

Filecoin



Filecoin Primer
July 25, 2017

PUBLIC DRAFT 1



Protocol Labs, Inc.
filecoin-sale@protocol.ai

Introducing Filecoin

Filecoin is a decentralized storage network, powered by a blockchain and a native token.

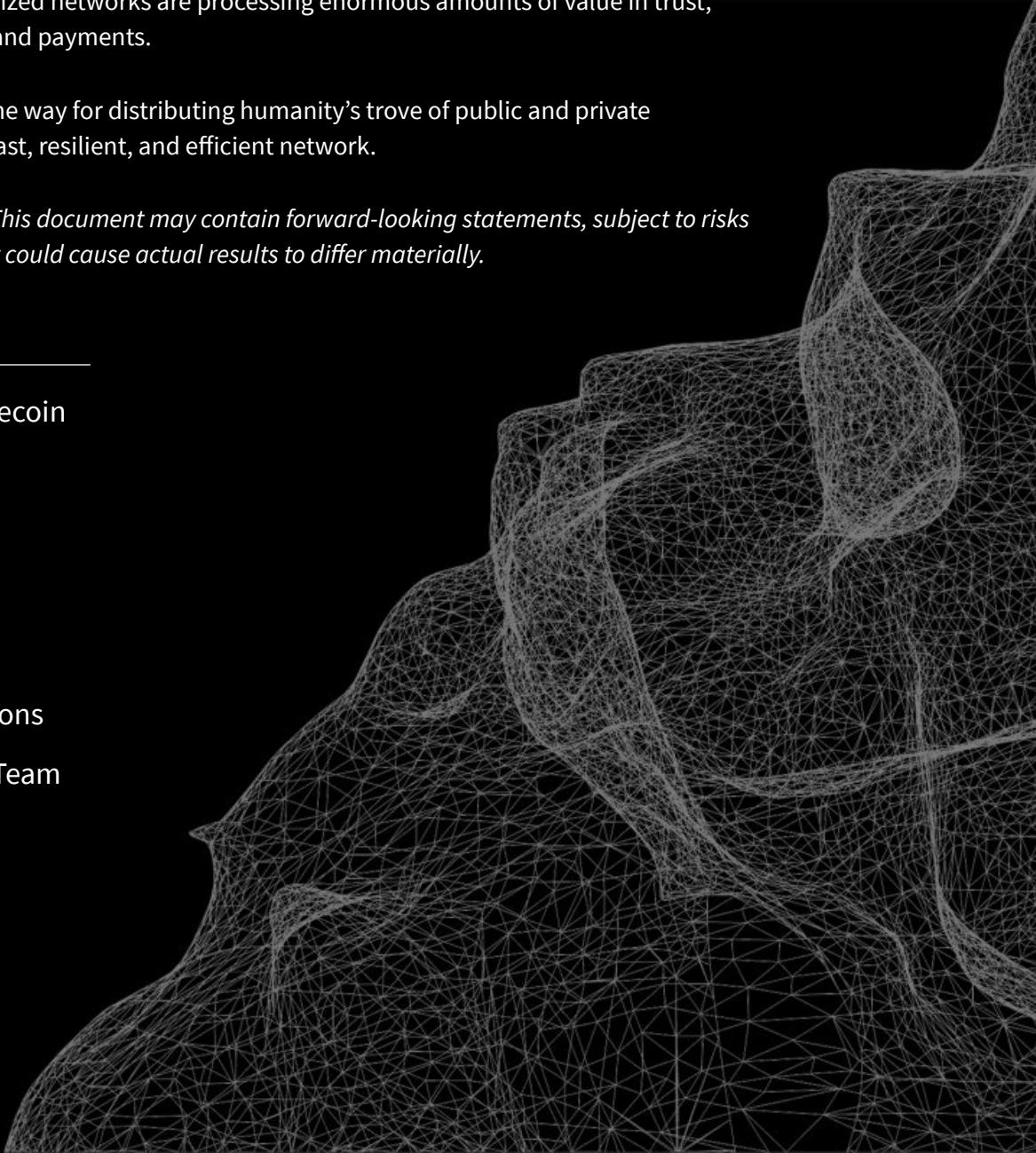
In the span of less than three decades, the world wide web has become one of the greatest achievements in human history. Today, we stand at the cusp of another transformation in computing.

Emerging technologies are transforming the web's underlying protocols. Using blockchain technology, decentralized networks are processing enormous amounts of value in trust, verification, storage, and payments.

Together, they pave the way for distributing humanity's trove of public and private knowledge across a vast, resilient, and efficient network.

LEGAL DISCLAIMER: *This document may contain forward-looking statements, subject to risks and uncertainties that could cause actual results to differ materially.*

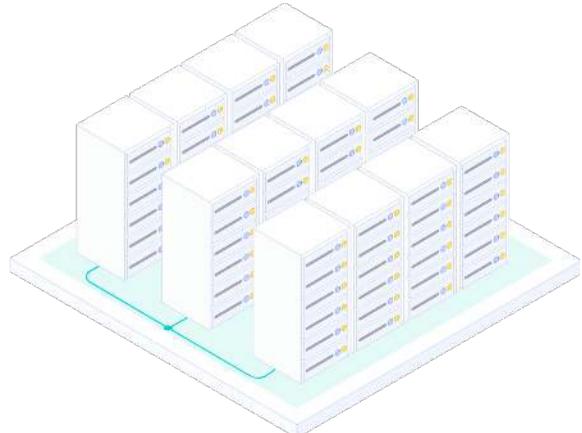
-
1. Introducing Filecoin
 2. Crypto Mining
 3. Overview
 4. Ecosystem
 5. IPFS
 6. Token, Allocations
 7. Protocol Labs Team



Unlocking the world's unused storage to meet the demands of tomorrow

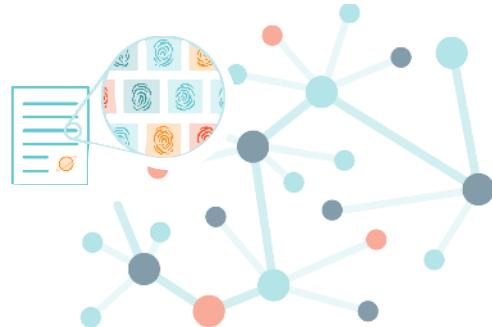
The world's storage is vastly underutilized

More data will be created in 2017 than the previous 5,000 years of humanity¹. Yet around half of the world's storage sits unused² — from hard-drives in basements to data centers. Filecoin creates an incentivized market to put this extra storage to work. With significantly more supply, we meet growing demand while lowering the price of storage.



Decentralization creates a better network

Filecoin uses IPFS, a peer-to-peer distributed network protocol which indexes each file by a unique fingerprint. Indexing files by these fingerprints, known as cryptographic hashes, allows us to find and distribute high volumes of data with high efficiency. The peer-to-peer network also rebalances and recovers in response to outages, creating a more decentralized and resilient web.



Filecoin is a token with fundamental value

Filecoin is like Bitcoin, but miners amass hard drives instead of hashing computers. Today's blockchains use a wasteful *Proof-of-Work* consensus. Filecoin uses a novel *Proof-of-Replication* function to create a useful and valuable storage service as a byproduct of the mining process. Miners are incentivized proportionally: the more they store, the more filecoin they earn.





Bitcoin mining began by cobbling together spare hardware.

Source: 99bitcoins

Today, industrial Bitcoin mines use special purpose hardware.

Source: Allied Control

The profits from mining Bitcoin and Ethereum have assembled
the world's most powerful computing networks³

Bitcoin miners around the world run large scale data centers with millions of computers. In aggregate, they earn billions of dollars per year.

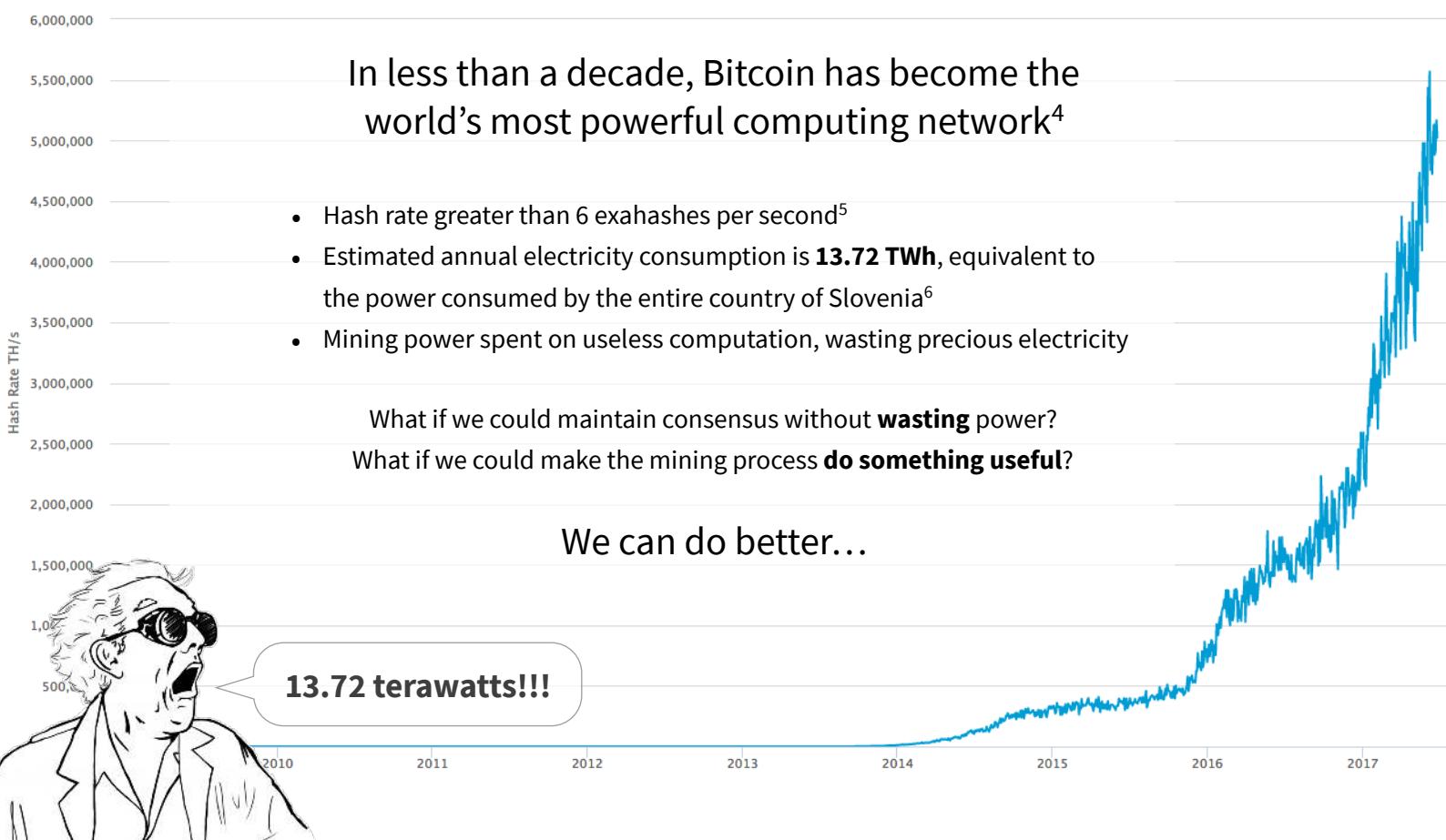


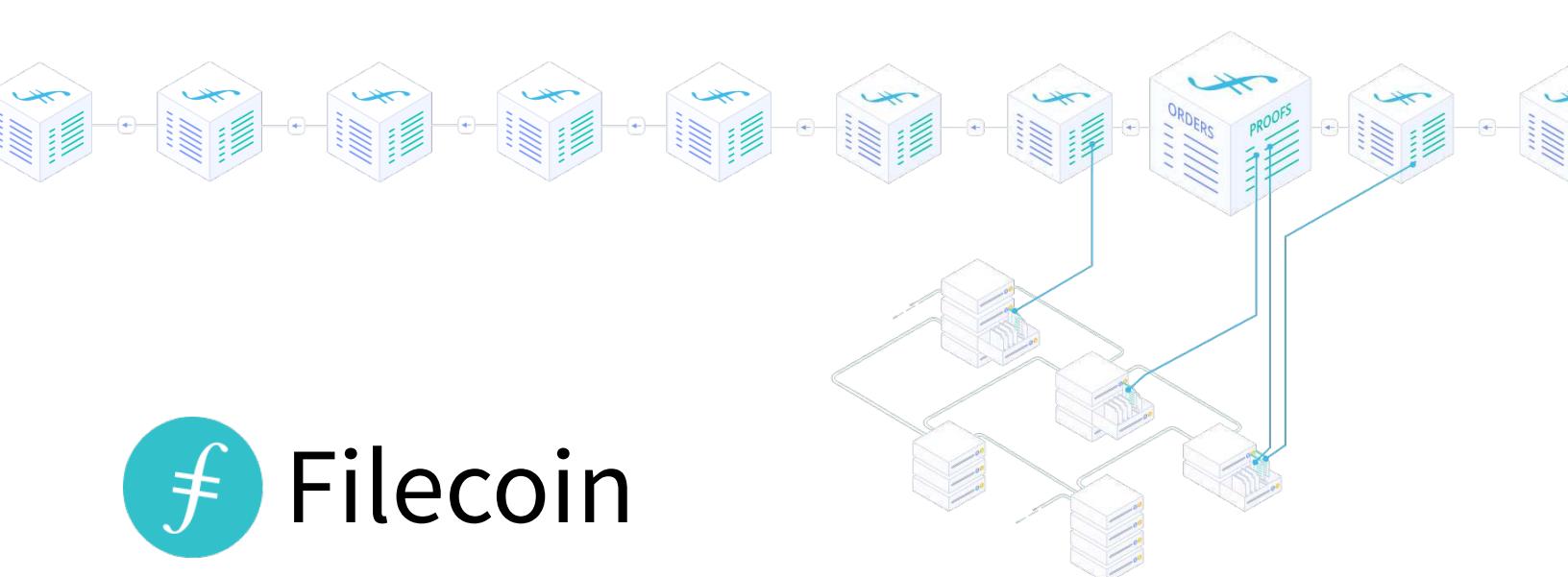
Mining Revenues

Year	Bitcoin		Ethereum	
	BTC	USD (EOY)	ETH	USD (EOY)
2012	2,520,000	\$ 34M	-	-
2013	1,314,000	\$ 959M	-	-
2014	1,314,000	\$ 411M	-	-
2015	1,314,000	\$ 559M	4,320,000	\$ 4M
2016	987,300	\$ 941M	10,512,000	\$ 84M
2017	630,720	\$ 1.5B	10,512,000	\$ 2.7B
TOTAL (since 2012)	8,080,020	\$ 4.4B	25,344,000	\$ 2.8B
WORTH TODAY	1	\$ 2,309	1	\$ 265
	16,422,188	\$ 18.6B	25,344,000	\$ 6.7B

For simplicity, mining totals do not include transaction fees or uncle rewards. Bitcoin mining started in 2008, we consider only from 2012 in this total. Ethereum totals do not include Genesis allocations. TOTAL calculated based on EOY price for each currency. WORTH TODAY calculated with prices on 2017-07-01. Data source: <https://www.coinmarketcap.com>.

Bitcoin Network Hash Rate





Filecoin

A decentralized storage network, powered by a blockchain and a token. Built by Protocol Labs.



Earn Filecoin for hosting files and mining

Mine Filecoin by putting your unused storage to work. Filecoin is a blockchain where mining requires storing files, instead of computing hashes. Use the Filecoin mining software to get paid for mining new blocks, processing transactions, storing files long term, or servicing retrieval requests.



Reliable storage at competitive prices

Clients can tune their storage strategy to suit their needs, creating a custom balance between redundancy, speed of retrieval, and cost. The worldwide Filecoin storage and retrieval markets make vendors compete to offer flexible options at the best prices.



Exchange Filecoin for tokens or fiat

Once the network launches, the Filecoin token can be traded on crypto asset exchanges and stored with various wallets. Miners and clients may exchange Filecoin for other currencies like ETH, BTC, USD, RMB, EUR, and more.



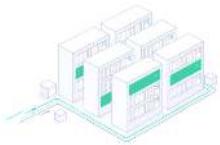
Cutting-edge tech x proven platforms

Filecoin is the culmination of years of cutting-edge research and development, featuring several important cryptography and blockchain inventions. This novel work builds on powerful and proven platforms. Filecoin uses **IPFS** for addressing and moving data, **libp2p** for ubiquitous and IoT friendly network connectivity, **IPLD** for interoperability with other blockchains, and **Ethereum** for its core blockchain functionality and smart contracts.

Filecoin Mining

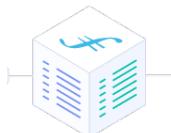
More storage, higher reward

Filecoin rewards miners for the storage they provide to the network. This happens in two parts. First, miners collect fractions of clients' payments over time, by continuously proving they are replicating the clients' data. Second, miners can collect block rewards for mining blocks, similar to Bitcoin and Ethereum. Storage rewards are proportional to the amount of storage miners contribute to the service.



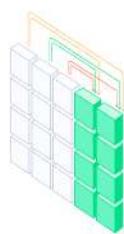
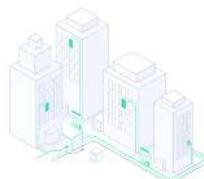
Storage as mining power

Filecoin is like Bitcoin, but miners amass hard drives instead of hashing computers. The amount of storage is what counts as power toward the Filecoin consensus, for both security and rewards. This is achieved through sequential *Proofs-of-Replication* over clients' data. This creates a valuable storage service as a byproduct of the mining process.



Resilience and self-healing

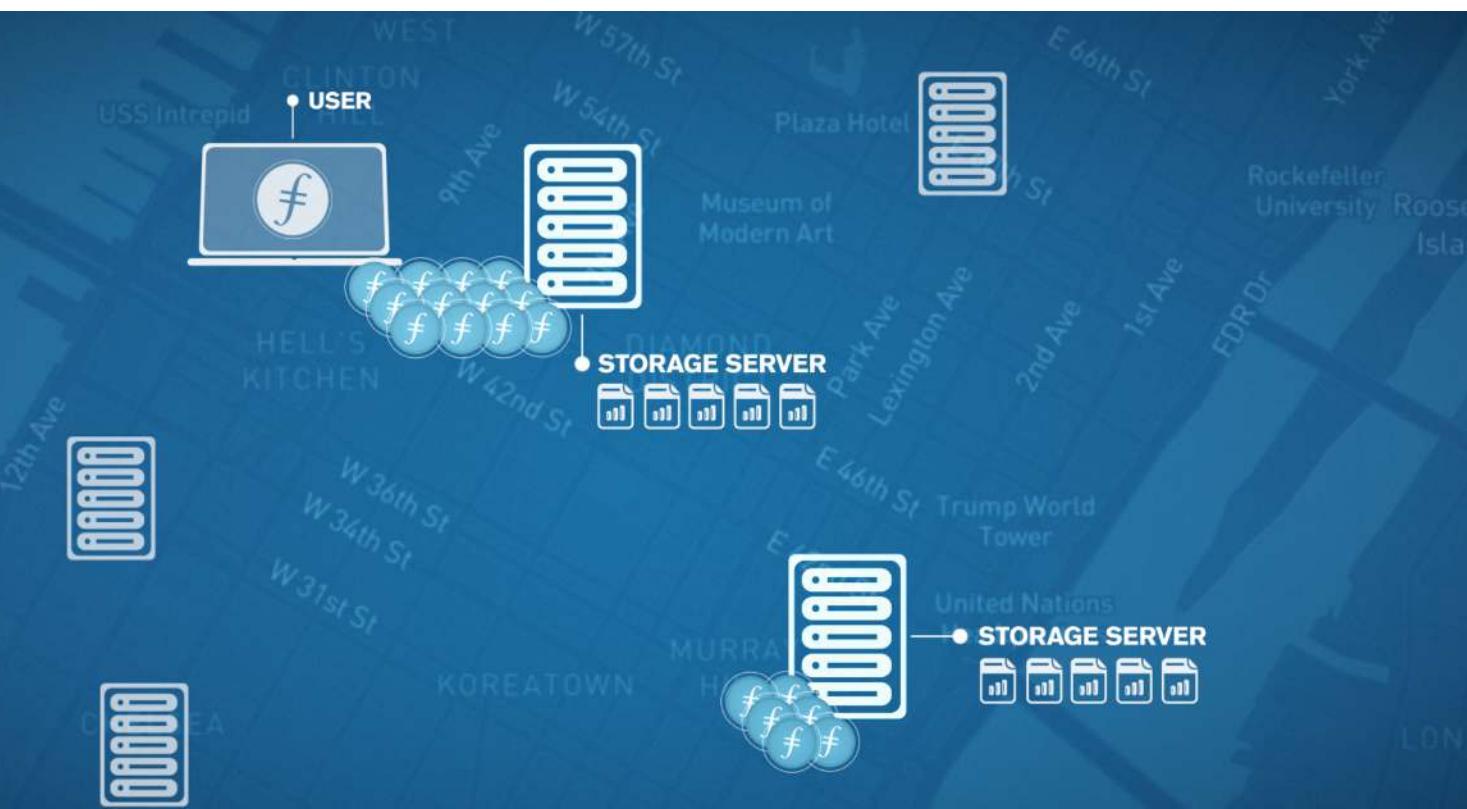
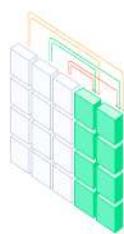
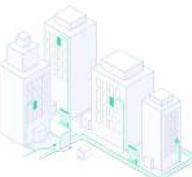
Data is stored using Erasure Coding (EC) and Information Dispersal Algorithms (IDA). This means smarter and more resilient replication, with lower storage overhead. These algorithms have parameters clients can tune, putting them in as much control as desired. Further, the network can detect missing nodes and re-allocate all the pieces they stored to other miners who can reconstruct them thanks to erasure coding. Thus, the Filecoin network self-heals!



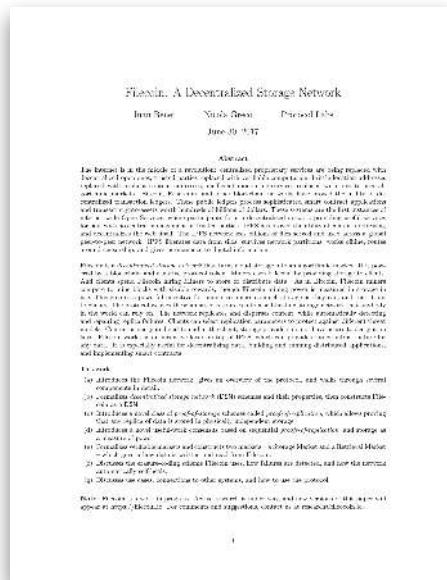
With these strategies, digital information can achieve new levels of permanence and persistence, even in the face of accidental outages or malicious attacks.

Faster distribution, higher reward

Miners collect strong rewards for distributing content to clients, and for doing so quickly. When a client wishes to retrieve some content, the miner who delivers it fastest will collect the rewards. This creates strong incentives for minimizing latency and maximizing bandwidth, effectively causing adaptive and fast CDN-like behavior. The strongest rewards will go to miners who are well-located in the network — i.e. close to many clients — such as ISPs, collocated servers, or even physical neighbors.



Technical Details



Filecoin: A Decentralized Storage Network

Juan Benet, Nicola Greco, Protocol Labs

Protocol Labs research over the last two years culminated in a new, significantly upgraded Filecoin protocol. We outline a few key inventions and features in the following sections. For complete technical details, please see the full technical whitepaper.

<https://filecoin.io/filecoin.v2.pdf>

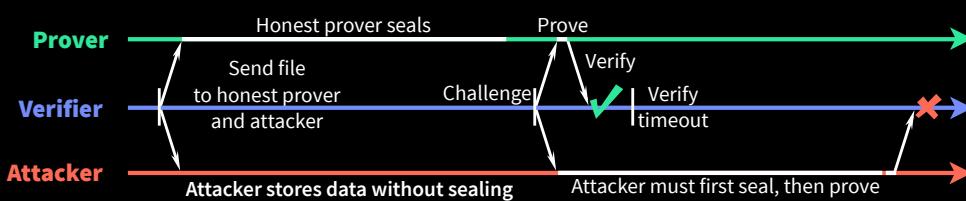
Full Node Storage

Full nodes store (a) the Filecoin Blockchain, which includes the latest Allocation Table, Order Book, and Transactions; and (b) storage sectors with the clients' data. The blockchain is far smaller than the storage sectors, and the cryptographic seal does not increase the size of the stored data, it has zero storage overhead!



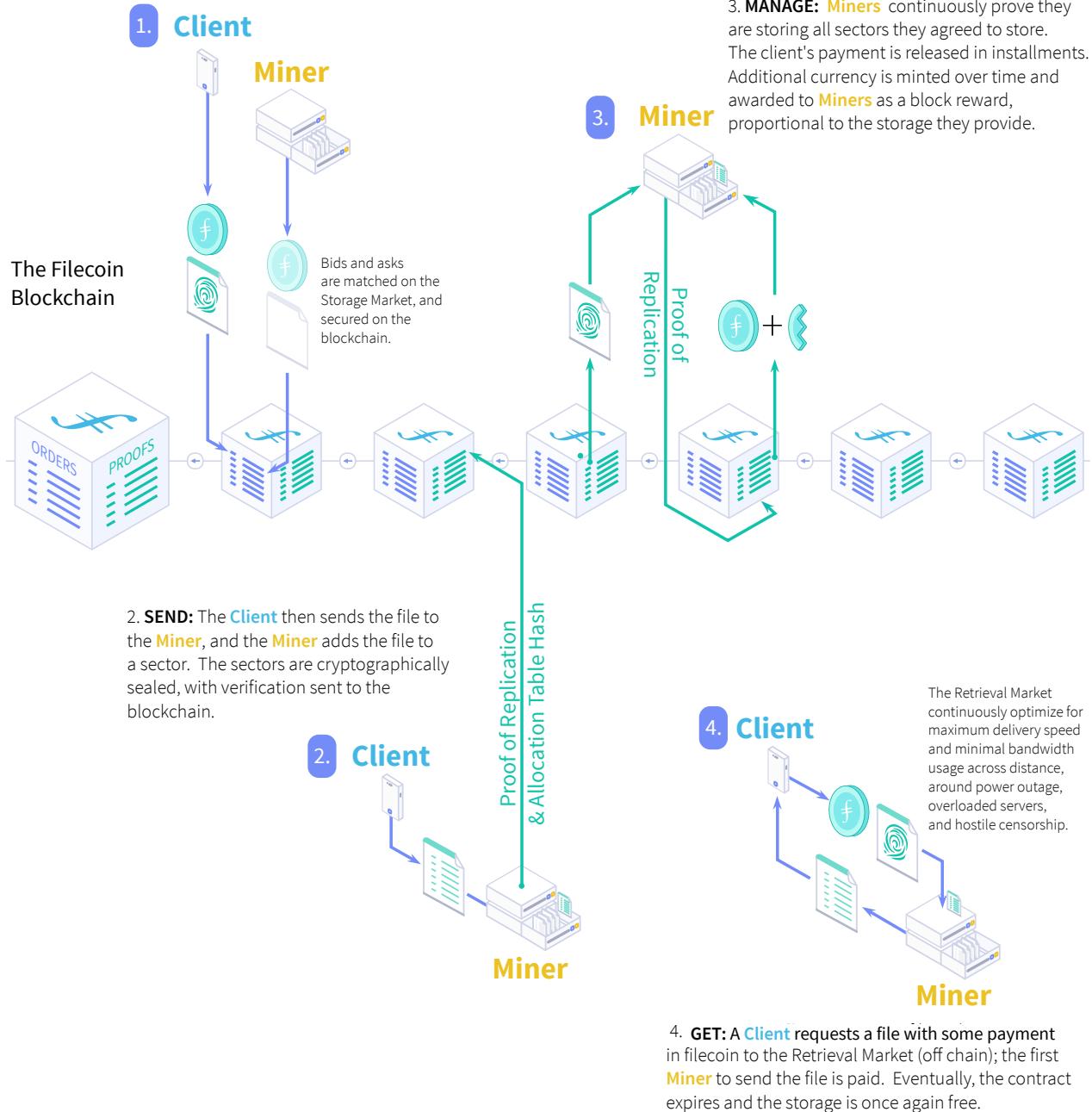
The Proof-of-Replication

The *Proof-of-Replication* functions cryptographically verify that every copy is stored independently, and allow this fact to be checked periodically. Each unique replica is generated by cryptographically sealing the data at the time of storage, using a per-replica encryption key. The *Seal* and *Proving* functions are chosen such that generating a new *Seal* cannot be performed fast enough to compromise the proof. These proofs also create a publicly verifiable record that the miner correctly stored the data as promised, and was online to serve it. The Filecoin Blockchain uses *Proof-of-Replication* in its mining process, to reward miners for storing files, to punish miners who fail their contracts, and to detect and recover any missing pieces.



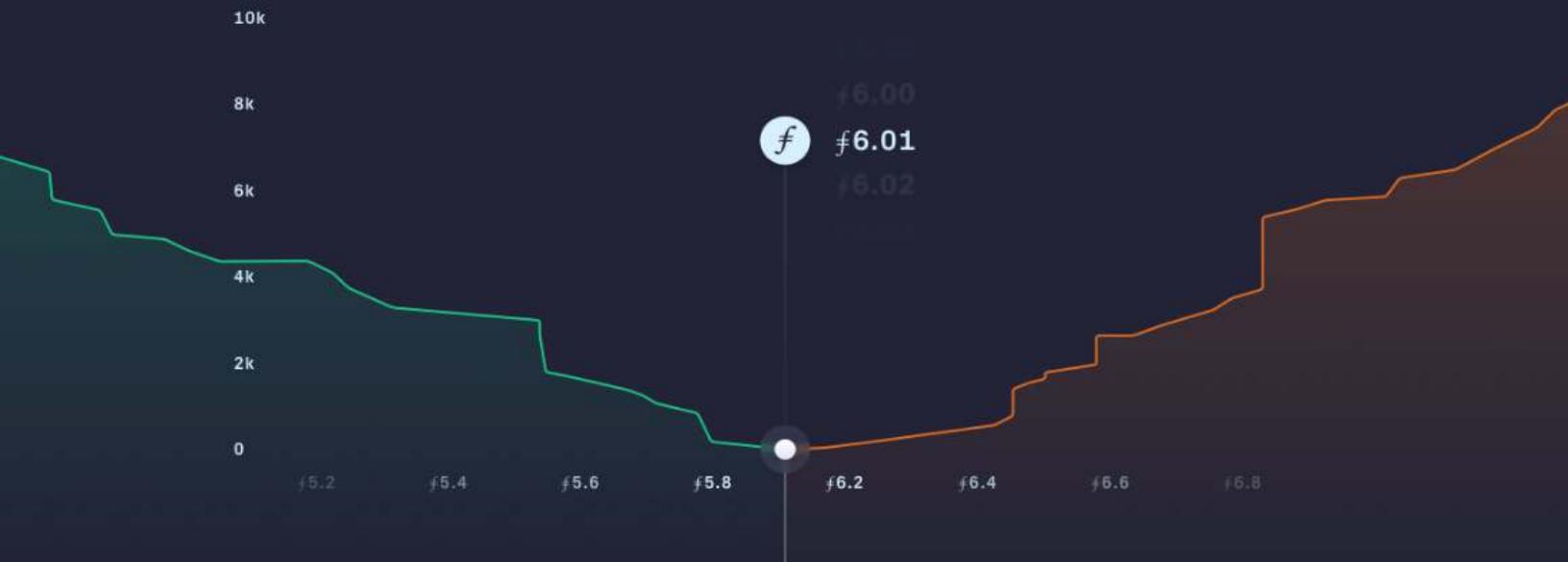
Filecoin: Lifecycle of a File

1. **PUT:** **Clients** send information about the file, storage duration, and a small amount of filecoin to the Storage Market as a bid. Simultaneously, **Miners** submit asks, competing to offer low cost storage. Deals are made in the Storage Market, on the blockchain.



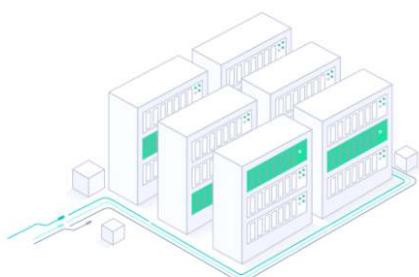
A Decentralized Market for Storage

The Filecoin network achieves staggering economies of scale by allowing anyone worldwide to participate as a storage provider. It also makes storage resemble a commodity or utility by decoupling hard-drive space from additional services. On this robust global market the price of storage will be driven by supply and demand, not corporate pricing departments, and miners will compete on factors like reliability, price, and reputation.



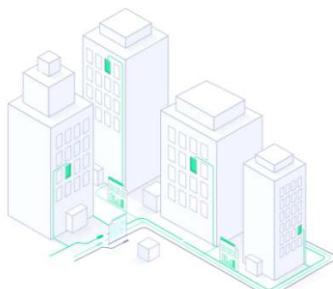
Storage Market

- On-chain *Bid* and *Ask* orders
- Global price discovery & optimization
- Enables storage provider competition to give clients the best prices
- Miners with large amounts of storage or operation cost advantages can earn significant rewards

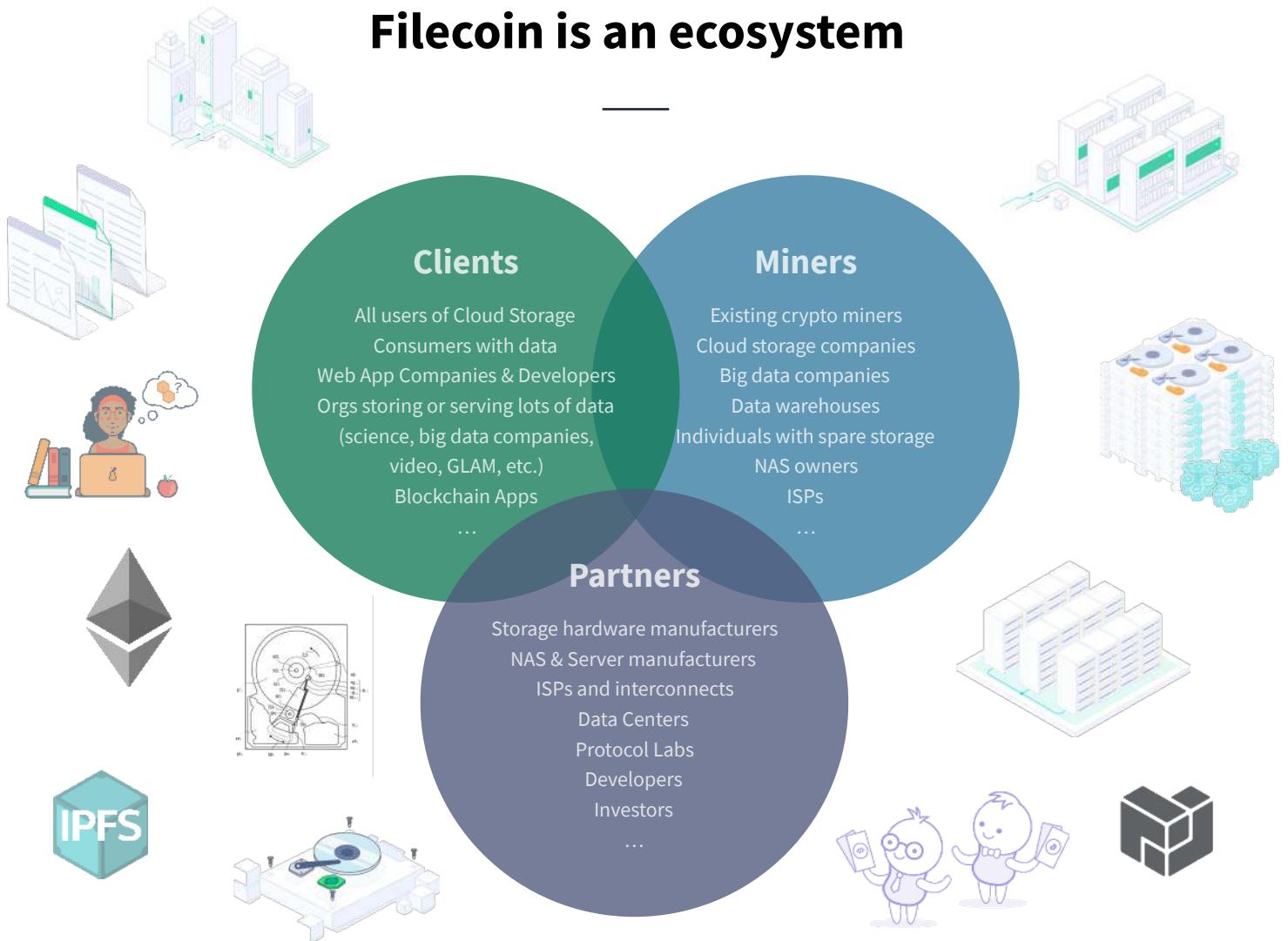


Retrieval Market

- Off-chain *Bid* and *Ask* orders
- Uses Payment Channels
- Minimizes request latency
- Small but well-located miners can earn significant revenue
- Regional hubs automatically optimize
- Hubs continue working through network partitions



Filecoin is an ecosystem



Filecoin is for clients

Filecoin offers many significant advantages over today's storage options: Significantly lower costs. End-to-end encryption at rest. Erasure coding for redundancy and self-healing. Resilience to failure and attack.

Clients can tune storage strategies to suit their needs, creating custom balance between redundancy, speed of retrieval, and cost. For example, clients distributing large volumes of data to users around the world (such as for media streaming) may choose to optimize for speed of retrieval.

Filecoin is for miners

Miners are the core service providers of Filecoin, and define the network. Miners will be diverse; lots of people and orgs will come together from all backgrounds and corners of the world. They will both compete and collaborate in the network.

The Filecoin network is designed to reward participants at multiple levels — from large scale data centers to local entrepreneurs with mining rigs that cover the last mile.

Miners who retain Filecoin tokens, which may appreciate in value as the network grows, are encouraged to collaborate to make the network as big and powerful as they can.

Filecoin is for partners, vendors, and investors

Filecoin network growth will yield opportunity for the whole storage ecosystem. Filecoin creates additional demand for hard drives and other storage hardware. Open source Filecoin mining software will come pre-installed on storage devices. ISPs, cloud storage providers, and data warehouses can participate both as miners, and as vendors to other miners.

Many companies and organizations will get more business or reduce their own costs thanks to Filecoin, its miners, and its users.



Filecoin is built with IPFS

They complement each other:
IPFS addresses and moves content, and
Filecoin is the missing incentive structure.

Learn more about IPFS:



The Next Internet Revolution

Juan Benet, TEDxSanFrancisco
<https://youtu.be/2RCwZDRwk48>



Decentralized Web: IPFS & Filecoin

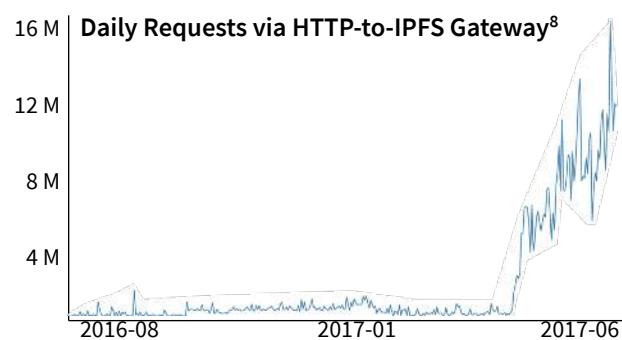
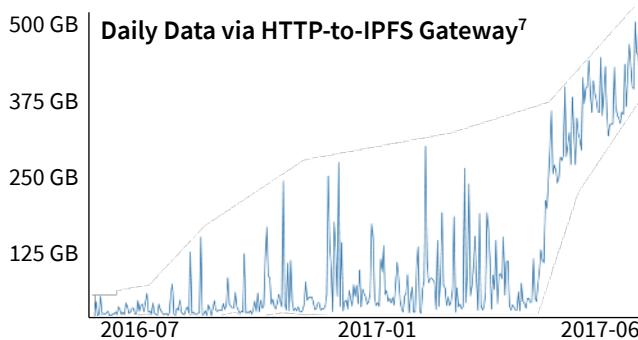
Juan Benet, Silicon Valley Ethereum Meetup
https://youtu.be/cU-n_m-snQ

5,000,000,000+ files on



The InterPlanetary File System (IPFS) is a next-generation protocol to make the Web faster, safer, decentralized, and permanent. Since the initial IPFS release in January 2015, it has gained strong traction in a variety of industries and organizations. Today, IPFS is a foundational technology for many applications in the blockchain industry. Over 5 billion files have been added to IPFS, spanning scientific data and papers, genetic research, video distribution & streaming, 3D modeling, legal documents, entire blockchains and their transactions, video games, and more.

IPFS and Filecoin are complementary protocols, and the adoption of the underlying IPFS protocol is a leading indicator of market demand for a faster, safer, decentralized storage service.



Example App: OpenBazaar

OpenBazaar is a fully peer-to-peer e-commerce platform where anyone can buy or sell things online, using Bitcoin or other crypto tokens. OpenBazaar is a full-featured app on top of IPFS, including: dynamic content, real-time encrypted p2p chat, crypto token payments, and (soon) a full mobile app.



Some IPFS Users



Blockchain Apps

these and many more



Archiving and Distributing Precious Data

from these organizations and many more

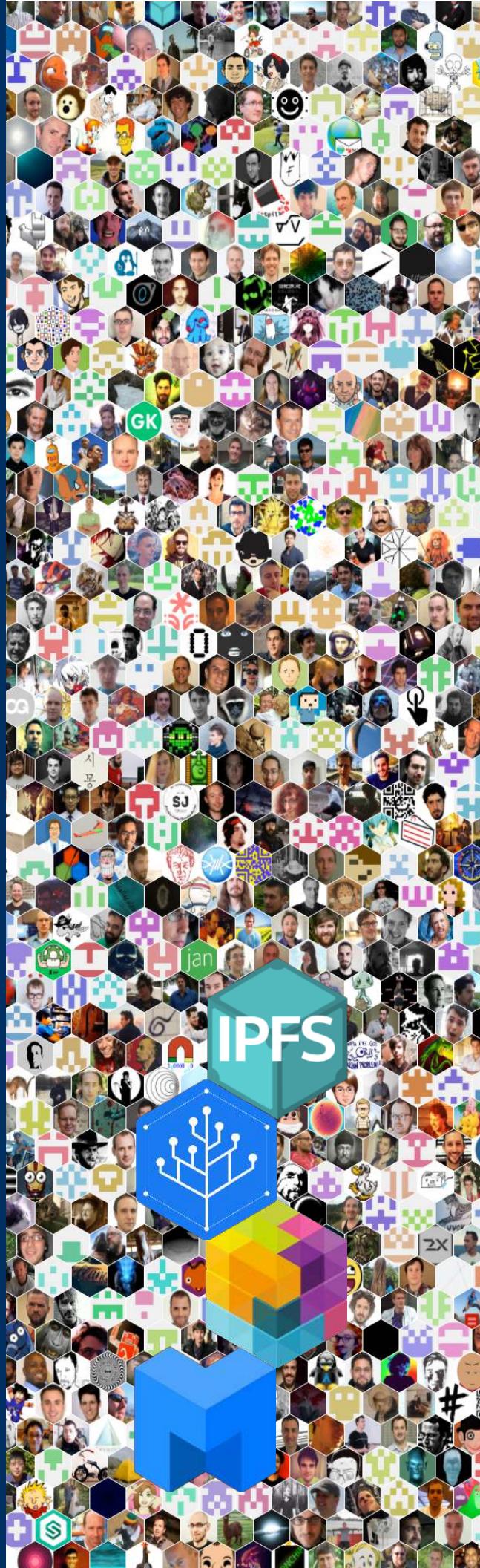
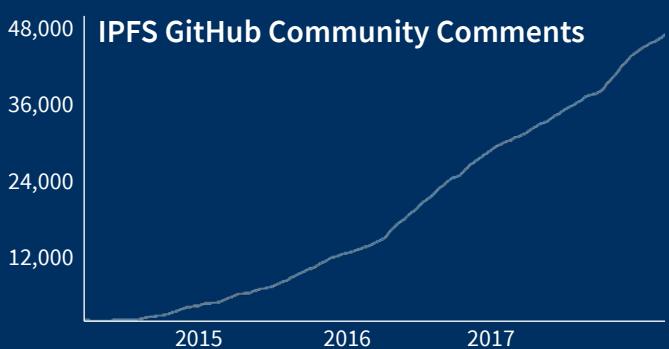
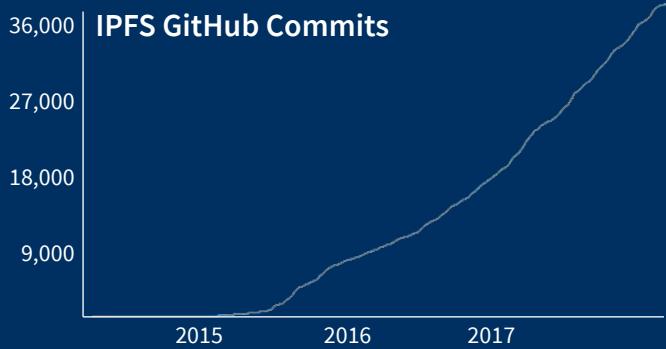
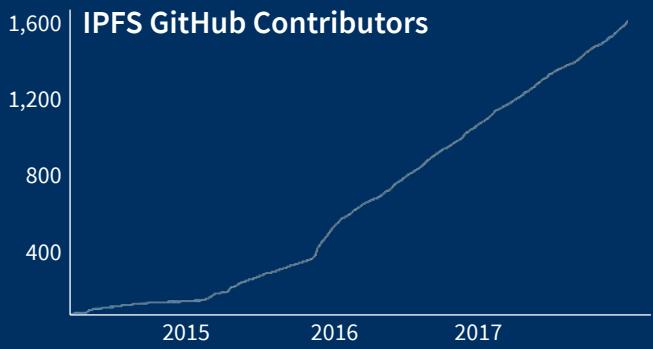


IPFS Open Source Community

The IPFS Project is a large community of open source contributors driven to decentralize the web. The community is made up of thousands of developers and users who have been working together for several years, building valuable and widely used software tools.

The same seasoned core developers of IPFS are also leading the design and development of Filecoin. The IPFS team has experience building ambitious software projects and coordinating thriving developer communities. A significant portion of the IPFS community plans to join the Filecoin network, building tools and applications on this new, exciting platform.

Join us!



Large Scale Value Creation

The Filecoin Network is designed as a decentralized storage network powered by a blockchain. It will create value in a number of ways, and the total impact of the network can be tremendous. Growth of the network will drive demand for the token. The more value created by the Filecoin Network, the more things people and organizations spend Filecoin on, and the greater the value and worth of the token.

Storage service use cases

Cloud Storage (*\$75B market size by 2021⁹*)

Filecoin will create a powerful and dynamic cloud storage service.

Decentralization (*new market*)

Filecoin is decentralized and trustless. It helps avoid relying on trusted parties, or vendors who keep your data hostage or try to lock you in.

Algorithmic Storage Market (*new market*)

Filecoin drives storage prices downward by encouraging competition from all providers, including newcomers bringing latent storage online.

Algorithmic CDN (*\$23B market size by 2021¹⁰*)

Filecoin optimizes content delivery, as an incented, auto-scalable, world-wide CDN.

File Contracts (*new market*)

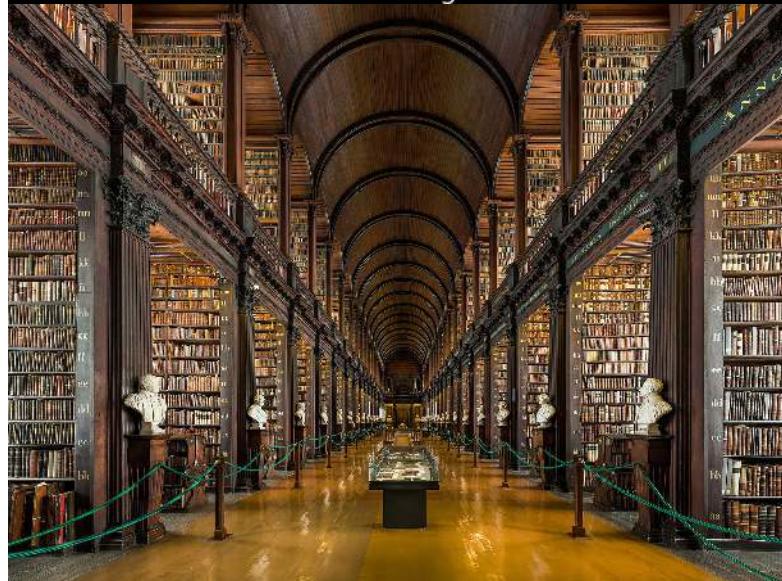
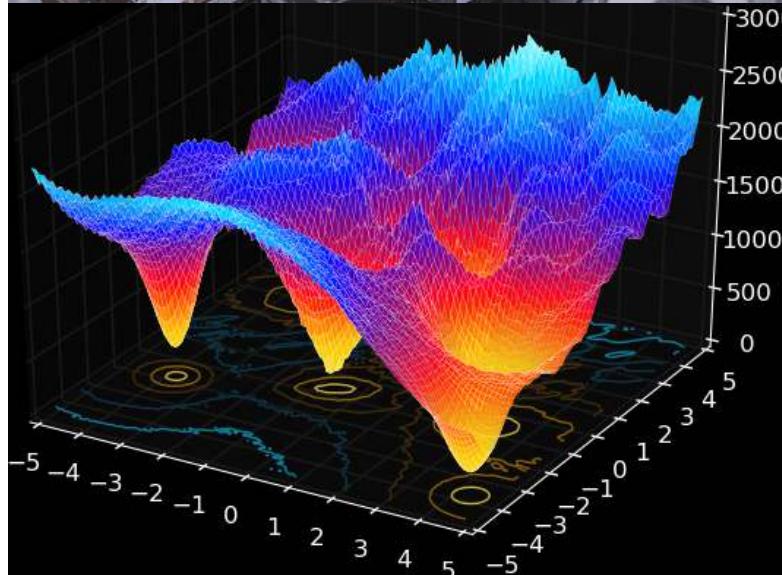
Filecoin can run sophisticated smart contracts that operate on large volumes of data, mediate valuable data transactions, and do to the data economy what Ethereum is doing to finance.

Data Exchange

Users can sell data on the network, facilitating data exchanges and markets.

Humanity's Data

Filecoin will store treasure troves of critically important public data, such as encyclopedias, open access scientific papers, creative commons data sets, historical documents, and literature.



Standard blockchain use cases

Market cap of Bitcoin: \$43B¹¹, Ethereum: \$26B¹²

Payments

Like any other blockchain, Filecoin tokens can be transferred between users.

Time-stamping

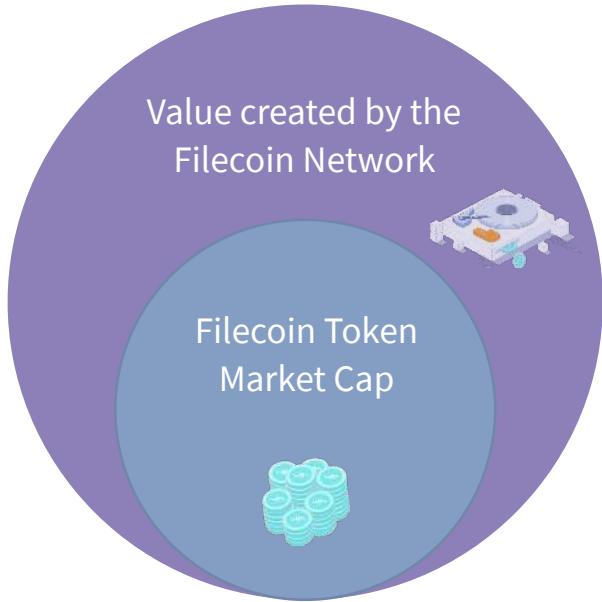
With the ability to store large amounts of data for long periods of time, Filecoin will be the ultimate time-stamping service.

Store of value

Filecoin can be a decentralized, free store of value, backed by something of real utility: a cloud storage service.



The Filecoin Token



What is the filecoin token?

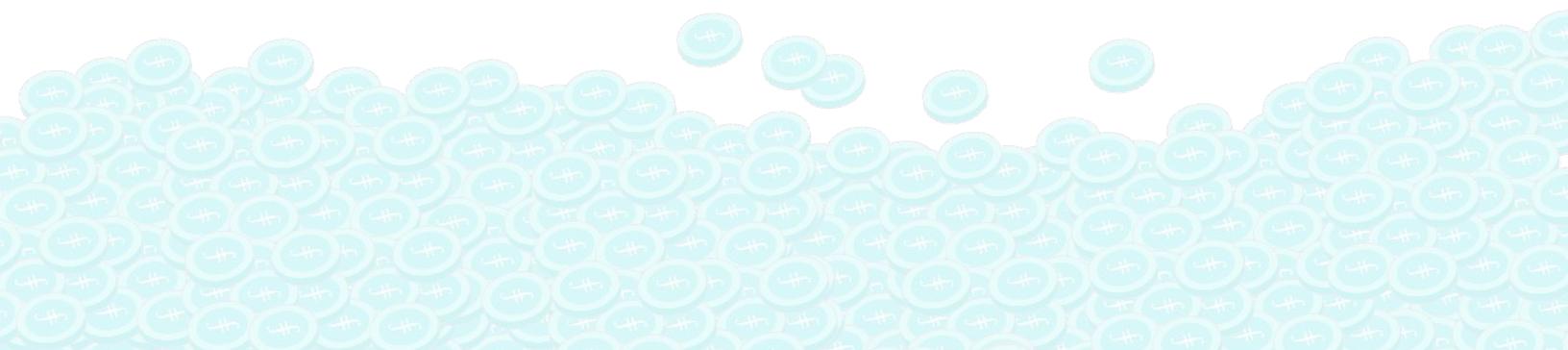
The filecoin token is the native crypto token of the Filecoin network, similar to Bitcoin and Ethereum. Filecoin is used to pay for storage, retrieval, and transactions in the network.

Monetary Policy

- **Limited Supply**, with total set by the token sale.
- **Minting** by block reward as in Bitcoin.
- **Genesis allocation** to fund creation, development, deployment, and reward creators.
- **Backed by useful service**: Demand for the storage service drives demand for the token.

Filecoin price and the cost of spacetime

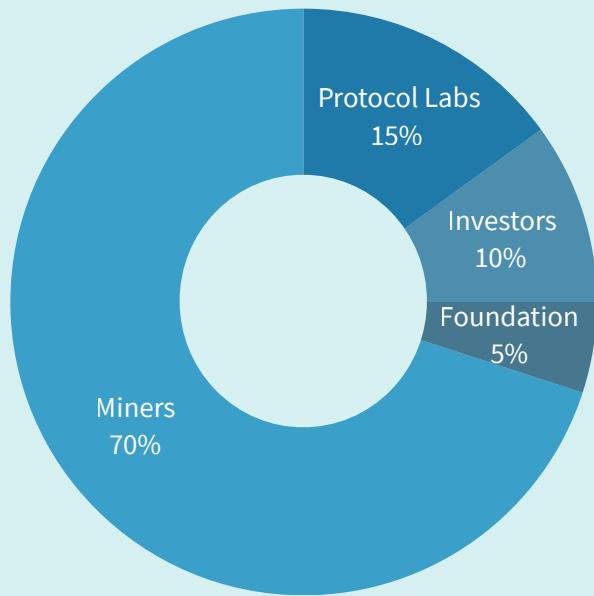
Filecoin will be **priced by markets and exchanges**, as any other crypto token. **Spacetime** is what we call *storage space over time*. It is the good or service sold by miners. The filecoin price floats above the price of storage: Miners list their spacetime storage prices denominated in filecoin. As the network grows — gathering more storage and clients — the total amount of filecoin remains limited, creating upward price pressure.



Filecoin Token Allocations

The Filecoin Token will be distributed to the major participating groups in the Filecoin Network: **Miners**, **Protocol Labs**, **Investors**, and the **Filecoin Foundation**. These groups are critical to the creation, development, growth, and maintenance of the network. This allocation is written into the protocol itself and the Filecoin blockchain's **Genesis block**. Allocations are vested for many years.

Filecoin Token Supply

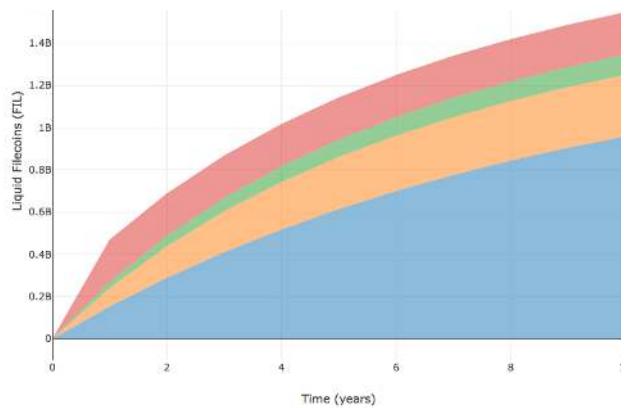


- **70% to Filecoin Miners (*Mining block reward*)**
For providing data storage service, maintaining the blockchain, distributing data, running contracts, and more.
- **15% to Protocol Labs (*Genesis*)**
For research, engineering, deployment, business development, marketing, distribution, and more.
- **10% to Investors (*Genesis*)**
For funding network development, business development, partnerships, support, and more.
- **5% to Filecoin Foundation (*Genesis*)**
For long-term network governance, partner support, academic grants, public works, community building, etc.

Token Release Schedule

- **Filecoin Miners:** Asymptotic vesting, similar to Bitcoin
- **Protocol Labs:** Linear vesting, 6 years
- **Foundation:** Linear vesting, 6 years
- **Investors:** Linear vesting, per block

(a more detailed page with the numeric values and an interactive version on the web will be released soon)



Protocol Labs

Protocol Labs, Inc. is a U.S. company building foundational internet infrastructure technology. Founded in 2014 by Juan Benet, it operates as a research, development, and deployment lab for network protocols.

Protocol Labs leads groundbreaking internet projects, such as IPFS, the decentralized web protocol; libp2p, a modular network stack for peer-to-peer apps and systems; CoinList, a token sale and investment platform; and Filecoin, a decentralized file storage network and protocol token. Protocol Labs works openly, and is focused on the creation of value at a massive scale.



Team and Community

The Protocol Labs core team holds deep expertise in distributed systems, cryptography, networks, blockchains, security, fintech, economics, software engineering, and open source. The team's experience includes the top CS universities, top tech and finance companies, and top systems and blockchain projects.

Over 1,700 individuals and institutions across the globe have contributed to open source projects led by Protocol Labs. We will continue to foster this remarkable community. We expect to use RFPs with rewards and other systems to organize large scale contributions.



Appendix

1. “More data will be created in 2017 than the previous 5,000 years of humanity” via App Developer Magazine. <https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity>. Retrieved July 12, 2017
2. Cisco Global Cloud Index: Forecast and Methodology, 2015-2020. <http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf>. Retrieved July 12, 2017
3. “Bitcoin is 100 times more powerful than Google” via Cryptocoins News. <https://www.cryptocoinsnews.com/bitcoin-100-times-powerful-google>. Retrieved July 12, 2017
4. “The World's Most Powerful Computer Network Is Being Wasted on Bitcoin” via Gizmodo. <http://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-504503726>. Retrieved July 12, 2017
5. “The Bitcoin Network's Hashrate Now Exceeds Six Exahash” via bitcoin.com. <https://news.bitcoin.com/bitcoin-hashrate-six-exahash-july-1/>. Retrieved July 12, 2017
6. Bitcoin Energy Consumption Index. <http://digiconomist.net/bitcoin-energy-consumption>. Retrieved July 12, 2017
7. Retrieved from IPFS internal monitoring July 6, 2017
8. Retrieved from IPFS internal monitoring July 6, 2017
9. “Cloud Storage Market worth 74.94 Billion USD by 2021” via <http://www.marketsandmarkets.com/PressReleases/cloud-storage.asp>. Retrieved July 12, 2017
10. “Content Delivery Network (CDN) Market worth 23.22 Billion USD by 2021” via <http://www.marketsandmarkets.com/PressReleases/cdn.asp>. Retrieved July 12, 2017
11. Cryptocurrency Market Capitalizations: ETH, <https://coinmarketcap.com/currencies/ethereum/>. Retrieved July 12, 2017
12. Cryptocurrency Market Capitalizations: BTC <https://coinmarketcap.com/currencies/bitcoin/>. Retrieved July 12, 2017

