Internxt

Table of contents

Introduction

Internxt® is disrupting thrilling industries through the application of revolutionary technologies. There are many widely used services which need to be rebuilt from the ground up. Internxt provides innovative products and services that strive to outperform those currently used by the mass-market. The goal is a vast suite of innovative services that are mass-market attractive. Internxt is registered in the United States at 18 Bartol Street 134, San Francisco, 94107 California, as Internxt Inc.

Public cloud computing and public cloud storage have proven to be an attractive business model for the large centralized cloud providers. Cloud computing is estimated to be a $186.4 billion-dollar market in 2018 and is expected to reach $302.5 billion by 2021. A major issue with existing cloud storage platforms is security and data centralization. Internxt's X Cloud brings a new and revolutionary solution to the market. The data on X Cloud is spread across a decentralized network of machines, and all the files are client-side end-to-end encrypted. There are no single points for hackers to attack. It would be an incredibly complex process for anyone to access a file on this network, and even if they could it would be worthless without the private key held by the owner. Internxt intends to begin to combat the security and privacy issues the Internet is currently facing with the development of its first service: X Cloud. Additionally, due to the decentralized nature of X Cloud, this is also significantly more affordable than any service currently used by the mass-market. We expect X Cloud to be of vast need amongst users who need to store vast amounts of confidential data on the cloud. This mainly includes businesses, thus mainly making of X Cloud a B2B product. X Cloud is designed as an alternative to services like Dropbox or Amazon S3, by providing a seamless web, mobile and desktop experience, as well as a complete API to which Amazon S3 customers can easily switch.

X Core is the foundational base of our first service, X Cloud. X Core is the infrastructure created by users all around the world participating in the creation of a decentralized, more secure cloud. Users can sell the resources of their machines to those looking to host their data in a more private, secure and efficient way. X Cloud leverages a superior technology to that of traditional cloud services, which allows it to offer a more secure and affordable cloud storage experience. All files stored in X Core are distributed and cryptographically end-to-end encrypted, reliably protecting against hacks and leaks. All of Internxt's code is open source and is available for peer review on GitHub.

Products

X Core

There are significant underutilized resources at the edge of the network for many smaller operators. We have found a long tail of resources that are presently unused or underused that could provide affordable and geographically distributed cloud storage. Conceivably, some small operator might have access to less-expensive electricity than standard data centers or another small operator could have access to less-expensive cooling. Many of these small operator environments are not substantial enough to run an entire datacenter-like storage system. We have found that in aggregate, enough small operator environments exist such that their combination over the internet constitutes significant opportunity and advantage for less-expensive and faster storage. X Core is the foundational base for Internxt's X Cloud service. X Core is formulated by a decentralized network of Hosts, which eliminates the need for a central controller. Hosts provide the unused resources of their machines, creating a global, distributed storage infrastructure.

Hosts are paid in the Internxt token, INXT, by providing their unused computer resources to the X Core network. Hosts do not need to be active with their computer, they may leave it running in the background and the computer will earn a passive income. X Core is a simple, downloadable open-source application

that enables anyone to act as a decentralized node to store and transfer data. Financial rewards for hosting encourage more people to sign up and grow the X Core network.

The more Hosts, the better the network will run. The system detects failing nodes and transparently adjusts and corrects the impacted blocks automatically. This removes the threat of theft or loss that is constantly present for any data stored in a central location, and ensures the network always functions optimally. User files are client-side end-to-end encrypted and split into shards when hosted on the X Core network. In our storage system, audits are simply a mechanism used to determine a node's degree of stability. Failed audits will result in a storage node being marked as bad, which will result in redistributing data to new nodes and avoiding that node altogether in the future. Storage node uptime and overall health are the primary metrics used to determine which files need repair.

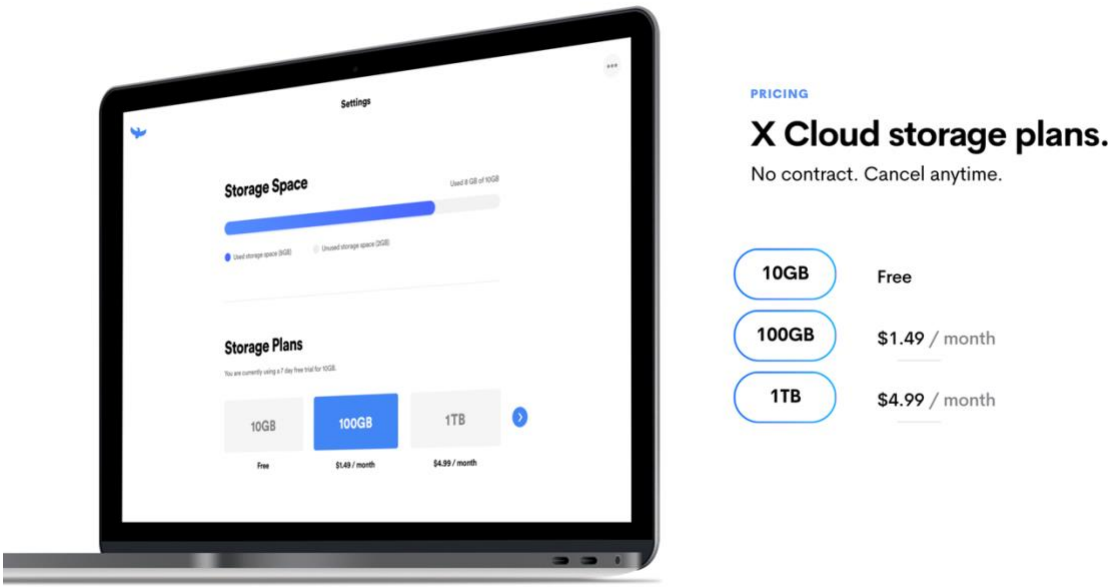
Each Host decides how much of their computer resources they designate to the network, as well as when and for how long. X Core automatically finds the optimum Host specific to the user's location, ensuring the data is retrieved as rapidly as possible. The network is designed to handle large numbers of Hosts and users joining by balancing the data-load across multiple nodes. Since the number of the nodes running may vary over time, X Core has an automatic adjustment feature, which enables X Core to regulate the workload of each networked computer efficiently. This means that the fluctuations in the number of Hosts or users online will not affect the usability of the entire network nor the working capacity of each particular computer within the network. Thus, the system automatically maintains the right balance between all available users in order to provide them with an equal operability of the network. Additionally, a much higher download speed is achieved through a simultaneous synchronization with many different nodes. X Core features desktop interfaces available for Windows, Mac, and Linux. The mathematical formula used to compute each node's monthly earnings can be seen under Appendix 1. To summarize, payments are always relative to how other Hosts perform in a given month. The amount of disk space allocated to each Host over a period of one month is given 70% of the payout weight. The number of Internxt tokens held (also relative to other Hosts) carries 30% of the remaining weight when calculating monthly payouts.

X Cloud

Internxt's X Cloud allows all users to store files in a truly secure, private and reliable cloud, without compromising on user experience. X Cloud is faster, cheaper, and more secure than traditional cloud storage platforms. Furthermore, Internxt fundamentally believes in beautiful design. It may take a little more time in the beginning to craft a joyful product experience for all users but the benefits of doing so are born out in the end. Internxt built X Cloud to be simple, elegant and intuitive, but also extremely powerful and highly customizable. X Cloud's desktop interface consists of an easy-to-use folder where files are automatically synchronized with X Core. (X Core's rapid synchronization of files throughout the P2P computers that comprise the network runs with Qt/C++ technology). With X Cloud, user data is no longer stored in a central location, but instead end-to-end encrypted, split into pieces, and then distributed amongst different machines all around the world. With X Cloud, the user is the only one with access to his/her digital possessions, the way it should have always been. The cloud services currently adopted and in use today are vulnerable to a variety of attacks, which can lead to encryption walls being bypassed and user's personal information accessible to hackers.

For far too long, companies like Google and Facebook have abused their position and violated their users' privacy. Recent events have highlighted the myriad of problems their business models create. Protecting their users' privacy conflicts with their business model; a business model which is to accumulate as much user data as possible in order to serve ever-more targeted ads. This is of course why these companies take every opportunity to collect, store and analyse more data than is actually needed for any interaction. Internxt is fundamentally transparent about its superior security and privacy practices. Here are the 3 most important steps we are taking to protect your data on X Cloud:

First, we encrypt all your data before it leaves your device and reaches X Core servers using AES 256-bit encryption. This is the same type of encryption that is being used by banks and government agencies to protect sensitive information. This is already a major difference from mainstream services such as Dropbox or Google Drive, which only encrypt customer data in transit and at rest, which means that these companies themselves can still access and use your data. With our encryption model, only you hold the keys to your data. Therefore, Internxt can never access your data and more importantly, in the event Internxt was ever hacked, the intruders would not be able to access your data either. Mainstream providers could offer this functionality as well, but they do not. As a matter of fact, Google started developing a way to encrypt emails end-to-end in Gmail after the Snowden revelations, but the project has been abandoned (and that's why projects like ProtonMail also happen to exist).



PRICING

X Cloud storage plans.

No contract. Cancel anytime.

10GB	Free
100GB	$1.49 / month
1TB	$4.99 / month

Second, Internxt does not store your data in a single location. It is instead spread across a large decentralized network. An attacker would therefore have to breach millions of servers in order to obtain your data, and if somehow successful in doing that, the data would still be encrypted.

Unlike other decentralized storage providers such as Storj and Sia, Internxt understands that superior technology is not the only requirement if one is to disrupt the market. It takes real effort, planning and execution to cross the chasm between early adopters and the mass market. One must tackle disruption from the correct angles. Because decentralized storage platforms cannot take many of the same shortcuts datacentre-based approaches can (e.g. firewalls, DMZs, etc.), decentralized storage must be designed from the ground up to support not only end-to-end encryption but also enhanced security and privacy at all levels of the system. We have not only developed a flagship infrastructure, but also a seamless user experience, which are honing and crafting our message for both early adopters of decentralized technologies, but more importantly for the mass market. Internxt also understands that businesses have different requirements than consumers and that they require certain legal protections. This is why Internxt will offer a special version of its services for regulated customers, such as businesses and government entities, that are subject to the General Data Protection Regulation (GDPR). This version of our service will also rely on a decentralized network, but we will control and carefully monitor which Hosts can participate in it. Every Host will have to sign a Data Processing Amendment with us and we will also require adherence to certain standards, which ensures that data is not only protected from a technical point of view, but also from a regulatory side. Additionally,

Technology

When data is stored in the network, the client encrypts and breaks it up into multiple shards. These shards are distributed to peers across the network. When this occurs, metadata is generated that contains information on where to find the data again. When data is retrieved from the network, the client will first reference the metadata to identify the locations of the previously stored pieces. Then the pieces will be retrieved, and the original data will be reassembled on the client's local machine. When the amount of redundancy drops below a certain threshold, the necessary data for the missing pieces is regenerated and replaced. The storage node's role is to store and return data. Aside from reliably storing data, nodes should provide network bandwidth and appropriate responsiveness. Storage nodes are selected to store data based on various criteria: ping time, latency, throughput, bandwidth caps, sufficient disk space, geographic location, uptime, history of responding accurately to audits, and so forth. In return for their service, nodes are paid. Because storage nodes are selected via changing variables external to the protocol, node selection is an explicit, non-deterministic process in our framework. This means that we must keep track of which nodes were selected for each upload via a small amount of metadata, which we also encrypt as early as possible.

Any type of file can be uploaded into our X Core platform using X Cloud. The encrypted shards are dispersed among separate Hosts, while the Bridge holds information about both the entire structure and the location of each bit of distributed data. Thus, nobody but the data owner is able to read the files since all shards must be collected and decrypted back to reassemble the file. It is technically impossible to read a piece of information stored on a separate Host's computer. The security of our network correlates directly with its size. The larger the number of Hosts that are participating as nodes, the more complex the entire system becomes and, therefore, the larger the number of shards all data can be divided into. At the same time, the P2P network protocol we use provides parallel data transfers making bandwidth

demands irrelevant. Furthermore, the multiple mirroring of shards adds even more security to X Cloud. This translates to an incredibly fast, reliable and resilient network. In retrospect, knowing what we do now, this is how the Internet should have originally been designed to operate.

X Core was forked from Storj, and some of its core features were kept as Storj developed them. Our primary focus has been improving their network speed and reliability, as well as adding features, creating intuitive interfaces and widely disseminating a message that the mass market understands. We are also running continuous independent audits to find vulnerabilities in our infrastructure and to ensure that it is always as robust as possible. We also implemented JSON data-interchange technology, which enables users to work with their files within a highly structured filesystem tree where both a root folder and numerous subfolders can be created in a very simple manner. X Core uses distributed technology and will be constantly maintained and updated to meet the requirements of our future services. In contrast with ordinary cloud platforms, our system is empowered with several types of cryptographic encryption at almost every stage of our processes. Files, shards, access passwords, and other textual data are protected with either SHA 256 or AES 256 CTR cryptographic methods. Both algorithms are applied to hashing and encryption of various data. While SHA256 creates digital signatures when the user's passwords are to be hashed, AES (Advanced Encryption Standard) is used for both encryption and decryption of files and shards. Even if a hypothetical hacker was able to figure out the exact location of a particular shard or a set of shards, the AES encryption protects the user's data from being read by this unauthorized person. In addition to the huge computation power necessary to hack even a single AES-encrypted shard, hackers would need to spend unprecedented efforts to select all dedicated shards that constitute a discrete file from the massive amount of data randomly distributed among various Hosts. As if this wasn't enough, the difficulty of the hypothetical hacker's task is further multiplied many times over due to numerous mirrors available for each shard that are distributed among different Hosts. Different Hosts can also change their state from active to inactive and vice versa over unpredictable periods, thus the complexity of figuring out the exact location of all shards of every single file begins to border upon the realm of the impossible.

Since users interact with the Bridge, Internxt's data management unit, they are relieved from a necessity to perform many operations manually. For example, they don't have to worry about the available storage space because no single Host can limit the overall size of the cloud. Collecting information about all available disk space throughout the active Hosts is the task of the Bridge. The information on storage space, velocity, and bandwidth available to users by all the currently running Hosts is managed automatically by the Bridge. A data owner simply needs to announce the size of a file to be placed in the cloud.
This is performed when a file from a local computer is uploaded to the X Cloud app. After that, the Bridge as a smart agent "decides" in which number of shards the file should be divided, as well as among which Hosts the shards, along with all their mirrors, should be distributed.

A similar process in the opposite direction occurs when a data owner wants to retrieve a file from the X Cloud. The data owner's X Cloud app informs the system about a particular file residing somewhere in the network. Holding the encrypted keys of both the user and the file, the Bridge collects all necessary shards through the X Core apps installed on the Hosts' computers. Neither the Bridge nor any Host is able to read

the encrypted content of the file since the decryption process is executed only via the unique keys on the data owner's local computer. The system cannot mistakenly confuse a particular data owner and another person's file. No mistake is possible because the Bridge connects a particular data owner only with those Hosts where the necessary shards reside. This process can be called a proof of availability since the data owner's X Cloud app shares shards along with the specifically hashed keys with the X Core apps of the selected Hosts. Any action where both a particular data owner and dedicated Hosts are involved implies exchanging the shards' hashes between them. The hashed keys are automatically updated in the course of interaction between data owners and Hosts. The whole process runs on a programmatic level. The users from either side of any interaction could be considered to be "hands off" in such a precise and secure proof of availability. Thus, the entire functionality of the system provides human-factor-free workflows wherein both premeditated as well as inadvertent errors are prevented by design.

Thanks to AES 256 CTR, X Core is able to decrypt the file for the user once it is returned. The file is divided into packages only after it has been encrypted to make certain that a Host has an amount of data that cannot be interpreted. It is not possible to decrypt one package and see any relevant part of the complete file's data. The maximum possible package size is to be set to 2MB. To be sure that a package saved by a Host was not modified, we use SHA 256 hashing. This is a one-way encryption technology. When we download a file from a Host, we calculate its hash and check if it coincides with that received from the Bridge. If it doesn't, we download the file from a mirrored Host.

Market position

Internxt is an innovation company. We are creating revolutionary services and solutions that strive to outperform the current options in the market – both the widely known and centralized options, and the decentralized projects that are attempting to compete. Internxt is ambition, excitement, and the sense of belonging to something better.

The Internet is a massive decentralized network consisting of billions of devices which are not controlled by a single group or entity. Much of the data currently available through the Internet is quite centralized and is stored with a handful of technology companies that have the experience and capital to build massive data centers capable of handling this vast amount of information. A few of the challenges faced by data centers are: data breaches, periods of unavailability on a grand scale, storage costs, and expanding and upgrading quickly enough to meet user demand for faster data and larger formats. Decentralized storage has emerged as an answer to the challenge of providing a performant, secure, private, and economical cloud storage solution. Decentralized storage is better positioned to achieve these outcomes as the architecture has a more natural alignment to the decentralized architecture of the Internet as a whole, as opposed to massive centralized data centers. News coverage of data breaches over the past few years has shown us that the frequency of such breaches has been increasing by as much as a factor of 10 between 2005 and 2017[1]. Decentralized storage's process of protecting data makes data breaches more di-cult than current methods used by data centers while, at the same time, costing less than current storage methods.

X Cloud's main competitive advantages center on privacy, security, efficiency and a user experience that is virtually indistinguishable from the centralized options. X Cloud's price and user experience are as competitive as those offered by the current top providers.

There are a few direct competitors to X Cloud. The decentralized space does contain some players striving to provide distributed cloud storage options and attempting to improve the way the Internet is organized. Although there are not many viable competitors, a few in the space have indeed developed impressive decentralized technologies. Internxt recognizes their outstanding work and applauds the progress made. However, none of these competitors have yet become mainstream, which truly must be the goal for decentralized technologies if we are all to realize the vision and purpose that brought us here in the first place. Internxt believes that the main issue preventing mainstream use resides in user experience and building a technology that is mature and robust enough to be used by the mass-market. X Cloud's beta service is available since Q3 2018, and the commercial version is scheduled for Q1 2019. Both releases include desktop, mobile and web apps. The focus for 2019 will primarily be growing and further improving X Cloud, and we also expect to develop additional services starting in 2021.

[1]Identity Theft Resource Center and CyberScout. Annual number of data breaches and exposed records in the United States from 2005 to 2018. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed/, 2018

To ensure that we can keep growing and operating until then, we will very likely be going through a Series A during 2019. More details on this will be provided in the coming months. If you feel you could add value to our company, believe in our mission and would like to be taken into consideration for our Series A, feel free to email us at ir@internxt.com.

Token

Internxt ran a token sale from September 7th – 28th, 2017, and a total of 629,610 INXT were distributed to crowdsale participants, bounty participants and the company, in varying percentages. The undistributed crowdsale tokens were locked forever (effectively burned). No more Internxt tokens will be generated, thus 629,610 INXT is the circulating and maximum supply of INXT. INXT will be used as a means of payment for all our decentralized Internet services using X Core, and potentially any future innovative tech services that Internxt may create. All revenue generated from our services is directly converted into INXT, which is fundamentally the same as customers purchasing and paying with INXT directly (which is also possible). For instance, $5M in revenue generated from our products and services during 2019, would mean a direct $5M in buy orders for INXT on public exchanges. These INXT, other than the commission kept by Internxt, are then distributed amongst the Hosts. INXT is an ERC20 token, divisible by 8 decimal places, allowing it to have decimal exponents if needed in the future. The design and implementation of the utility and token economy of the INXT token is a subject of utmost importance to Internxt. An essential and robust token economy is critical if decentralized technologies and their network participants are to succeed, flourish and broadly realize the vision, benefits and existential reason for being that birthed the concept of trustless ecosystems in the first place.

Appendix

Appendix 1. X Core Payout Formula

$E_i = (E / x) * (1 + \alpha_i)$
$\alpha_i = 0.7A_i + 0.3B_i$
E_i = Monthly earnings per node
E = Monthly total earnings
x = Total number of nodes
α_i = Correcting factor per node
A_i = Node's percental deviation from network average used disk space
B_i = Node's percental deviation from network average INXT held

Minimum monthly average used disk space for a node to be considered valid for variable A_i: 10 GB
Minimum monthly INXT held for a node to be considered valid for variable C_i: 100 INXT
Minimum monthly payout per node: 10 INXT (unless that threshold is met, no payment will be sent)

Case study. Month j. 3 Nodes

$E_i = (E / x) * (1 + \alpha_i)$
$\alpha_i = 0.7A_i + 0.3B_i$

Sample computation for variable A
Node 1: 10 GB average used disk space
Node 2: 12 GB average used disk space
Node 3: 20 GB average used disk space
Weighted average: 14 GB

A_1 = (10 - 14) / 14 = - 28,5714286%
A_2 = (12 - 14) / 14 = - 14.2857143%
A_3 = (20 - 14) / 14 = 42.8571429%
Similarly, we compute the variable B for each of the nodes. For the sake of simplicity in this example, we assume that $A_i = B_i = C_i$ for each node

α_1 =
= 0.7 * (- 28.5714286) + 0.3 * (- 28.5714286) =
= - 28.5714286%
α_2 = - 14.2857143%
α_3 = 42.8571429%

Assuming that in Month j a total of 100 INXT were collected:

$E_1 = (E / x) * (1 + \alpha_1)$
$E_1 = (100 / 3) * 0.724285714$
$E_1 = 23.8095238$ INXT
$E_2 = 28.5714285$ INXT
$E_3 = 47.6190476$ INXT