Athena Network: A New Approach to Decentralized Storage Systems

Miłosz Tomiński

MiloszTominski@gmx.com

February 2023 - Poland – Katowice & Estonia – Tallinn

Legal disclaimer

This public document is not financial advice, and no party associated with the project assumes responsibility for losses or actions taken within or outside of the Athena Cloud. Investing in decentralized projects, especially cryptocurrencies carries significant risk due to their volatile and decentralized nature. Thorough research, staying up-to-date with industry developments, and evaluating potential projects is essential. It's important to consider your financial situation and risk tolerance before making any investment decisions. Nothing in this document is a guarantee that Athena will look, work, or be considered as described below. This document is only a description of the idea and project. Note that this document can be updated in the future.

I Abstract

The release of the Bitcoin whitepaper by the enigmatic Satoshi Nakamoto in 2008 marked a significant turning point in the world of decentralized technology. Since then, blockchain technology has been adopted by an ever-growing number of industries and individuals, leading to rising demand for secure and reliable storage solutions. While the potential of decentralized private spaces related to blockchain technology has been recognized for some time, there has been a notable gap between conceptualization and practical application. Athena has been developed to bridge this gap and strike a perfect balance between reliability and performance. At its core, Athena is a platform designed to offer a secure and decentralized solution for storing data in the digital world. This public document serves as a provider of a detailed explanation of the technology behind Athena, as well as an overview of the project's long-term plans for contributing to the growing global adoption of cryptocurrencies.

II Introduction

Athena is a decentralized cloud system that has been meticulously designed to offer maximum security and reliability, while also delivering high network throughput performance. The platform leverages an external peer-to-peer network, which allows it to operate independently of the payment processing blockchain (initially built on Ethereum, but with plans to expand to other platforms shortly). This careful approach eliminates the need for trust in the reliability of the payment processors, setting it apart from other solutions that rely on centralized authorities. To ensure top-notch security and privacy for its users, the Athena software relies on AES (Advanced Encryption Standard) key-based encryption and data compression. These measures ensure that all files stored on the platform are protected and can only be accessed by authorized users. Furthermore, the high-performance capabilities of the platform ensure that users can access their files with ease and efficiency, regardless of their location or device. Athena is an excellent alternative to centralized cloud solutions that come with inherent limitations and risks. The platform offers a decentralized approach to cloud storage that provides greater security, privacy, and flexibility. With a user-focused approach and a commitment to meeting the needs of the worldwide public, Athena is rapidly emerging as a

serious competitor in the cloud storage space. Whether you are an individual, a small business owner, or a large enterprise, The proposed solution has the potential to revolutionize the way you store and access your data in a more secure, reliable, and high-performing manner.

III Architecture

The main goal while developing the architecture for our solution was to make it as simple as possible, meanwhile delivering the before-mentioned requirements. The connection between peers on a decentralized server and clients is based on a standard peer-to-peer model, where every machine has a rank, chosen automatically depending on the version of the program. The most important, and the hardest factor considered while developing the peer-to-peer network is finding a way to connect to different peers. The most important part of solving this is network scanning, which is crucial to find new peers that have just joined the network. It is worth noting that the scanning is done continuously, so the gap in time between peers is reduced to a minimum. The process of scanning is only done on addresses and ports that are not saved in the peer list, which contains all data about peers from previous connections. On our network, every machine is equal to others, which means that there is no hierarchy between the peers (this is done by using pseudo randomness of time). Athena is divided into two layers, the first of them being a peer-to-peer storage network described above. The second one contains several factors located on an external blockchain. The most important of them is a smart contract (written classically in Solidity) located outside of the storage layer. The split is a cover for removing the trust in the external network, which leads to better safety and reliability. Overall, the architecture of Athena is dedicated to decentralization, safety, and solving the complicity of peer-to-peer networks. This blueprint of the connection in the network can be recognized as the base of the proposed solution.

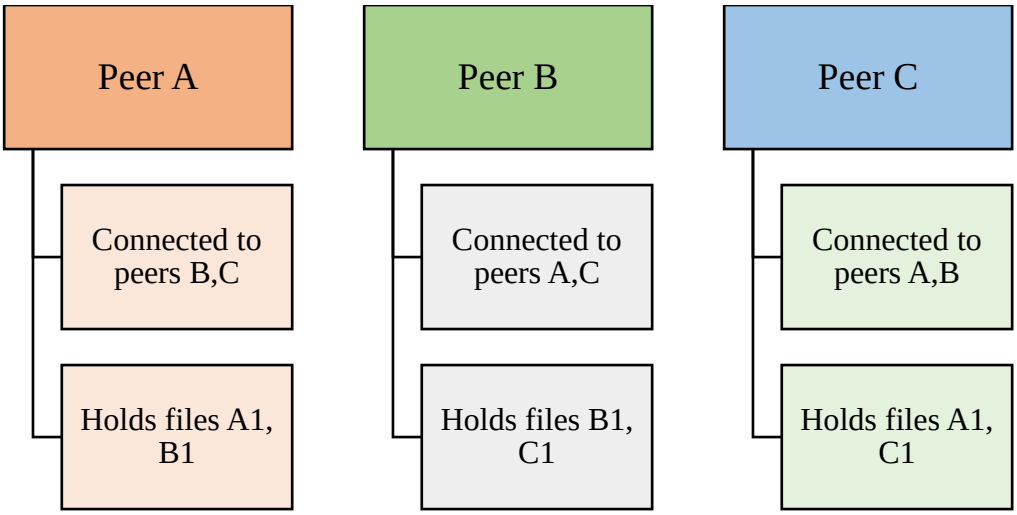


Figure 1 – Architecture of Athena

IV Decentralized server

Athena's decentralized server operates as a peer-to-peer network composed of storage providers that function as equals, without a hierarchy of connections. The primary responsibility of each peer is to guarantee the security of the files against any external interference. Once the client sends the data, the peer allocates it in its internal memory, separately from other data. To access the encrypted database, a map file in JSON format is used to locate the specific data. The map file contains the hashed file key and a list of file names related to that key. Every peer listens continuously for requests from clients and other members of the network. The internal

data storage comprises a list of available peers and those sharing the same files. When a part of the server receives a file-sharing request, it first verifies the authenticity of the files. The requested peer then reaches out to other peers holding the same file to verify the data's consistency across all units by comparing the amount and order of characters in each file. If the data is not correct, it is standardized by the most common version of it. The verified data is then transmitted to the client, along with a hash function result that serves as evidence of the storage provider's work. This evidence is called Proof of Logs (PoL). One of the most important parts of the decentralized server is the local logging system, which is used to calculate important payment statistics. This system is crucial for the network to operate safely, as collected data is processed locally and is not sent anywhere else. The Proof of Logs partly uses this system for delivering proof to the client, by sending a one-way hash function result that is based on the results of work from this element. In essence, the storage process is easy and requires little effort from the user. All that is needed is to maintain a computer connected to the network for seamless file uploads. The system works automatically without the user's intervention.

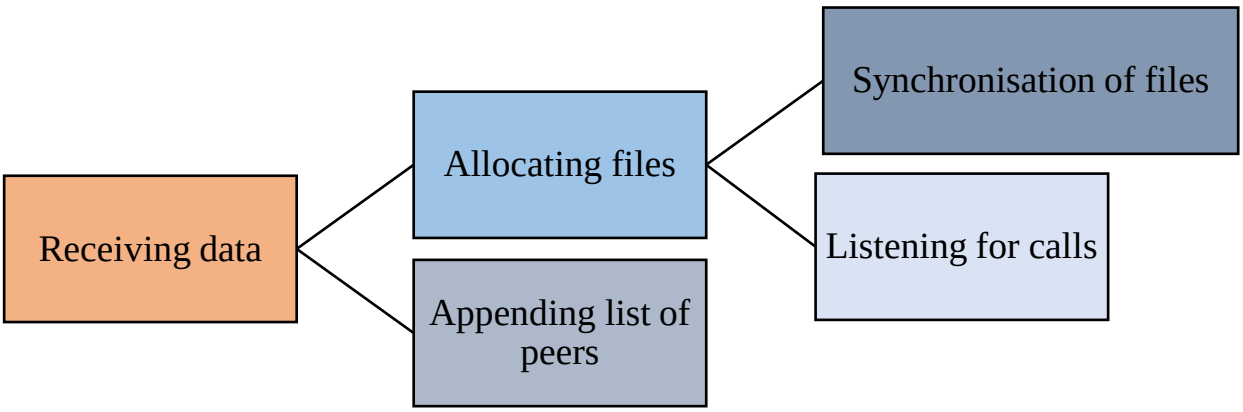


Figure 2 – Decentralized server queue of actions

V Client side

The client side of Athena enables users to upload and download content from the network. It plays a crucial role in enhancing the overall user experience, as it handles most of the algorithms, such as peer selection and encryption. To upload a file client has to complete the steps provided below:

a) Scanning the network to find peers
b) Creating a connection between client and peers
c) Calculating amount of peers needed to securely handle data
d) Choosing the peers, based on previous calculations
e) Encrypting the data with AES encrypting function
f) Compressing the files and sending them to one of the chosen peers, which will then distribute them through the network

The scanning and connecting process in Athena Network is akin to the trial and error method, based on the architecture mentioned earlier. The client appends a list of discovered peers, which can be used to establish connections with other machines.

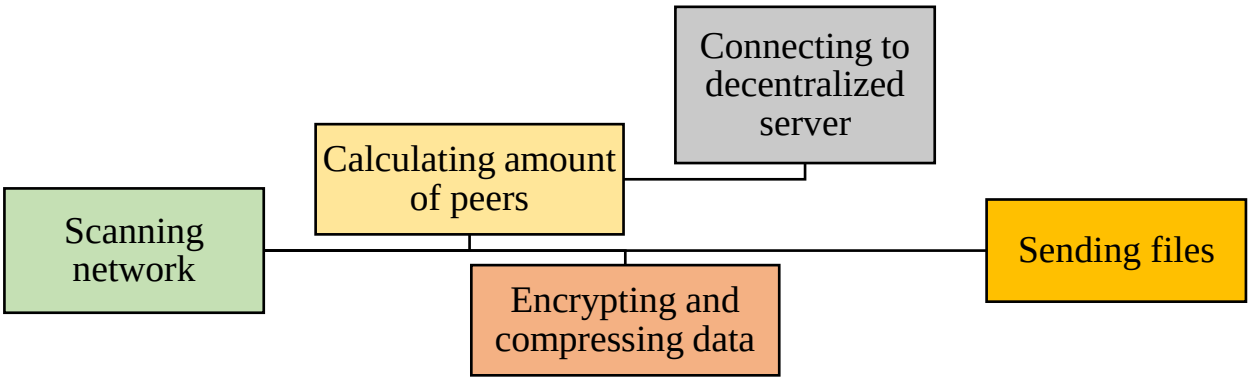


Figure 3 – Queue of actions on client side

Moving to the third step, the amount of peers calculation is one of the most important steps toward creating decentralization. We can assume a situation where a peer goes offline for a longer time, then who will send the requested files? The distribution between different peers is one of the most crucial solutions to that problem. The outcome is based on the overall number of peers active in the network. We can describe it with the following mathematical function:

$$Q(x) = \left\lceil 2\left|\sqrt{\log x}\right|\right\rceil$$

The above mathematical function is combined with the Quick Sort Algorithm, and pseudo randomness of time to bring a high-level decentralization to the network. To successfully choose peers, the following steps have to be completed:

a) Performing the above-provided calculation
b) Segregating the peers, by the amount of shared storage (Checking if a peer has shared the proper amount of space to upload files)
c) Sorting the list with Quick Sort Algorithm
d) Diving sorted data into k parts
e) Choosing one peer from every part (based on time)
f) Returning the results

This procedure would protect the network from choosing improper peers, which would result in sending files to the wrong machine. The math behind it takes care of the acceleration of required peers to successfully upload files by smoothing the result with a square root. The pseudo-randomness of time would solve the default inequality of machines. The next step involves encrypting the files with AES (Advanced Encryption Standard) algorithm. To fully understand this algorithm we would have to dive deeply into cryptography. Starting with a short description, AES is a symmetrical block cipher algorithm, considered to be one of the most

important, secure, and durable encrypting algorithms available. This means that the security of files uploaded into Athena is in good hands. The first mentioned trait, symmetrical encryption, means that the same key is used to encrypt and decrypt the data. This provides simplicity of self-custody storing chosen key. To safely secure the data, AES encrypts and recreates every byte of the provided value. It is worth noting that this algorithm is widely used for encrypting important and even undercover governmental data. Provided factors prove the rightness of the algorithm choice. The mathematical proofs are shown later in the document.

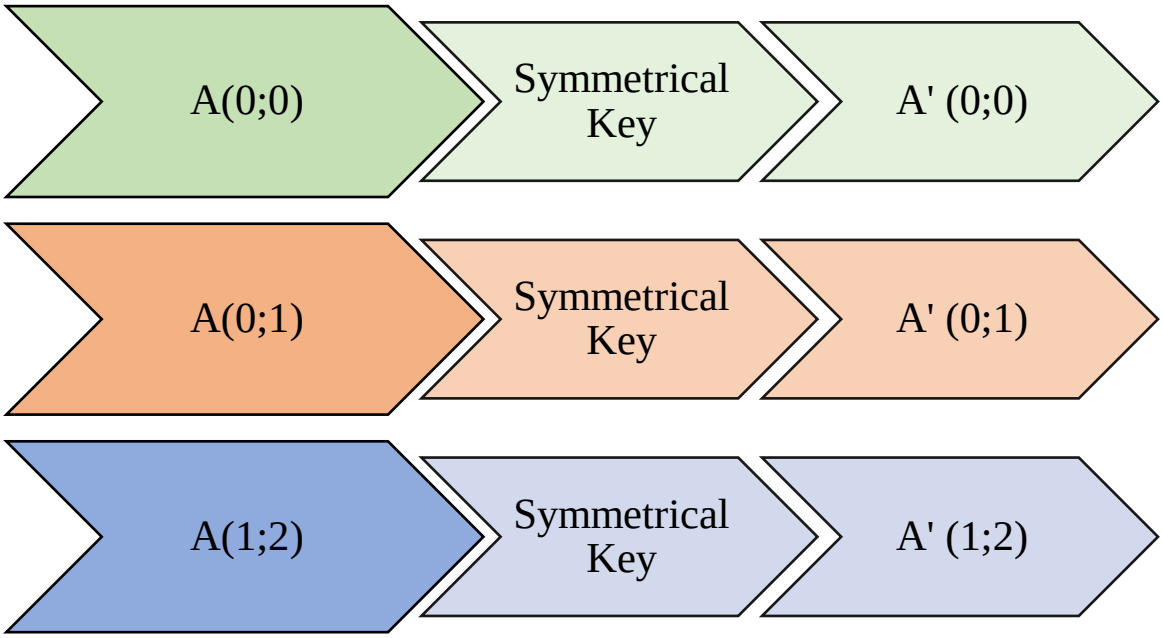


Figure 4 – Advanced Encryption Standard explained as graph

Later on, the files are compressed to lower the data used by the network to transfer files. This step is one of the most important steps, as without the network could be filled very fast in its begging development states. After completing all the above-mentioned steps, the files are finally sent to the peer that later distributes the files to other required peers active in the network. Overall, Athena's client side is crucial to develop a healthy ecosystem, that would be able to handle the high throughput and security of the network.

VI Economical view

The Main Athena Network payment method would be a smart contract-based token located on an external network. To fully understand the concept we would have to define the smart contract fittingly. A smart contract can be defined as a programmed agreement between users and nodes that specifies actions that are consistent with the rules and limits of the blockchain in its current state. This definition is based on the concept of a blockchain as an interpreted state transition system that is constantly changing as new transaction blocks are added.

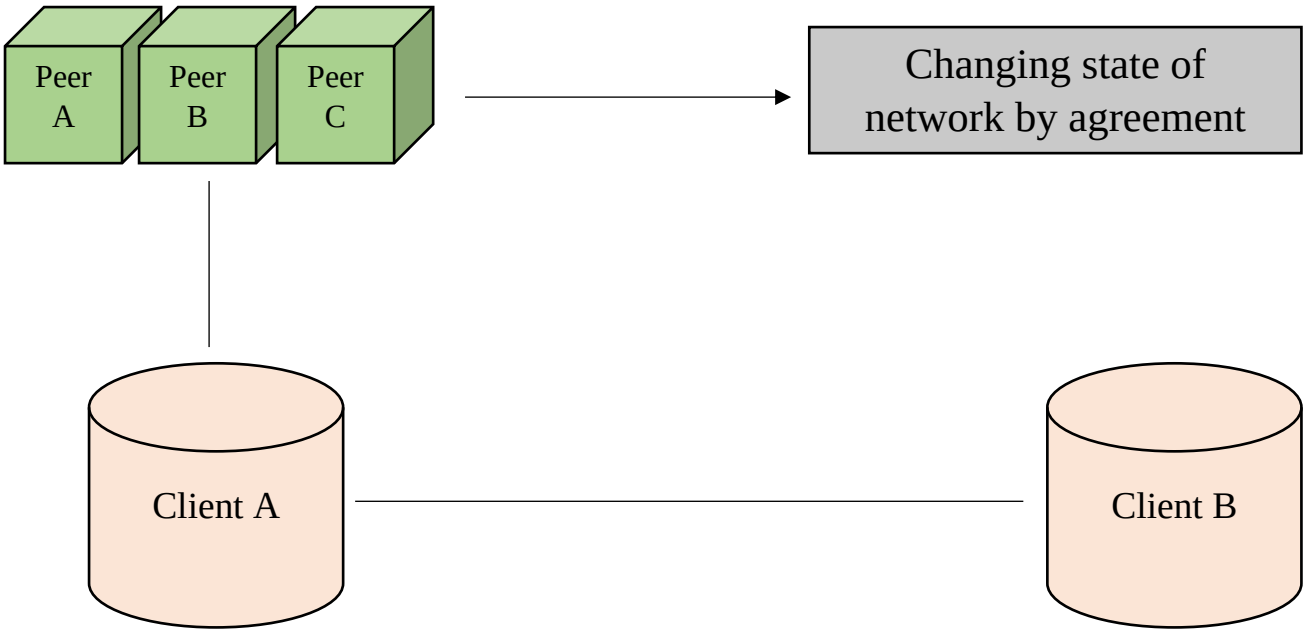


Figure 5 - Changing state of network by smart contract agreement

In our particular example, the state of the network is not a state of external payment processing blockchain, it is a state of the user's action. We can singularize three types of actions as follows:

a) A withdrawal request is done by a peer
b) A payment request began by the client
c) An exempt transaction is done with Athena Token
d) Deprivation state

To be clear, we do not consider the third state as an action done within the network, as every step of it is processed on the external blockchain. A withdrawal request is an action done by a peer when it wants its payment to be sent to a specified address. This works as follows:

a) The peer constantly proceeds data collected by the logging system
b) Provider unit generates a Proof of Logs, that is used as evidence of work done within the network
c) The necessary data, such as the withdrawal amount, a public key, and the proof is then sent to the smart contract operating blockchain
d) The withdrawal is processed by the blockchain
e) If everything was done correctly, the withdrawal should be complete
f) In other cases, the feedback is sent to the peer, and from here the process can be repeated

It is worth noting that the speed of transactions would completely depend on the external network as it is treated as a decentralized payment processor. A payment request state occurs when the client is paying for service. This works as provided below:

a) The payment is done via payment processing blockchain with a special signing
b) Smart contract appends a database of public keys and assigned storage size
c) Network lets the user make use of the bought space
d) When the memory limit is exceeded, the smart contract makes the file uploads from the user no longer available, until expanding accessible memory

e) When the public key is changed the smart contract is updating data to the current key provided by the user

The last state appears as the most common, as it occurs when a user doesn't actively participate in network transactions. Switching to the Athena Token (ATT), we took into account the issue of token deflation, which is a significant challenge for utility tokens. To address this, we have introduced a cap on the number of tokens available for minting, which has been set at 184 million (184 000 000) tokens. This procedure would lead to maintaining better control over the token circulating supply. But every solution has its disadvantages. In this case, the problem would be reaching maximum supply, but we consider a situation when some peers would sell made tokens to any source, that could, later on, sell it to the customers.

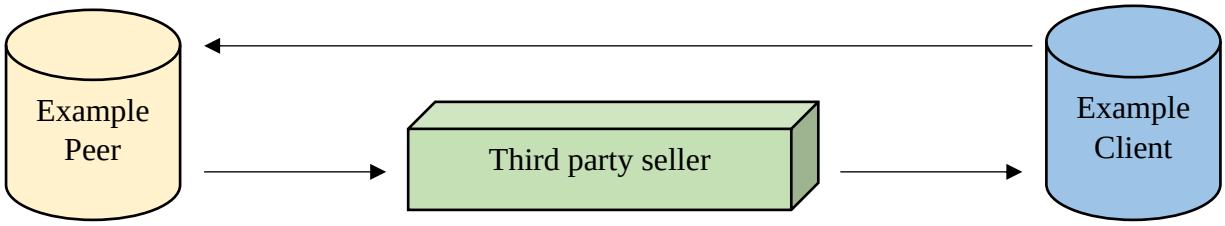


Figure 6 – Future economy of Athena Token

Also to make this possible the halving process, which stands for cutting in half the price of storage and payments, was introduced into the network. As every machine can count time on its own, this event would occur every two years counted in Unix Time.

Estimated years (Yr.)	Price per 1 GB of storage (ATT)
Starting year (U)	6,24
U + 2	3,12
U + 4	1,56
U + 6	0,78
U + 8	0,39
U + 10	0,195
U + 12	0,0975

Table 1 – Halving

Overall, the economy of Athena would depend on different smart contracts, which would be listening for calls on an external blockchain. To fully balance the circulation of Athena Token, we introduced the maximum limits of minted units. The circulation would also be impacted by the halving process that regulates the price of storage and payments in time.

VII Exceptions

Double sending

Double sending refers to the occurrence of transmitting data twice with the same timestamp, which is a common type of error. This issue can be resolved by sending the time stamp to the server side, which then compares the time stamps of the files and prioritizes them based on their recency. The more recent file is given higher importance. If two files are sent at the same exact time, the client side is notified of the situation, and feedback is provided to indicate whether the file needs to be retransmitted.

Peers' disagreement

Disagreements among peers can arise during file checks, leading to a voting process to determine the correct information. During the voting process, peers use the data they possess as their votes. The results are then calculated, and the option with the most votes is sent to the client. If the number of votes is equally divided, the file's overwrite timestamp is used to select the correct information, preventing incorrect information from being sent.

Offline peer

When a peer logs off, it notifies other peers, and they subsequently distribute files across the network and update their information to ensure Athena's security. If the peer designated to retrieve data is offline, the client side continues to scan the network and tries to connect with other saved peers. The allocation of peer numbers, as explained in a previous paragraph, helps to minimize trust issues.

Infecting the client-server bridge

For a third party to gain access to the communication between a peer and client, one of the parties must have shared their device information carelessly with an unauthorized entity. To prevent this from occurring, it is the responsibility of both the clients and providers to protect their keys, passwords, and other sensitive device information. Users must ensure the safety of their machines from hacking attempts, as the security of Athena is designed with the utmost care, minimizing the possibility of data being extracted from a peer or client's machine. To ensure a secure connection and devices within the network, it's crucial to avoid the following actions:

a) Neglecting the computer's security

b) Sharing sensitive device information

c) Carelessly granting access to external machines

By taking these precautions, the network's devices and connections can remain secure.

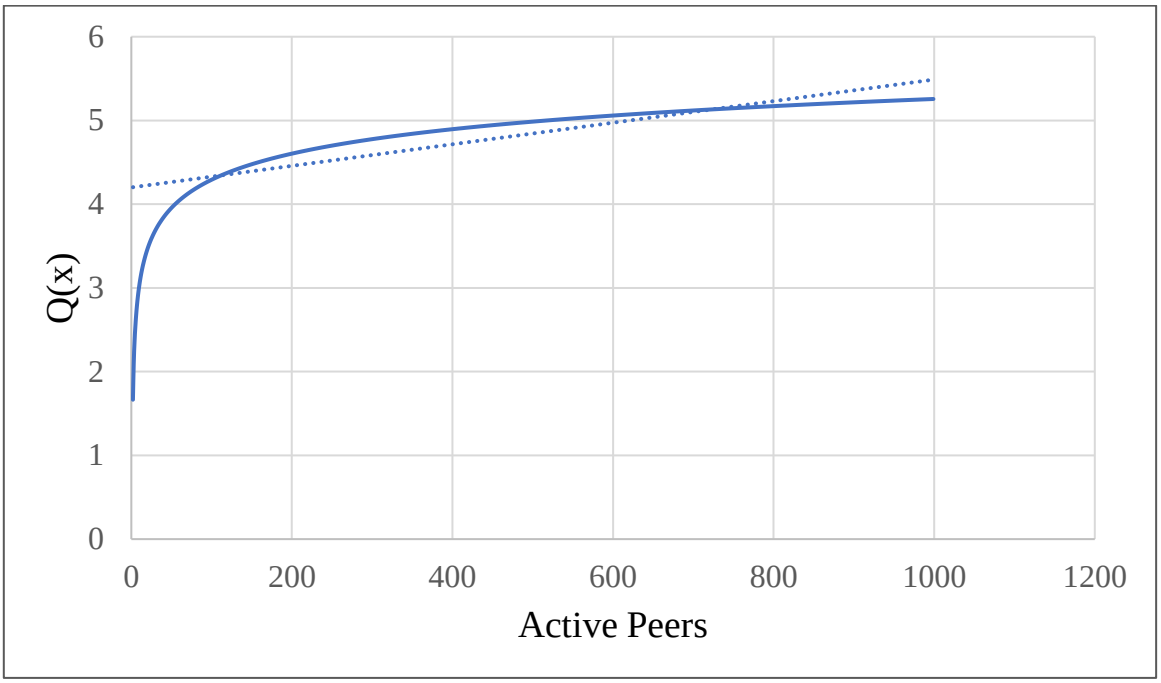
VIII Calculations, research, artificial environment testing

In this chapter, we will show the mathematical proofs, examples, and behaviors of different factors in an artificial environment. This part of the document should be treated specially, as it can show the true potential of the solutions that the network is created with. Starting with the number of peers that files are allocated on, we should provide a few examples of the outputs for different figures of active peers:

Number of peers	Output of Q(x)
2	2
10	4
18	4
26	4
34	4
42	4
50	4
58	5
66	5
74	5
1000	6

Table 2 – Example outputs of Q(x)

Considering these values, we can see that the output is not rising rapidly, which can be interpreted as a good sign of the function work because if the value rose sharply, the peers would be quickly filled with data from all the clients. Here we can assume that for two peers, there can be even a few hundred clients. This eliminates the issue of a low number of peers in the begging states of the network. Now we can show the graph of the before-mentioned Q(x) function (please note, that considering the scale, small measurement error may occur).



Graph 1 – Q(x) mathematical function

It is worth noting that, as there is no possibility to choose peer as a float value, the output of this function is always rounded up to the next integer. As we can see on the chart, the values are slowly rising to infinity. We can form a domain of function as follows:

$$x \in (1 ; \infty)$$

Then we can calculate the set of values as provided:

$$Q \in (1 ; \infty)$$

And the limits of Q(x) function:

$$\lim_{x \to \infty} 2|\sqrt{\log x}|$$

$$x = \infty$$

$$Q(\infty) = 2\,|\sqrt{\log \infty}\,| = \infty$$

Overall, the before-mentioned function provided the best results for a task like this. Other tested functions were not capable of balancing the Q value in the long or short term. An example of a function like this can be:

$$F(x) = \frac{\sqrt{x^3+4x^2+8x + 10x^3}}{10}$$

The problem with any other function similar to the one provided above is that even for $x > 1$ the values are rising too high at the beginning or near the limits. The used mathematical function does handle these problems very well. Moving on to the AES encryption, we can show example outputs of the function for specific keys:

State A	Key	State A' (Hex)
Text	fs6ap5FKnE7mt6ub	2643278a390044888ad57c1d2658db83
Text1	jz4nRrEsmNyCXM9L	b44e3bbb3f2459108e27ffe6f366744b
Text2	wnk3Y2jrb8VRFxMv	f2e194d428b00e1fdad117c97431a0fb

Table 3 – Example AES encryption

As we can see similar text doesn't produce similar encryption, which is a very good sign for using it, as the input text is not encrypted similarly with different keys. The time to break this algorithm can be evaluated for a 2GHz machine with the following calculations:

$$\lambda = \frac{\text{amount of keys}}{\text{keys checked per second}}$$

$$\lambda = \frac{K}{T}$$

$$\lambda = \frac{2^{256}}{2^{20}}$$

$$\lambda = 2^{236} \text{ seconds} = 1.8404656924774837e + 69 \text{ hours}$$

$$\lambda = 7.668607051989516e + 67 \text{ days}$$

$$\lambda = 2.1009882334217852e + 65 \text{ years}$$

We can do the same for the Frontier (the most powerful known supercomputer in the world):

$$\lambda = \frac{\text{amount of keys}}{\text{keys checked per second}}$$

$$\lambda = \frac{K}{T}$$

$$\lambda = \frac{2^{256}}{2^{40}} = 2^{216} \text{ seconds}$$

$$\lambda = 2.0036585172860958e+59 \text{ years}$$

And the probability of guessing the key on the first try (without considering pseudo randomness of choosing algorithms):

$$\lambda = \frac{1}{2^{256}} = \frac{1}{1{,}157920892373161954235709850086 9e+77}$$

The provided values are only evaluated, but their precision can be considered very high as the numbers are very high. It is worth noting that to break the AES encryption in the worst calculated case with a 2 GHz processor, the time needed would be 1.3×10^{53} times higher than the age of the universe. Switching to the frequency of repeating peers, is considered one of the most dangerous unwanted events. It can be described as one of the disadvantages of using pseudo-randomness based on time, or any other factor dependable on calculations or any other type of math. To check if it occurs, we can create an artificial environment containing 256 different peers, that are all capable of holding any capacity of files in any given state of the network.

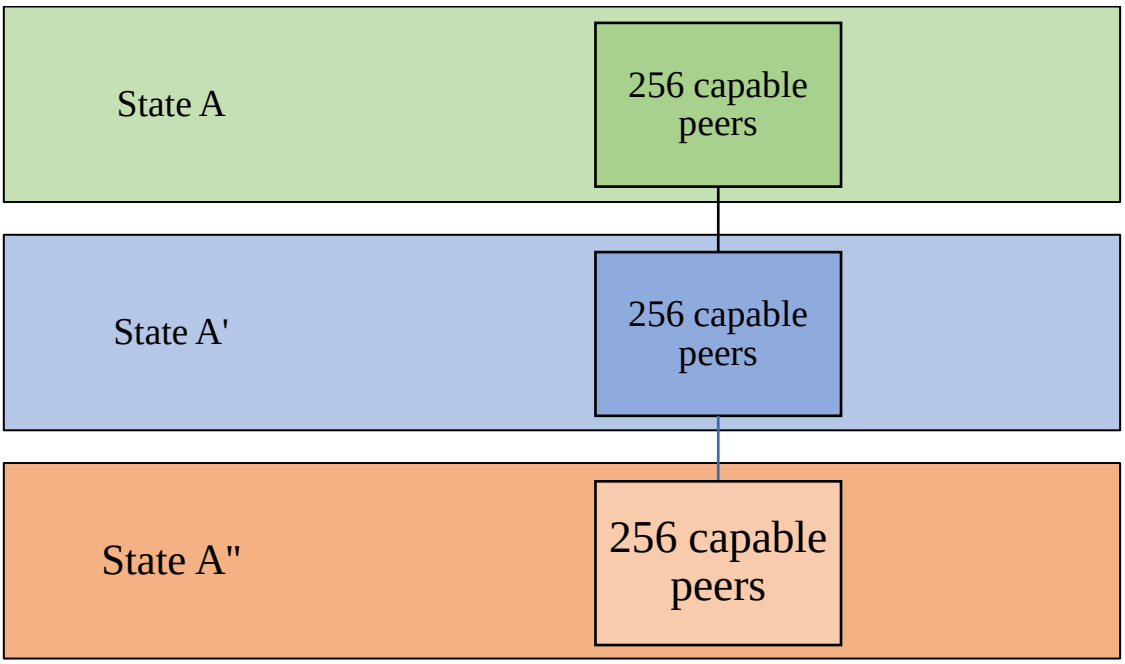
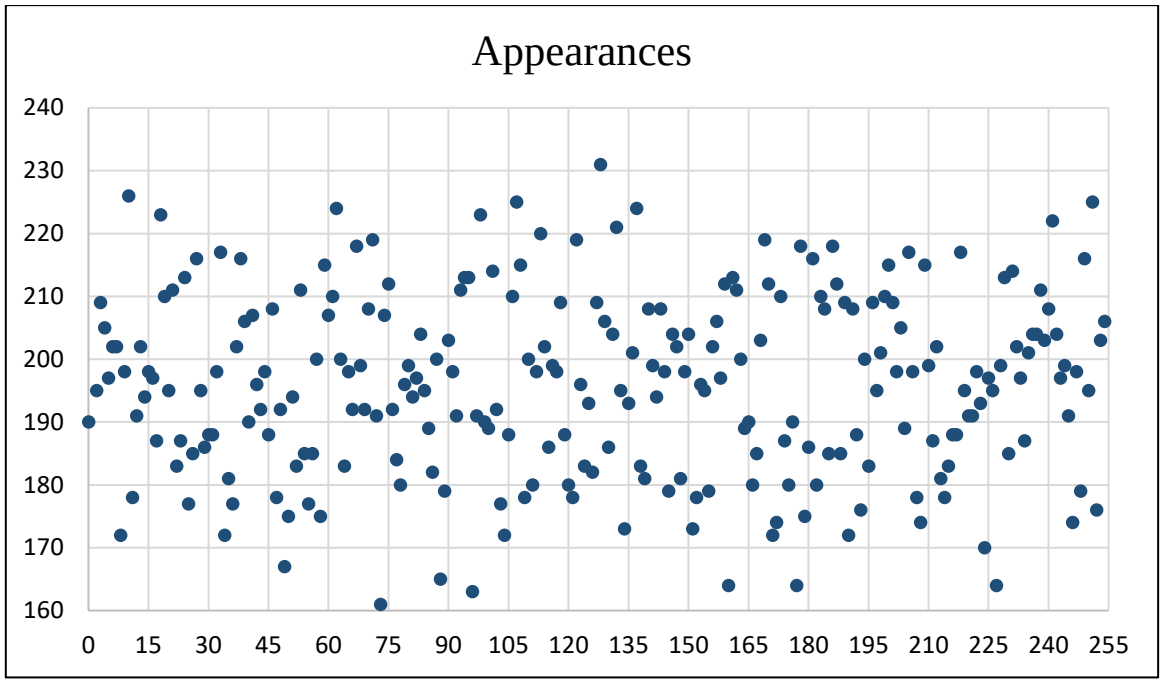


Figure 7 – Simulation model

The results of simulating 10 000 cases can be presented as following table:



Graph 2 – Simulation of 256 peers working in the network repeated 10 000 times

As we can analyze the graph, we notice that the problem hardly appears for provided values. If we consider lower values, we can assume that repeating here wouldn't be something unnatural for this type of calculation.

IX Roadmap

The roadmap of Athena Network is a comprehensive and strategic plan that outlines the development and growth of the project over time. It encompasses a range of activities and milestones that are designed to achieve specific objectives and targets. It can be described with the following steps:

a) Creating an external peer-to-peer network, as described in the third chapter of this document. Then testing its limits, performance, and safety in terms of pure source code (without considering machines' connection and hardware performance)
b) Establishing and developing safety around the created network, by providing hash messages, hashing and AES algorithmic encryption.
c) Forming the logging system described in the fourth chapter, that would be later on used with the before-mentioned security tools
d) Programming the smart contract, and integrating it into both the external storage network and payment processing blockchain
e) Connecting all the necessary functions and algorithms into a decentralized server client, and user-friendly interface app that would enable file uploads to the network
f) Publishing the code, as an open source project on the outer platform, such as GitHub with GNU, Apache, or MIT license (this will be considered before the network launch)
g) Creating an ICO (Initial Coin Offering, but in this case a Token) that will raise funds for maintaining the network and creating an environment around it
h) Launching the network in early 2024

In terms of the future, the most important action is to ensure the security, and performance of the network. To make this happen, in short term before launching the company called Athena Labs. Its main goal would be to care about the network and all subjects created around it. Athena Labs plays a crucial role in ensuring the success of the Athena Network project. The company is responsible for implementing a wide range of initiatives designed to guarantee the performance, safety, and reliability of the network. In addition to overseeing the technical aspects of the project, Athena Labs is also responsible for creating an ecosystem around the network. This includes developing partnerships with other blockchain-based companies and fostering relationships with community members and investors. A key priority for Athena Labs is ensuring that the network is highly secure. To achieve this, the company plans to use a combination of sophisticated encryption algorithms and advanced security protocols. This includes implementing multi-factor authentication, and continuous monitoring of the network for potential threats. Another important initiative for Athena Labs is ensuring the scalability of the network. As the popularity of the network grows, it will need to be able to handle increasing amounts of data and traffic. To achieve this, Athena Labs is exploring a range of strategies, including the use of sharding, which can help to distribute data across multiple nodes and improve network performance. To ensure the long-term viability of the project, Athena Labs is also working on developing a range of applications and services that can be built on top of the network. These include a multi-blockchain, self-custody cryptocurrency wallet, that could be integrated into the client side of Athena. In addition to these technical initiatives, Athena Labs is also focused on building a strong community around the project. This includes creating educational resources and engaging with community members through social media, online forums, and other channels. Overall, Athena Labs plays a crucial role in ensuring the success of the Athena Network project. By focusing on security, scalability, and ecosystem development, the company is working to create a robust and sustainable network that can provide value to users for years to come.

X Use cases

Athena has been developed to serve the needs of both individuals and businesses. It can provide secure and efficient storage for a wide range of data, from simple pictures to entire projects, while also handling high volumes of traffic. Whether you're a business owner or a family member looking to clear some disk space, Athena can accommodate your needs. Additionally, the graph depicting the standard software engineering use cases can be used similarly as shown in Figure 2 and Figure 3. The use cases graph represents every step involved in the process of utilizing a network. The described figure is located on the next site of this document.

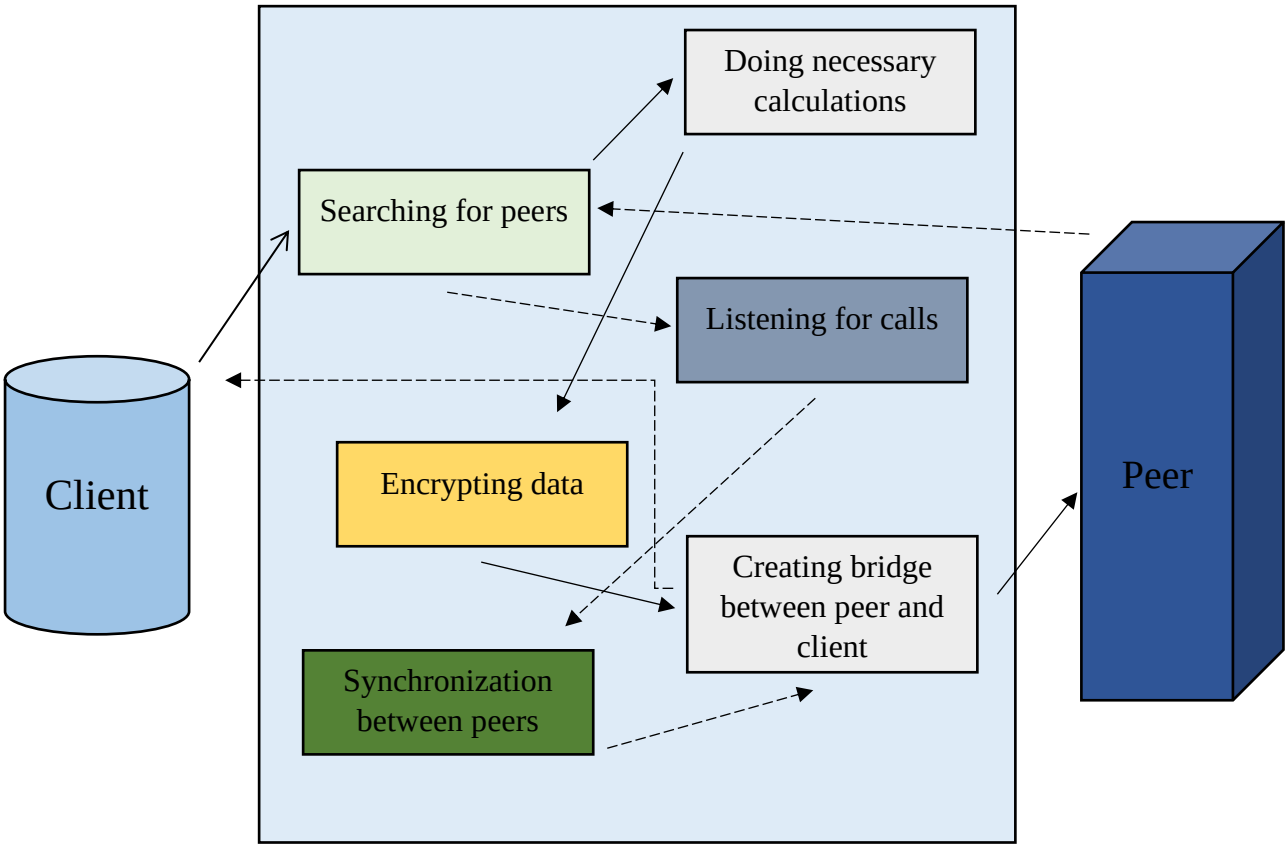


Figure 8 – Use cases

XI Conclusion

We have presented a solution for creating a fully decentralized storage system that is both secure and performant. Our calculations show that the overall security level is high. The scalability of Athena, however, is dependent on the internet speeds used by clients and peers in the future. For those seeking an advanced and dependable decentralized cloud solution, Athena would be an excellent choice that is poised to exceed expectations and continue to innovate in the years ahead.

XII Further reading

To gain a thorough understanding of the architecture of the Athena Network, it is necessary to have an advanced knowledge of smart contracts, blockchain, and the philosophy that underpins the technology. The Ethereum whitepaper is an essential document to understand the concept of smart contracts as presented in chapter VI. Additionally, it is crucial to recognize the significance of the InterPlanetary File System (IPFS), which can be considered a more advanced precursor to the proposed solution. To comprehend the chosen algorithms utilized in the network, acquiring advanced cryptography knowledge would be imperative to achieve a comprehensive understanding of the system.