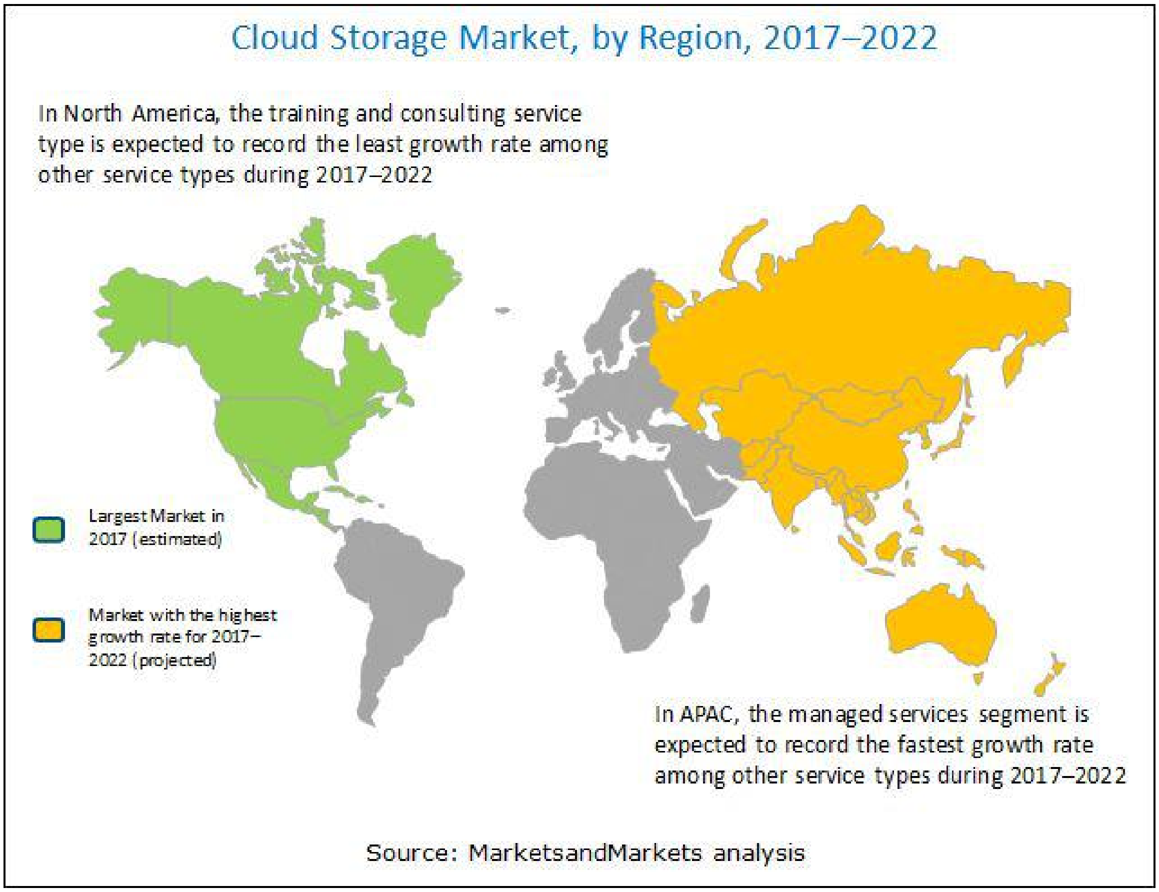
Spock Chain——A Decentralized Storage Application Platform

Table of contets

1. Abstract

According to the latest report from MarketsandMarkets, the global cloud storage market is expected to rise from $23.4 billion in 2016 to $88.9 billion, with a compound annual growth rate of 23.7%. The demand for cloud storage is driven by many factors, such as the increasing popularity of artificial intelligence, IoT, and VR/AR. Cloud data storage has become the infrastructure of many new technology services, especially with the advent of 5G. Accelerate the explosion of cloud storage needs. With the availability of cloud storage solutions and services, the need to maintain local storage infrastructure such as disk storage and tape devices has been eliminated.

The North American market is expected to remain the largest in 2017-2022, while the Asia Pacific region (APAC) is expected to grow at the highest compound annual growth rate during the forecast period of the cloud storage market. The growing demand for efficient computing frameworks and the shifting of workloads to the cloud environment is said to be driving the demand for cloud storage globally. The growing popularity of organizations turning to cloud solutions and services and digital business strategies is a major factor expected to drive adoption of North American cloud storage
products.


Cloud Storage Market, by Region, 2017–2022

In North America, the training and consulting service type is expected to record the least growth rate among other service types during 2017–2022

🟩 Largest Market in 2017 (estimated)
🟨 Market with the highest growth rate for 2017–2022 (projected)

In APAC, the managed services segment is expected to record the fastest growth rate among other service types during 2017–2022

Source: MarketsandMarkets analysis

However, nowadays centralized private services are being replaced by decentralized open services, and trusted centers are being replaced by verifiable computing, precisely because traditional centralized data services face the following challenges: (a) hosting and distribution Data at the PB level is costly. (b) Privacy data disclosure and abuse. (c) Big data calculation across organizations.

This article describes the Spock Network, a decentralized data storage network designed to address these issues. Spock Network combines the experience and lessons of many previous systems and carefully designs an implementation path that can ultimately lead to a large-scale decentralized storage network.

2. Introduction

Spock Network is a decentralized storage platform. In the early stage, Spock Network mainly stores Proof of Capacity (POC) consensus data to effectively utilize the most suitable decentralization technology to encourage miners providing hard disk space. At the same time, on this basis, the support of smart contracts has also been added to support decentralized applications and POC-type tokens. In the future, the data stored in the Spock Network will support documents in any format such as documents, videos, and images, and truly fulfill the ideal of making block chain technology beneficial to everyone.

Spock is the leading charactor in the American classic sci-fi series Star Trek. This character represents rationality, justice, and the courage to explore the unknown. We chose Spock as the project name to encourage the team's keep exploration of the new possibilities of the blockchain.

2.1 Proof of Capacity (POC)

Bitcoin is a successful decentralized asset network. However, with the development of the Asics chip mining machine, it has gradually moved away from the original intention of Nakamoto to hope one-cpu-one-vote in the Bitcoin white paper, and at the same time, on the power resources. Huge consumption is also a problem that has been criticized for a long time.

Burst launched its own main network for this problem in 2014. It proposed Proof of Capacity (also known as Proof of Space) consensus algorithm to replace Bitcoin's Proof of Work consensus, making the mining process extremely Save on the dependence on power resources.

In addition to improving the mining POC consensus algorithm, Spock Network will introduce a better economic model to encourage miners to join the mining queue, and will also build a Solidity-based Turing-complete scripting language to support intelligence. Contracts, decentralized applications and other ecological construction, but also support developers to use the existing consensus "computing power" to build their own POC block chain.

As we all know, Proof of Works (POW) is introduced by Nakamoto in the Bitcoin system as a solution to the "double payment" problem. Its core algorithm is for a value α, a random prediction function H, if we wish The hash value H(a) satisfies the previous t-bits being 0, so it takes 2^t times of hash calculation to find the alpha value. The core value of the POW is that all the people follow this verification rule, except for the execution. With so many hash calculations, no one can speed up the calculation process. All miners can only perform so many operations honestly to find the proper nonce value. The miners who find the first one can be responsible for the next block write. And get rewards at the same time. So in order to complete these Hash calculations faster, the miners experienced a transition from CPU, GPU to Asics chip mining. Because a lot of calculations require a lot of power, for large-scale POW networks like Bitcoin. Even being criticized for destroying the ecological environment, at the same time, for the eliminated Asics chip mining machines, they can only be treated as garbage, because they can't do anything except mining.

Proof of Capacity (POC) is also called Proof of Space. Its basic idea is to put the calculation in the initialization stage, that is, write the result of the hash calculation to the hard disk in advance, and retrieve the data in the hard disk during the execution phase. To reduce the POW algorithm, a lot of hash calculations are needed, and only a small amount of hash calculations are used in the execution phase. In this way, the entire network has been improved in the following aspects:

- Environmental protection: When a mining machine is initialized, the mining cost is relatively small, requiring only a small amount of disk access and a small amount of calculations per block.
- Economy: Many PCs have unused disk space. The marginal cost of using these spaces for mining is small, with immediate rewards and can be used for mining. It is not necessary to consider the cost of electricity as a bitcoin mining machine.
- Equality: Today Bitcoin has become the world of Asics mining machines and large mines, and small-scale investors have struggled to participate in the bitcoin mining ecology, while POC-based mining machines are hardly faced with bitcoin-like The mining machine is constantly updating its iterations so that it is completely eliminated.
- “computing power” sharing: BCH is a BTC hard fork chain, so BTC's proprietary mining machine can also dig BCH, but it can't dig BTC and BCH at the same time, and the POC mechanism can make the hard disk for different chains. The spatial "computing power" data structure is consistent, and these "computing power" can be used to dig assets on these chains at the same time.

At the same time, in order to better build the ecology of the Spock Network, we will refer to some features of the Proof of Stake (POS) consensus and introduce the Staking mechanism into the consensus algorithm. The miner needs to hold a certain amount of tokens to mine. Details See Section 4.

2.2 Decentralized storage network (DSN)

In a DSN network, files are fragmented, copied, and uploaded to several nodes, and the corresponding data is maintained through a distributed hash table. Customers store and retrieve money by paying for network fees, and miners provide disk space and bandwidth to get rewards.

2.2.1 Distributed hash table (DHT)

A distributed hash table (DHT) is a type of distributed computing system used to distribute a set of keys to all nodes in a distributed system. The nodes here are similar to the storage locations in the hash table. Distributed hash tables are usually for systems with a large number of nodes, and the nodes of the system often join or leave.

2.2.2 Kademlia algorithm

Kademlia is a protocol algorithm for DHT, designed by Petar and David for P2P networks in 2002. Kademlia specifies the structure of the network and also defines the way in which information is exchanged through node queries.

3. Core technology

3.1 POC consensus algorithm

The POC consensus algorithm was first proposed by Stefan Dziembowski in 2013. Burst-coin was the first blockchain project based on the POC consensus algorithm. At the same time, Burst-coin completed the POC2 consensus upgrade in 2018, making POC Network is safer.

3.1.1 Terminology

In blockchain systems with POC consensus, some terms are similar to, but not identical to, POW mining systems. For ease of understanding, we have some of the main terms that need to be highlighted below.

- Shabal/Sha256/Curve25519

  Shabal,Sha256, Curve25519 Is the cryptographic hash function used in the Spock Network, Shabal is the main function used, Shabal is not a highly efficient cryptographic hash function, but since our hash calculation mainly occurs in the plot phase, it is needed for our runtime. It is enough for the verification work. We mainly use its 256-byte version, which is Shabal256.

- Hash Value

  The hash value represents the result of a cryptographic hash function. If not specified, the hash value mentioned in this article is generally 32 bytes.

- Plot File

  When mining, the mining program will read the pre-calculated hash value from the disk. These values are stored in the file on the disk. These files are Plot files.

- Nonce

  In a plot file, there are several groups of nones, a nonce contains 8192 hashes, so a nonce has a size of 256K bytes. Each nonce has an independent number of 8 bytes. The number range is 0-18446744073709551615 (2^64).

- Scoop

  The 8192 hashes contained in each nonce are placed in 4096 different places, and 2 hashes are placed in each scoop.

- Account ID

  When creating a plot file, this file is associated with the miner's digital account Account ID. This ID will be used to create a nonce. The different minins created by different miners are not the same, although the nonce numbers they use may be the same.

- Deadline

  Deadline is the value used by different miners in the mining process to compete with each other. This value is calculated based on the nonce on the plot file. When this value is submitted to the wallet, and the wallet is not received in the deadline time (seconds) Blocking broadcasts from other nodes in the network will be packaged.

- Block Reward

  When a miner is responsible for packing a block, he can get a block reward.

- Base Target

  Base target is calculated based on the block out of the past 24 blocks. This value is used to adjust the difficulty of mining. The smaller the value, the harder it is for the miner to find a small timeline.

- Network Difficulty

  This value is equivalent to the total hard disk space used for mining in the current network, in units of Terabytes.

- Block Generator

  When a new block is packaged, the account that needs to be packaged is the block generator. That is to find the account corresponding to the nonce used by the deadline.

- Generation Signature

  The generation signature is based on the generation signature and block generator of the previous block. This value is used to pack a block with a length of 32 bytes.

- Block Signature

  Block signature is created by the block generator when packing the block. It is the signature of most of the data in the block and the private key of the block generator after Sha256 and Curve25519 hash calculation. The length is 64 bytes.

- Solo/Pool Mining

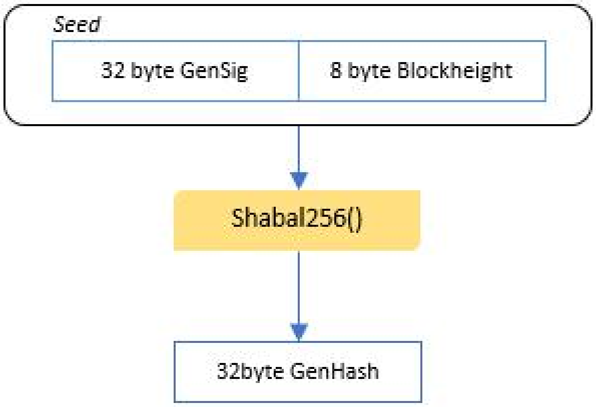
  Solo mining and mining pool mining, solo mining is the result of the miners submitting direct competition with the results of other independent miners and pools in the entire network, when winning, all block rewards. Mining pool mining is the result of submitting the results to the mining pool. After the mining pool has harvested the minimum deadline values obtained by other miners in the mining pool, it compares with the results submitted by other independent miners and pools in the network. If it wins, the mining pool will be fairly distributed to the miners involved in mining according to their own distribution mechanism.

- Reward distribution

The distribution is mainly for mine mining. When the miners set up the reward distribution as the mine pool, the miners are equivalent to inform the network mine pool to take over the miners' block rewards, that is, when the original block rewards, they are assigned to the miners. The account that is now assigned to the pool, and if the deadline is received from the miners, the pool is responsible for packing the blocks.

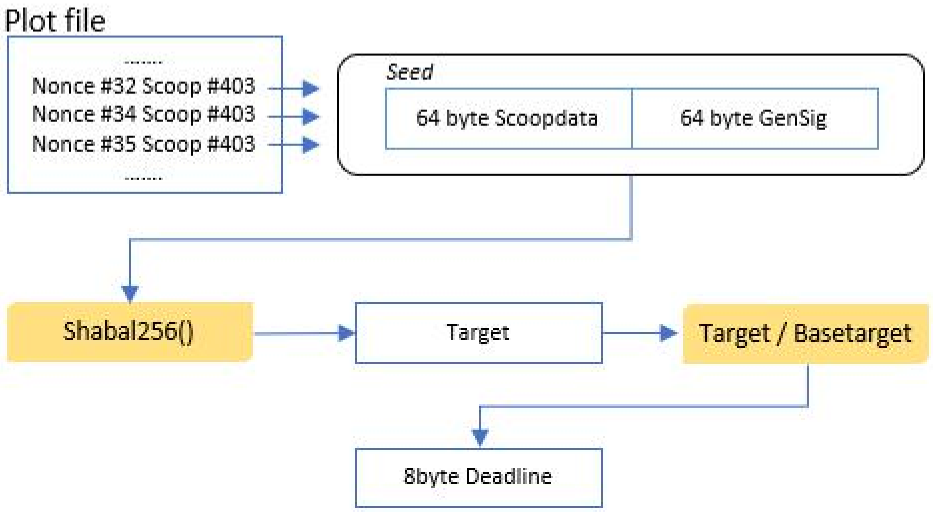
3.1.2 Mining process

When mining begins, the mining program will obtain mining information from the wallet, such as generation signature, base target and the next block height, where the generation signature is generated by the wallet program on the previous generation signature and the previous block. The miners Id are combined and generated by Shabal256 calculation. The mining program combines the generation signature and the block height as a seed for Shabal256 to get a generation hash.



Next, the mining program will take the value of the generation hash value 4096 to calculate which scoop data to use.

Then the mining program will read the data of the scoop corresponding to all nonce, scoop data and generation signature as the seed to get a new target value, then divide the target value by the base target and take the first 8 bytes as the deadline value.



The mining program will select a minimum value from all calculated deadline values. If the value has a meaning worth submitting (if the value is too large, it is not necessary to submit the result, because it will not be accepted), submit The information contains the miner ID associated with the plot file, and the nonce value corresponding to the optimal deadline found by the current scoop data.

3.1.3 Packaging process

After receiving and verifying the information submitted by the mining program, the wallet program (or the mine pool program) will observe whether the valid block broadcast by other miners on the network is received within the time (in seconds) of the deadline. , the wallet will abandon the packaging block, otherwise the wallet will use the current deadline information to pack the block.

Each block can contain up to 255 transaction information and up to 44880 bytes of payload data. The wallet program will put the unconfirmed transaction information into the block being packaged as much as possible. For each transaction that needs to be packaged, the wallet program will verify the signature, timestamp and other information, and the verification will be put in. In the block. The block information only contains the Transaction ID of the packaged transaction. The details of each transaction, such as the number of transactions, the handling fee, etc., are stored separately.

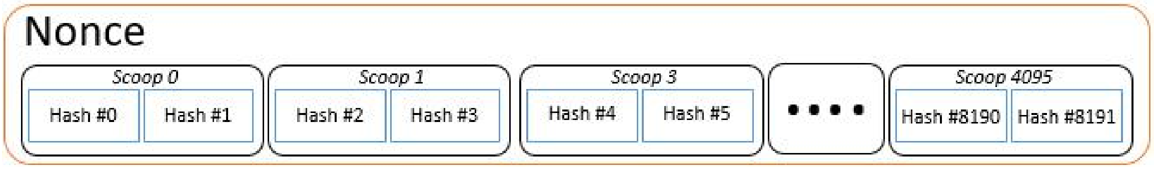
3.1.4 Nonce Generation

As we mentioned earlier, the nonce of the POW is calculated by performing a random prediction function. The POC processes the nonce value and stores it on the hard disk. The size of each nonce is 256K bytes, and 8192 hashes. Value composition.

The first step in creating a nonce is to create a seed. The first seed is a 16-byte long value consisting of a miner ID and a nonce number. We get the first hash value through Shabal256, and we put this value first. Before the seed, form a second seed, and then get the second hash value through the Shabal256 function, then put the value before the previous seed, form a third seed, and so on to produce 8192 hash values. (When the stitched seed exceeds 4096 bytes, the first 4096 bytes are selected as the seed). Finally, we stitch all the 8192 hashes and the initial 16 bytes as the final seed, and get a SHAB256. The final hash value. The pseudo code of the above process is as follows：

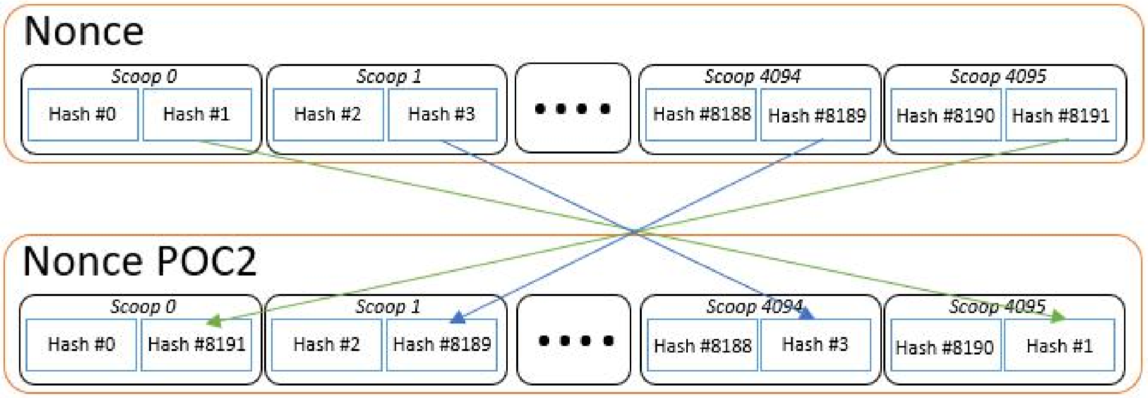
```
seed= account_id+ nonce_id //8 bytes + 8 bytes
for(i = 0; i < 4096; ++i){
    hash = Shabal256(first 4096 bytes of seed)
    seed = hash + seed;
}

final_hash = Shabal256(seed);
```

This hash value is XORed with the above 8192 hash values to get a total of 8192 new hash values. This set of hash values is the contents of the plot file we write to disk.



3.1.5 POC2

The nonce generation mentioned in 2.1.4 is based on POC1.0, but it has a fairness problem: since a generated hash value is sequentially stored in the scoop, for some "cheating" miners, It can generate no more than 8192 hashes, but only one hash value, and the remaining 8191 hashes can be calculated when the deadline calculation is needed. Thus, the miner needs 256K bytes of space. Data, only 32 bytes is enough. This problem is not a serious security hole, because these "cheating" miners only use the characteristics of the data structure to save space, and failed to change the rules of packing blocks and verifying blocks. Based on this, POC2.0 was proposed to solve such a problem, mainly by adjusting the hash values stored in the order of scoop in the order, and the adjustment rules are as follows：



In the Spock Network, we will use POC2 as a consensus algorithm, and POC1 is not supported.

3.2 Blockchain system based on state transition

Like Ethereum, the Spock Network is a state transition system that enables anyone to create smart contracts and decentralized applications by creating a system of ultimate abstraction and a built-in Turing-complete programming language.

3.2.1 Accounts

In the Spock Network, the state consists of the transfer of values and information state transitions between the object of the account and the two accounts. The account contains the following sections:

- Random number, a counter used to determine that each transaction can only be processed once
- Current token of the account
- The contract code of the account
- Account storage
- Identification number of the account

3.3 Virtual Machine

The virtual machine environment is a function required by any blockchain project that supports the scripting language. In order to develop the developer ecosystem better and faster, Virtual Machine will support the Solidity language, making the existing Solidity developers almost unnecessary. Development can be introduced into the Spock Network.

3.4 Smart Contract Security Check

Smart contracts on Ethereum often reveal endless security vulnerabilities. When deploying smart contracts, Spock Network will detect smart contract vulnerabilities through intelligent detection platforms, so that the corresponding smart contracts can bring some security to make sure potential dangers are killed in the cradle.

4. Issuance

SPOK is the name of the basic circulation unit within the Spock ecosystem and is the only commercial and financial delivery deadline. In addition to recording account balances and payments, SPOK can also be applied to smart contracts within the system.

4.1 Basic information

Total Supply	4,200,000,000
Consensus	POC
Hash Algorithm	Shabal256
Block Header Size	8MB
Block Interval	180 seconds

Initial Single Block Reward	1800
Reduction Period	133440
Reduction Percentage	1%

4.2 Issuance

SPOK has a total of 4.2 billion, consisting of 8% of open pre-mined and 92% of POC+POS mining mechanism.

4.3 POC+POS

The issuance mechanism is realized through the consensus mining of POC+POS. It is divided into three stages, which are named as the origin stage, the ecological development stage, and the ecological maturity stage.

4.3.1 POS mechanism (2001-infinite block)

When a miner packs a block, if its address balance satisfies the amount of mortgaged block, then all proceeds can be earned. Otherwise, the miner's revenue = block reward / miner needs Staking * miner's actual Staking.

The miner needs the amount of Staking = the miner is assessed the manpower * F(x), x is equal to the current total network computing power.

F(x) = 1200 – (power (P) / 10 – 1) * 8.

When the miner does not meet the full Staking requirements on the chain, the less harvested coins will be destroyed.

4.3.2 Original Stage(Block 0-2000)：

All award awards for all blocks are obtained by miners. After the origin number, the POS phase will start.

4.3.3 Ecological Development Stage (Block 2001-174720)

During this period, the entire network will be given PoC ecological mining and ecosystem construction based on smart contract.

4.3.4 Ecological Maturity Stage (Block 174720)

During this period, the Dapp and developer ecology of the whole network has developed better. The community voted on the chain to determine the distribution of community governance bonus pool and the subsequent ecological development.

4.4 Goverance

Spock is the first public chain to support Solidity Smart Contracts with POC consensus. With the support of smart contracts, community governance will be more in line with the block chain spirit.

As a highly community-autonomous block chain project, community governance will be conducted by way of currency holders' voting. Members of the community will vote through smart contracts to determine project function expansion and use of community governance bonus pools.

Whenever an issue needs to be discussed, community members can initiate a smart contract vote and broadcast it through the community. The holder of the currency can sign the vote and submit the vote through the wallet program, when more than 60% of the currency is held. When the number of users is reached, the community developer will follow the community decision to upgrade the system.

The launch and voting of the issue will be placed in the smart contract and anyone can see the result of the vote through explorer.

5. Technology Roadmap

In the technical roadmap, we use the famous episodes of Star Trek as the stage name to inspire us to explore the unknown bravely.

Stage	Time	Content
Origin	Q4, 2018	Technical research, project preparation
Next Generation	July,2019	Testnet release
Voyager	August,2019	Mainnet release, mining pool release
Enterprise	Q4,2019	Smart contract support release
Discovery	Q1,2020	Expand developer ecology
Deep Space Nine	Q2-Q4,2020	Storage layer protocol consensus upgrade, support multiple files
The Undiscovered Country	2021	Build a decentralized storage data application network

6. Reference

1. Dziembowski S., Faust S., Kolmogorov V., Pietrzak K. (2015) Proofs of Space. In: Gennaro R., Robshaw M. (eds) Advances in Cryptology -- CRYPTO 2015. CRYPTO 2015. Lecture Notes in Computer Science, vol 9216. Springer, Berlin, Heidelberg. https://eprint.iacr.org/2013/796.pdf
2. Park, S., Pietrzak, K., Kwon, A., Alwen, J., Fuchsbauer, G., Gaži, P.: Spacemint: A cryptocurrency based on proofs of space. Cryptology ePrint Archive, Report 2015/528 (2015). http://eprint.iacr.org/2015/528
3. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
4. Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper (2014b)
5. Burst wiki https://burstwiki.org
6. Burst blog https://www.burstcoin.ist

7. Appendix

This white paper is a conceptual document [white paper] elaborated by the SpockChain project. It is not a sale or solicitation of shares, securities or other regulated products of the company involved in the tender. This document may be modified or replaced at any time, however, we have no obligation to update this version of the white paper or provide access to additional information for readers.

Legal Notice

SPOCK Token ("SPOCK Tokens") is sold only as a medium of exchange for specific people or participants, nor is it a prospectus or offer document of any kind, nor is it intended to constitute any form of securities offer or business. An entity in a trust, a unit in a collective investment plan, or any other form of investment, or an offer of any form of investment in any jurisdiction. No regulatory body reviews or approves any of the information listed in this white paper. This white paper has not been registered with any regulatory body in any jurisdiction. By accessing and/or accepting any information in this white paper or part thereof (as the case may be), by default you are:

(a) You are not in the territory of the Chinese Republic, nor are you a public or a resident of the Chinese Republic (tax or otherwise), or reside in the territory of the Chinese Republic;

(b) You are not in the United States of America, nor are you a public, resident (tax or other) or green card holder of the United States of America, or reside in the United States;

(c) You are not in a jurisdiction, in whole or in part, that prohibits, restricts or authorizes the sale of tokens in any form or manner, in accordance with the laws, regulatory requirements or rules in your area;

(d) You agree to meet the conditions and restrictions described above.

Risk warning

This information does not represent investment advice, or permission to sell, and directs and attracts any purchases.