Storer nodes by checking their online state, together with the credit weight table described more in the Sharder Consensus section.

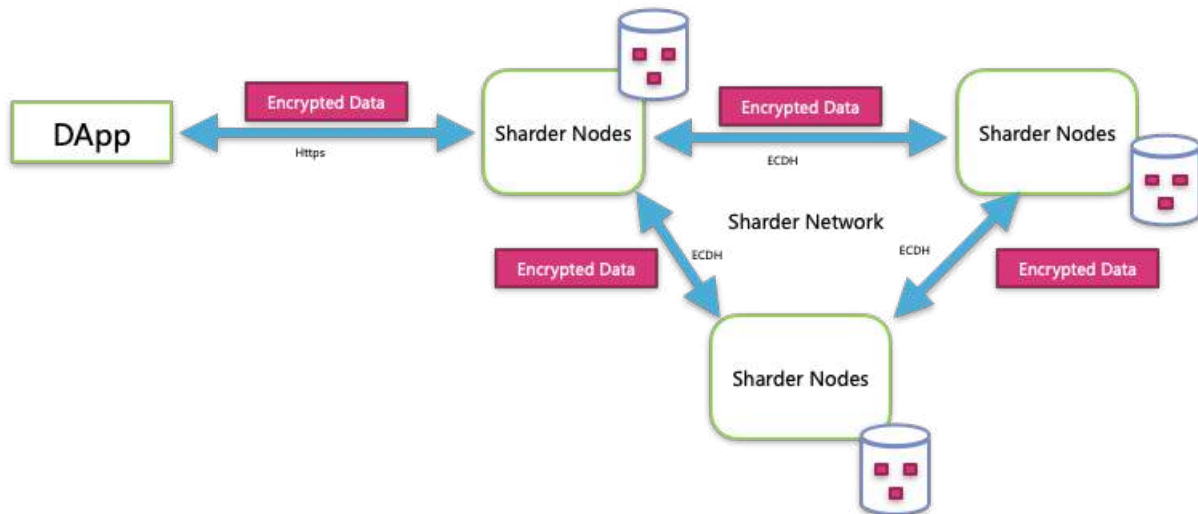
¹ "Kademlia - MIT PDOS." <https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf>

4.3 Data Security

The core elements of data security are confidentiality, integrity, and availability. Sharder leverages cryptography algorithms, data sharding and data replication technologies to ensure the data stored in Sharder network is always available to users without worrying about data destruction, modification or disclosure.

4.3.1 Data Encryption

The data is always encrypted when it's transferred via the network or stored on local storage systems. As shown in the below diagram:



When users interact with Sharder nodes via a DApp to send storage requests along with data, a secure channel is established via https, the data transferred between a DApp and Sharder nodes is always encrypted.

ECDH (Elliptic-curve Diffie–Hellman (**ECDH**) is a key agreement protocol that allows two parties, each having an elliptic-curve public–private key pair, to establish a shared secret over an insecure channel) is used between Sharder nodes to exchange data when required. Finally the data is securely saved in local storage within each Sharder node with AES-256-CTR algorithms².

4.3.2 Data Sharding

Data stored with Sharder is split into multiple shards (small fragments) via data sharding. It can then distribute the data shards to different Sharder storer nodes. When data owners require high data security, sharding is a great solution since it's more difficult for hackers to get complete data content by attacking a few servers.

² "RFC 3686 - Using Advanced Encryption Standard (AES" <https://tools.ietf.org/html/rfc3686>.

This is a big differentiation to general cloud storage solutions which usually store one data object on one or two servers without sharding. This makes the data vulnerable to hackers who could get all data content by attacking a few servers.

To ensure the availability of sharding, we introduce Erasure Code.

Erasure Code³ is a way to protect data by splitting data into pieces, expanding and numbering the redundant blocks, and storing them at different places such as hard disks, storage nodes, or other physical devices. In order to ensure data availability without taking too much storage space (increasing the utilization of Storers), the Sharder Network adopts data erasure on data shards.

4.3.3 Data Replication

The default strategy for Sharder is to create 3 replicas for each copy of data. Higher levels of security strategy requires more storage space, more complex “watching” and “adjustment”. Sharder allows data owners to define security strategies according to their own needs. The current configurable parameters are: replica quantity and shard quantity. The security strategy will directly influence how Watchers fix the issue of lost data; and will impact the convergence speed of the entire network’s data objects.

Watchers continuously adjust the data replication and distribution to ensure the current data file is secure and at least one resource is always accessible.

Assume there are b Storers in the Sharder Network, the data is split into p shards and each has n replica. The probability of successful retrieval R_s will be:

$$R_s(b, p, n) = \frac{\binom{b-p}{n-p}}{\binom{b}{n}}$$

³ "Erasure code - Wikipedia." https://en.wikipedia.org/wiki/Erasure_code.

5. Sharder Storage & Validation (SV) Network

Sharder released the closed Alpha test network in Q3 2018. SignEase is one of the crucial nodes and users. SignEase uploads signed contracts and validated files onto the Sharder chain for storage. The transaction ID of the stored data will be displayed to users on Sharder's inquiry tool. This demonstrates the traceability and immutability of all stored contracts and files to SignEase users. Based on these blockchain properties, all e-contracts and files stored and validated on SignEase are legally valid as evidence.

SignEase has been using Sharder as an independent blockchain storage network from the beginning. Every e-contract on SignEase has been stored and validated on the Sharder chain with the Sharder network providing automatic file storage and multiple backups.

SignEase gradually evolved to become less reliant on Sharder for e-contract storage. This is due to China's blockchain technology and applications developing rapidly since 2018. The Judicial Chain of the Hangzhou Internet Court, also one of SignEase's partners, began to change its method of providing storage and validation in 2019. SignEase no longer has to upload the files themselves to the Judicial Chain. SignEase is only required to upload file hashes and other key data to the chain.

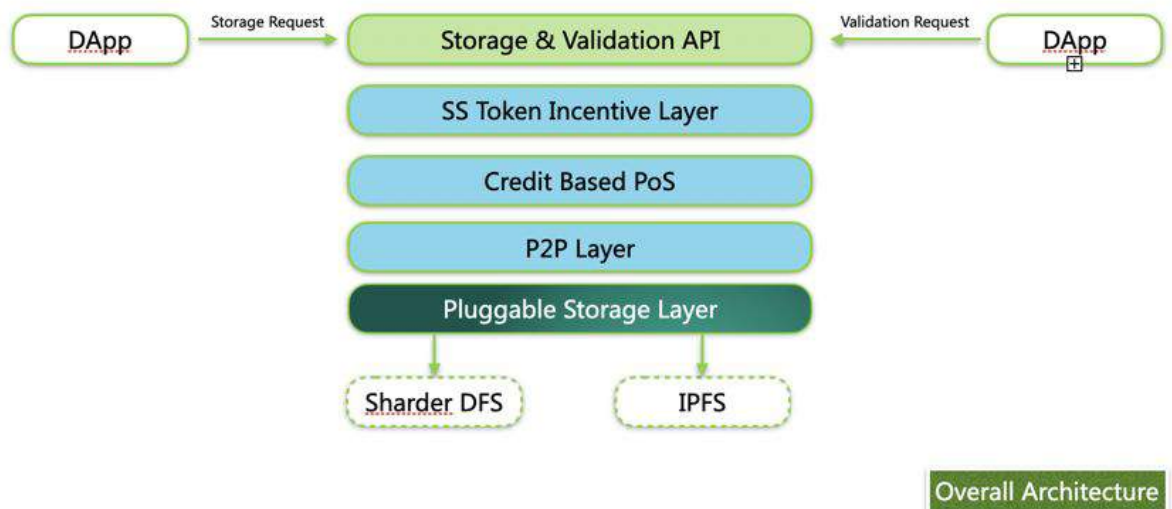
A file hash is like the file digital fingerprint. Every file will have a unique hash. Therefore, SignEase has adjusted the SV methods of e-contracts. Files are no longer stored on third party blockchain SV or blockchain storage networks and instead file hashes are stored.

The current commercial scenarios place greater emphasis on blockchain properties such as immutability, traceability, authentication, transparency and credibility. In a way, SV networks are a combination of blockchain storage and properties.

Sharder successfully released Hub nodes and set up a beta test network in Q2 2019. The released Hub nodes can already provide hash SV and authenticity capabilities without the need for external disks. On the basis of the current COS (Client Of Sharder), Sharder can provide blockchain SV, authentication, and file hash storage capabilities by adding Provers, SV and authentication transactions, and making some consensus adjustments. As a result, Sharder is now positioned as a global blockchain SV network.

5.1 Sharder Architecture

Below is the overall architecture for Sharder:



DApp's can be built on top of the Sharder Network.

Storage and Validation API:

This provides an SV service API for external applications to leverage the SV capability provided by Sharder.

SS Token Incentive Layer:

Provides SS tokens to miners to secure and maintain the stability of the Sharder Network.

The P2P Layer (Peer to Peer):

The fundamental network layer for Sharder to build a P2P network for Sharder chain. Credit Based Proof of Stake (CPOS) is the consensus mechanism for Sharder to maintain the public ledger for Sharder Chain.

Pluggable Storage Layer:

The adaptor used to interact with different storage engines. It hides the storage engine difference and provides one unified storage interface for other components to use.

Sharder's vision is to become a shared blockchain storage network with SV and authentication capabilities. That's why sharder has one pluggable storage layer in the architecture.

Sharder DFS (Distributed File System):

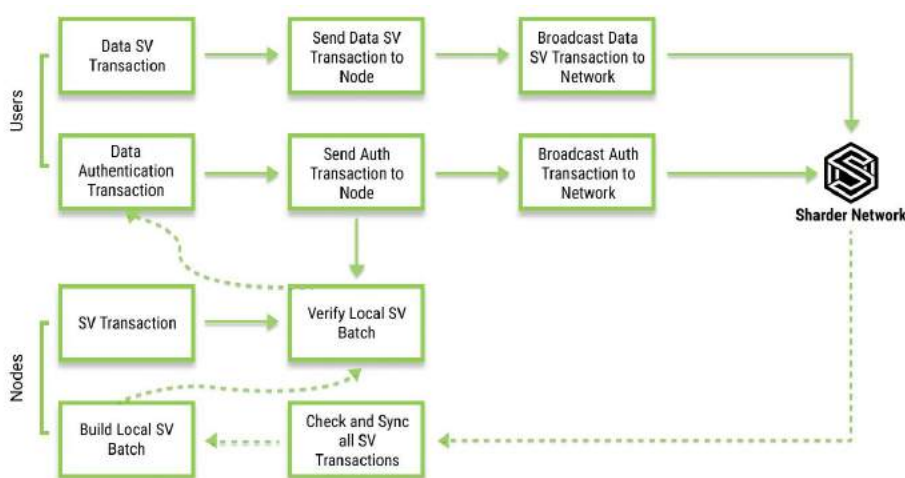
Designed by Sharder’s team and will be enabled as the default data storage system by Sharder client.

IPFS:

Integrated into the Sharder client as part of Sharder’s storage layer and could be switched to use it manually.

5.2 SV and Authentication Transaction Process

Sharder provides on-chain SV and authentication capabilities to its two native transactions (SV and authentication).



5.3 File Hash (Fingerprint)

The file hash is created from using a special algorithm on the file contents. The file hash is an effective way to determine whether a file has been tampered with. It forms the basis for Sharder’s SV and authentication capabilities.

There are two ways to calculate the file hash: md5Hex and sha256Hex. Users can calculate a file hash before uploading an SV file to the chain or they can leave it to Sharder to calculate the file hash.

5.4 SV Transactions

The essence of the SV transaction is to record the file hash onto the chain. SV transactions can be considered as a simplified file storage transaction. In order to provide Baas (Blockchain As A Service), SV and authentication transactions in Sharder occur in pairs.

The user can implement, design, or authenticate the SV files according to the data structure of the SV transaction and the algorithm of the file hash. In this case, the user does not need to use Sharder's native authentication transaction to authenticate the SV transaction.

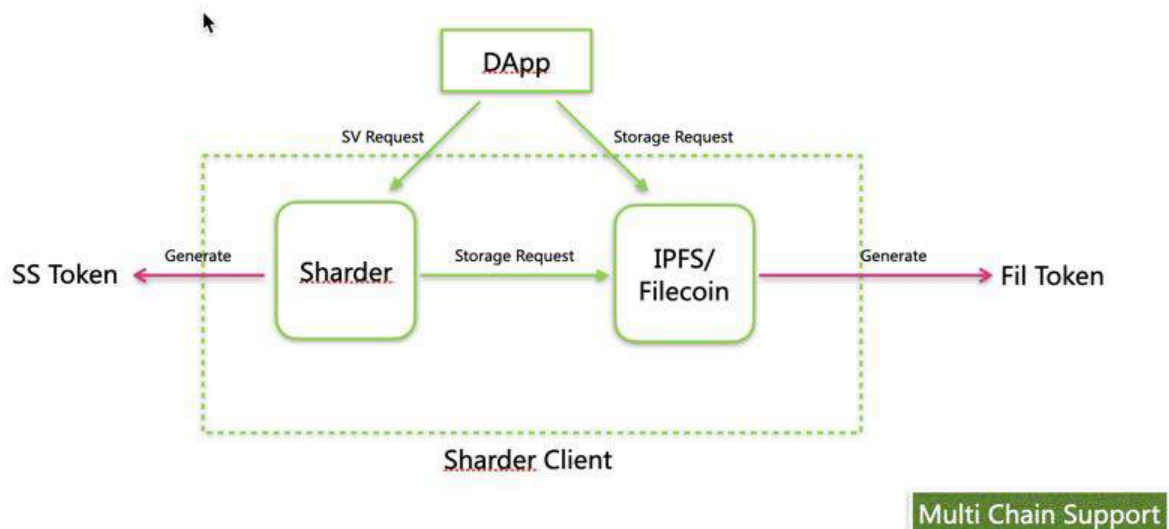
5.5 Authentication Transactions

The purpose of the authentication transaction is to verify the authenticity of the SV data on chain and to inform the user whether a document has been stored and validated on chain. Through the authentication transaction, the user can clearly know the time of upload and whether the data has been tampered with after the upload to the chain. For the storage of entire file contents using storage transactions, SHARDER can still provide authenticity verification capabilities. However, it is less efficient than using file hashes.

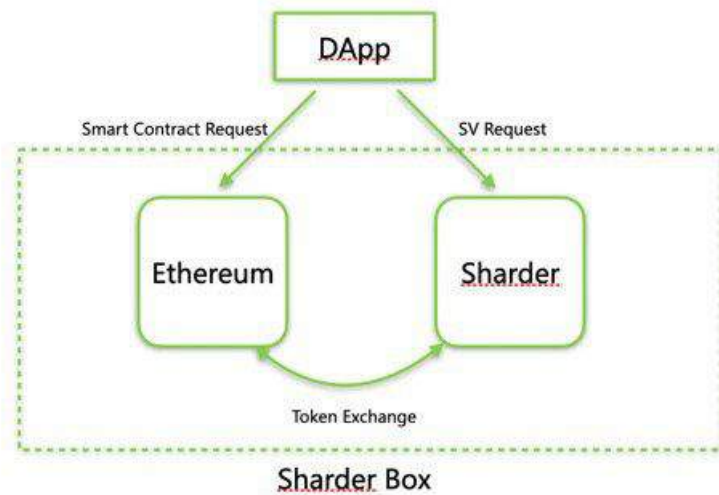
5.6 Multi-chain

Sharder is designed as a cross-chain storage network that defines the basic operations of data.

The latest version of Sharder client has already integrated IPFS storage. DApp users could seamlessly use SV service provided by Sharder and storage service provided by IPFS.



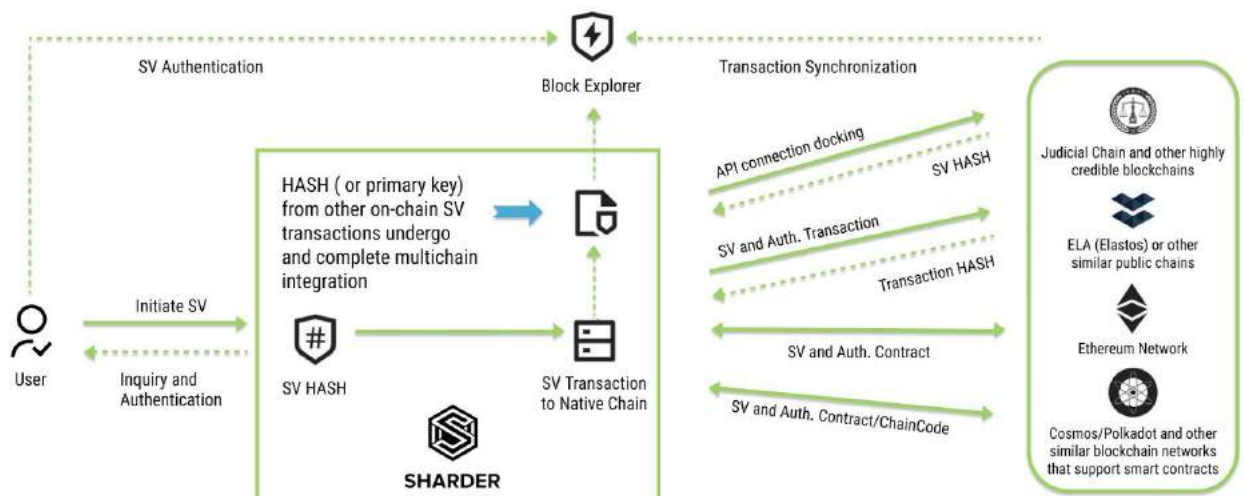
Future versions of Sharder Client will enable smart contract requests and SV requests to be made simultaneously. Like in the below diagram

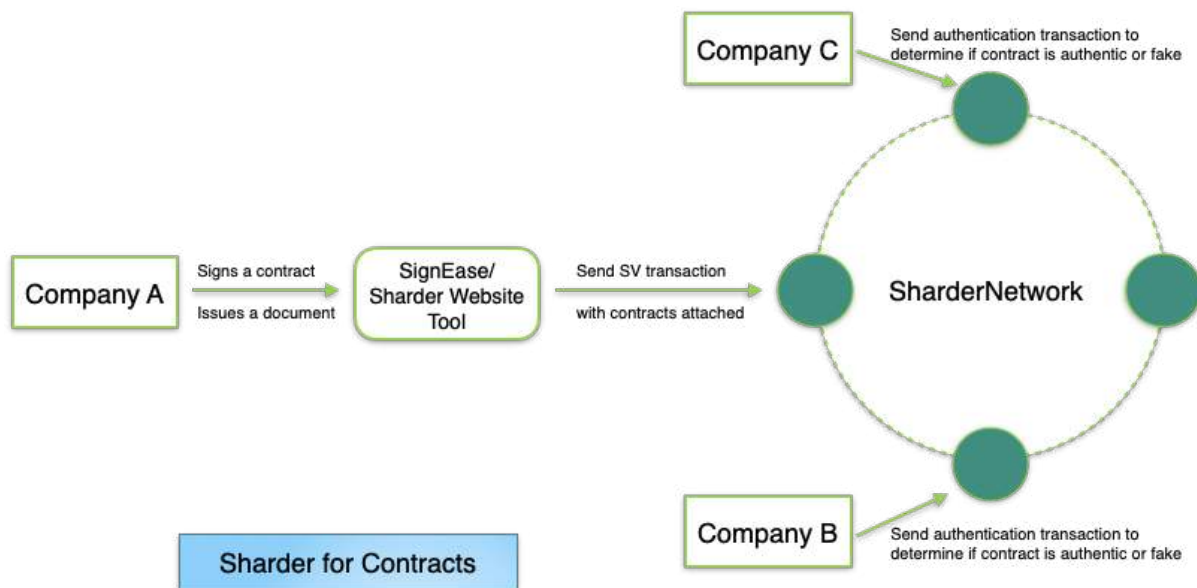


Multi Chain Support

Sharder’s ability to complete cross-chain uploads to multiple blockchains enables other chains to utilize Sharder’s SV capability. It reduces the need for other chains to build their own SV functions and also makes the cross-chain data verification possible.

The basic principle is as follows:





5.7 Blockchain as a Service

Sharder plans to use BaaS (Blockchain as a Service) to export SV, authentication, and storage capabilities externally. Customers who want to use Sharder's SV service will not need to install Sharder client or buy a Sharder Box or Hub themselves. They can use the BaaS API directly to serve their specific business case. This will greatly reduce the time and effort to get new blockchain based products to market. It's like a plug and play blockchain storage solution for business use.

Users do not have to worry about the technical details of nodes, network topology, block generation or consensus of the Sharder network. It is consistent with the API services provided by current internet service providers. The difference is the capabilities above carry blockchain properties.

5.8 User Interaction

Users need to download the Sharder client or the web client provided by the Foundation node to create an SV or authentication transaction.

SignEase users can also use SV and authentication functions from the SignEase user interface.

5.9 Document Validation & Authentication for Business

Sharder can also store and validate documents, contracts and reports utilizing blockchain technology. Doing this will guarantee that all digital files are immutable, traceable and are securely stored.

This will greatly improve the efficiency in proving the existence of original documents and ensuring that original documents have not been tampered with. Document validation and authentication can ensure issues of falsified documents are a thing of the past.

Sharder can store entire documents on its network or, alternatively, the digital fingerprint / hash of a file, as it does for SignEase.

The economic costs of fraud, in relation to document manipulation, storage and authentication cannot be understated. According to the Association of Certified Fraud Examiners, the typical organization loses 5% of its revenues to fraud each year⁴. Fraud is costing businesses and individuals across the world \$5.127 trillion each year⁵.

The key benefits Sharder offers to help reduce fraud are:

- Document immutability, traceability and security
- Quick & easy access
- Full interoperability
- Verified ownership and authenticity of documents and other digital files
- Space-saving, cost-effective and highly scalable storage

Sharder's storage validation and authentication service opens up endless business opportunities in a diverse range of industries.

Sharder is seeking interest from existing businesses and entrepreneurs to develop new applications customized for use in different industries across the globe.

⁴ ACFE 2014 Global Fraud Study <https://www.acfe.com/rtnn/docs/2014-report-to-nations.pdf>

⁵ Crowe 2019 Financial Cost of Fraud

<http://www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf>

Some examples of how and where Sharder can be used are listed below:

Industry	Who	Types of Documents	Benefit - Validation & Authentication protects multiple parties to any one document
Accounting	Accounts Payable/ Receivable	Invoices	Ensure invoices are the original & issued by the correct company
Aerospace	Aircraft Maintenance Engineers	Repair Maintenance Report	The airline, authorities, safety inspectors can verify job report is authentic
Cargo/Freight	Carrier / Receiver	Bill of Lading	All parties can verify what was delivered, when it was delivered and by who
Construction	Building / Contractor	Building Contract	Employer / client can verify job was completed according to the specifications
Education	Colleges / Universities	Diplomas / Degrees	Potential employers can verify the diploma or degree is the original
Finance	Banks	Loan Documents	Lender, borrower, courts can verify loan documents are authentic
Government	Passport Office / Department of Motor Vehicles	Passports / Drivers Licenses	Governments could issue a digital passport or license removing the need for notarized copies
Law Enforcement	Police Officer / Witness	Police Report / Witness Statement	Police reports or witness statements can never be unlawfully altered or manipulated
Medical	Doctor / Surgeon	Medical / Surgery Report	Hospital, next of kin, malpractice attorneys and courts can verify reports are the original
Oil & Gas	Maintenance Personnel	Inspection & Repair Reports	Client / contractors can verify exactly what work was completed without any risk of manipulation
Real Estate	Agents & Self Acting Agents	Sale, Lease & Rental Contracts	Ensure the original signed version of a contract has not been illegally changed or altered

Sharder's goal is to not only provide storage and validation services to its own clients, but also to partner with other blockchain storage projects such as IFPS, SIA, STORJ, GENARO and SWARM to provide them with a viable storage validation solution.

6. Sharder Account

The public and private keys of Sharder accounts are analogous to the HD wallet of Bitcoin⁶. The seed is responsible for the security of Sharder accounts and the private keys of seeds are held by users (a set of signs by BIP44 will be provided to facilitate memorization).

The Sharder account model automatically identifies the users and merges the digital assets with the account balance (without the confusing address change of Bitcoin's UTXO model). As long as the seed is securely stored, the account is safe. The key is created by an elliptic curve algorithm and the signature is implemented by EC-KCDSA⁷.

Sharder web client will also provide the ability to use mobile phone numbers & email addresses to identify accounts.

7. Sharder Consensus

To provide a fair environment for Sharder nodes to generate blocks, more stable nodes will be added to the network to promote network dispersion. Credit based Proof of Stake(CPoS) consensus is used by Sharder to maintain the network. Such consensus leverages the benefits provided by both PoS (Proof of Stake) and PoC(Proof of Credit).

Based on the CPoS consensus, the Block generation rights in the Sharder Network are determined by a node's PoC score and the amount of SS held.

7.1 Sharder Nodes

Types of Nodes in the Sharder consensus network:

Sharder Foundation Nodes : A node operated by the Sharder Foundation. Other than competing for block generation rights, it maintains the minimum amount of nodes in the network, provides guidance to nodes, and provides basic functions such as business APIs.

Community Nodes : Stable nodes approved by Sharder and the community. Nodes must be able to maintain a 99%, 24/7 uptime status and meet the following hardware

⁶ "Deterministic wallet - Bitcoin Wiki." 6 6月. 2020, https://en.bitcoin.it/wiki/Deterministic_wallet.

⁷ "KCDSA - Wikipedia." <https://en.wikipedia.org/wiki/KCDSA>。访问日期 : 3 7月. 2020。

& network configuration requirements: 3.1GHz+ Quad-core processor, 8GB+ RAM, and a 5+ Mbps internet connection with a public IP address.

Hub Nodes : A node operated from the Sharder Hub, it has the ability to create Sharder Pools. The Hub client will be run off the Hub node. The hub client will continue to be updated and will gain additional functionality to mine storage tokens such as File Coin.

Sharder Box/Hub nodes are special miners used as physical nodes and can be activated after startup. The only difference between the two is the Box node requires an independent public IP, stable bandwidth, and online time.

Box Nodes : A node operated from the Sharder Box, the Box client will be run off the Box node.

Normal Nodes : Any personal computers or servers running a node off the Sharder client will be recognized as a normal node.

In order to make the authentication and SV network work better, these Sharder nodes are subdivided as: Mining node, SV node, Authentication node, Storage node.

Different nodes will be providing different functions as follows:

Role Type	Mining	SV	Authentication	Storage
Foundation Node	✓	✓	✓	✓
Community Node	✓	✓	✓	✓
Box Node	✓	✓	✓	✓
Hub Node	✓	✓	✓	✓
Normal Node		✓	✓	✓

Mining nodes are the cornerstone of the network. In order to ensure the stability of the mining nodes, mining nodes will be required to stake SS as a security deposit. This will ensure the stability of the node and block generation in addition to the hardware and bandwidth required in accordance with the Sharder consensus. If the mining node fails to meet the basic requirements, it will be fined from the deposit.

In order to ensure that Sharder can have commercial capabilities, based off operating conditions of the test network, nodes that are already running Hubs are encouraged to switch to using public IPs if possible (otherwise mining cannot be performed normally when forking). All subsequent nodes should have a public IP, otherwise they cannot be successfully registered as valid nodes in the Sharder network.

7.2 Sharder Pool

A Sharder Pool can only be created by nodes that possess the authority to create them. Each Sharder account can stake their SS to a Sharder Pool. The amount of SS within the Sharder Pool will determine the relevant nodes' block generation rate. The block generation rewards obtained from the Sharder Pool will be distributed in accordance to the amount of SS staked from each Sharder account.

Simply put, every user can participate in mining when they stake SS to a Sharder Pool even if they don't run a node. The pool creator is the "proxy" for every participant in the pool.

7.3 CPoS weighted table

The CPoS score of nodes in the Sharder Network is calculated with the CPoS weighted table as below.

Distribution	Weighted Category	Weighted Value				
25%	<u>Node Type</u>	Sharder Node; Community Node; Box Node; Hub Node; Normal Node				
20%	<u>Role</u>	Miner; Watcher (Sharder and community nodes); Storer				
40%	<u>SS Held</u>	SS held in the Sharder account or within the Sharder Pool				
5%	<u>Hardware Config</u>	Low: 2.7GHz+ Dual-core 4 threads processor; 4GB+ DDR3 RAM; 100GB 5400RPM HDD/SSD	Midi: 3.1 GHz+ Quad-core 4 threads processor; 8GB+ DDR4 RAM; 1TB+ 5400RPM HDD/SSD	High: 3.6GHz+ Octa-core 8 threads processor; 16GB+ DDR4 RAM; 10TB+ 7200+RPM HDD/SSD		
5%	<u>Network Config</u>	Very Low: Non-Public IP	Low: Public IP, 1-5Mbps	Midi: Public IP, 5-10Mbps	High: Public IP, 10+Mbps	
5%	<u>Tx Processing Performance</u>	Low 100-300 TPS	Mid 500-1000 TPS	High 1000+ TPS		
	<u>Amount of Loss Blocks</u>	Zero	Low: 1 block/month Less than 3 accumulated lost blocks	Med: Less than 3 blocks/week Less than 10 accumulated lost blocks	High: 3+ blocks/week 10+ accumulated lost blocks	
	<u>Fork Convergence Speed</u>	Hard Fork	Slow: Over 10 blocks	Medium: Less than 5 blocks	Fast: Less than 2 blocks	
	<u>Uptime</u>	99.99%; 8751.24 hours/year 167.832 hours/week	99%; 8672.4 hours/year 166.32 hours/week	97%; 8497.2 hours/year 162.96 hours/week	90%; 7257.6 hours/year 151.2 hours/week	

Node Type: The Sharder Node is deployed by the Sharder Foundation. It maintains the minimum amount of nodes necessary and provides stable online services. Community nodes are deployed by Sharder community members. Hub and Box

nodes are operated by a person or the team after purchasing a Hub or Box. Normal nodes are personal computers or servers running a Sharder client.

Uptime: Sharder nodes are required to achieve a 99.99% online status. Community nodes are required to achieve a 99.00% online status. Hub and Box nodes are required to achieve a 97.00% online status. Normal nodes are required to achieve a 90.00% online status.

Hardware Configuration: The Sharder client will automatically obtain and rate a system's hardware configuration.

Network Configuration: Networks with a public IP will be categorized into 3 classes.

Transaction Processing Performance: When the Sharder node and community node connect online, they will be tested on their performance while they're being validated and will be rated based on their test results. After they're connected, they will undergo periodic performance evaluations (at present, timeframe is set to quarterly) and their ratings will be adjusted accordingly.

Amount of Loss Blocks: The amount of loss blocks will increase by 1 if a miner fails to generate a block at its scheduled block generation time.

Fork Convergence Speed: The nodes in the fork will automatically report the amount and duration of blocks that are: currently in the fork and blocks that will eventually return to the main chain.

SS Held: There are no limits to solo-mine on a single account. At present, each mining pool will be able to hold a minimum of 20,000 SS and a maximum of 300,000 SS.

8. Tokenomics

SS is Sharder's native utility token. SS holders get access to Sharders storage and validation network.

SS tokens are used to pay for storage and validation services. SS tokens are also used for rewarding miners for storing data and validating transactions.

When external business applications or individuals / enterprises use Sharder's services they must first purchase SS from the free market to pay the relevant fees for the services used.

Demand for SS tokens will increase as more data is stored on the network and more SV transactions are completed.

8.1 Token Type:

SS tokens are and will remain an ERC-20 Token. This makes it easier for SS to circulate in the market, be safely stored and traded.

Following the release of Sharder's mainnet, SS tokens will be differentiated as SS & SS-M (mainnet). The tokens are interchangeable for each other and the total token supply does not change.

SS will refer to the circulating SS tokens (ERC-20) which can be stored in commercially available wallets or traded on cryptocurrency exchanges.

SS-M (Mainnet) will refer to tokens which have a functional role within the Sharder network, such as paying storage fees and system rewards.

In COS V2.0 there will be an automatic exchange function for SS (ERC-20) and SS-M (Mainnet).

< Tokens are Interchangeable >	
SS (ERC-20)	SS-M (Mainnet)
* Storing in wallets	* Paying storage fees
* Trading on exchanges	* System rewards

Total Supply: 500 million

8.2 Total Supply

500 million.

8.3 Burning / Reduction of Supply

The total supply of SS tokens will continually reduce as 10% of fees from all storage and validation transactions will be burnt.

8.4 Storage Costs & Transaction Fees

Fees will be paid by the storer / initiator.

All fees are paid in SS Tokens, USD value is converted to SS at the time of the transaction.

Storage: 0.01 per GB per month

Upload Bandwidth: \$0.04 per GB per month

Download Bandwidth: Free

Storage Validation Transaction: 10 SS per Transaction

Box Node Creation Transaction: 50,000 (100% burnt)

8.5 Fee distribution

Storage fees are split amongst the storer / validator, Sharder Foundation and being burnt.

Storer / Validator: 75%

Sharder Foundation: 15%

Burnt: 10% (except box node creation transaction will be 100% burnt)

For data storage, the storage rewards are based on the stored replications of the data / shards. If there were the standard 3 replications. The 1st replication storers would receive 70% of the reward. The 2nd & 3rd replication storers would both receive 15% of the reward.

8.6 Sharder Pool Staking Limits

Pool creators can set the earnings distribution ratio, creators can earn a maximum of 30% pool earnings.

Minimum Stake: 20,000 SS

Maximum Stake: 300,000 SS

8.7. System / mining rewards

Sharder relies on a Credit based Proof of Stake (CPOS) consensus to determine who stores and validates data / block generation. A smaller number of nodes that are discrete and reliable is the best solution to create a higher consensus efficiency, stronger fault tolerance, higher transactions per second, and a lower probability of block errors and rollbacks.

Sharder will not follow the Bitcoin networks method of attracting nodes (miners) to join the network by rewarding solely on mining. Most of the Sharder nodes will be rewarded for providing SV, authentication and storage capabilities.

Users of Sharder must pay for these services just as we use the Ethereum network's smart contract to pay the Ether Fee and use the Bitcoin networks transfer function to pay the BTC fees to the nodes (miners).

A total of 100 million SS were reserved for system rewards. Of that:

- 11,470,568 SS tokens were awarded during the initial testing phase.
- 88,529,432 SS tokens remain for system rewards.

The system reward allocation will be reduced from the V.1 Whitepaper which was distributed over a 10 year period. Specific details will be released following the completion of the test network in Q3 2020.

9. Applications

Sharder encourages businesses and entrepreneurs to build innovative storage applications on the Sharder network.

9.1 SignEase

SignEase is an electronic signature application part owned by Sharder.

SignEase is connected to the Hangzhou Internet Court's Judicial Chain. The on-chain authentication is recognized by the courts and can be used as judicial evidence for possible litigation disputes.

SignEase uses Sharder's Network for storage and validation of file hashes.

9.2 ISLAND

ISLAND is a blockchain based storage application for sensitive photos, videos, documents and notes.

Sharder has been commissioned by a 3rd party to develop the application.

Sensitive data no longer needs to be stored in a phones gallery or files. Data can be uploaded to Sharder's storage network making it safe from unauthorized access. Data can be easily downloaded back into ISLAND whenever the user requires access to it.

ISLAND will be available in the App Store and Google Play in Q4.

Island will pay for the storage of all its users data and upload bandwidth with SS tokens purchased at market rates from exchanges.

10. Road Map

See [Sharder.org/#/road-map](https://sharder.org/#/road-map)