OPACITY
Private file sharing and secure cloud storage, powered by crypto

WHITE PAPER

Private cloud storage | Crypto enabled for privacy | Competitive cost through Opacity payments | Easy to use for non-crypto users

POWERED BY

CRYPTO

Opacity

PRIVATE FILE SHARING AND SECURE CLOUD STORAGE, POWERED BY CRYPTO

White Paper

Private cloud storage ◆ Crypto enabled for privacy ◆ Competitive cost through Opacity payments ◆ Easy to use for non-crypto users

ABSTRACT: Opacity.io provides completely private cloud storage. By using a utility token for the purchase of cloud storage, regular users are able to enjoy full privacy of their data. Unlike other service providers, Opacity does not require personal identification information. Opacity stores no information on its users, and allows people to store their private files, photographs, legal documents, and any personal data, with assurance that their personal data stays personal.

OPACITY

This Document is not a Prospectus

This document does not constitute nor imply a prospectus of any sort. No wording contained herein should be construed as a solicitation for investment. Accordingly, this whitepaper does not pertain in any way to an offering of securities in any jurisdiction worldwide whatsoever. Rather, this whitepaper constitutes a technical description of the functionality of the Opacity product and deployment. Opacity is a privately held company and this whitepaper does not offer any type of token or share in the Opacity company.

CONTENTS

EXECUTIVE SUMMARY

Opacity.io is a cloud storage provider with one major difference: privacy. Privacy is a basic human right, supported by the US constitution. Yet with the rise of digital property, governments have exercised flexibility in what they consider protected by privacy law, and many people have increasingly been concerned about the security and privacy of materials stored with cloud storage companies such as Dropbox, Google, and others.

Small businesses, individuals, and enterprises want to keep their data private. Opacity protects people's basic rights and provides cloud storage to anyone through its Opacity token. The token can be purchased on a crypto exchange and then used to purchase data storage plans that are completely private, and can be accessed only by the purchaser with the private key.

Unlike other service providers, Opacity does not require personal identification information. Opacity stores no information on its users, and allows people to store private information, such as company secrets, intellectual property, personal photographs, legal documents, and family moments, with assurance that their personal data stays personal.

MARKET

The cloud storage market today is dominated by large companies such as Amazon, Rackspace and Google, as well as some smaller cloud providers such as Dropbox and smaller private companies in different geographies. Apple and Microsoft push users to store their documents and materials on their cloud storage systems rather than locally on their computers. All of these systems require full identification of the individual, and given the abundance of security breaches, users are concerned about the privacy and security of their private data, whether that is personal information or legal and company proprietary data.

Two privacy centric storage options, Mega and Sync, are available, however, they require credit cards and store user data. While the data itself might be private, as long as companies store the data somewhere, it is susceptible to hacking. Crypto-based solutions have come on the market, including Siacoin, Storj and Filecoin. Filecoin has not yet delivered a product, despite raising $200M, and Storj and Siacoin are too difficult to use for the average user. By combining the privacy offered by cryptocurrency with the fast delivery time of a for-profit venture, Opacity provides the best of both worlds.

OPACITY TOKEN

The Opacity token is the key to privacy on the Opacity network. While it will be possible to purchase full-priced storage with a credit card on the network, privacy is enabled by the use of the tokens. Opacity minted a limited supply of 130 million OPQ tokens, available on several cryptocurrency exchanges. Similar to a voucher, each OPQ token entitles the holder to 1 year's worth of 64 GB of storage, with absolutely no need to reveal any private information.

SOLUTION

The Opacity network is up and running today. Within just 3 months, Opacity.io has created a fully-functional private cloud storage network, available to anyone through the OPQ token. The system now runs on proprietary servers managed by Opacity, and over time the network will expand to provide a resilient, global privacy-oriented system.

BACKGROUND/INDUSTRY

MISSION

- Opacity preserves every person and business' right to digital privacy by providing private cloud storage and secure private file sharing.

THE INDUSTRY

For many individuals and companies, the biggest concern in using cloud-based services is security and privacy. Security breaches, identity theft and theft of private data have become daily occurrences.

While many cloud services offer a variety of security add-ons, they are still subject to a variety of vulnerabilities, and they aren't built-in by default. Furthermore, no matter which service is used, these subscription providers always retain the user's personal information and credit card data for the convenience of monthly billing. The trade-off for this convenience is that hackers and other entities can find out who accounts belong to, and credit card data will always leave a trail to where the data is stored. While many people don't require the high-level privacy of zero credit card trail, options are limited for those who do, or for those who simply want to maintain their right to privacy. Whether you want to keep your trade secrets out of the hands of competitors or foreign players, or whether you just want your family photo album to remain completely private, today's centralized cloud providers offer very little in the way of fully private and secure storage that belongs only to the owner.

The cloud storage market today is dominated by large companies such as Amazon, Rackspace and Google, as well as some smaller cloud providers such as Dropbox and smaller private companies in different geographies. Apple and Microsoft are increasingly aggressive in pushing users to store their documents and materials on their cloud storage systems rather than locally on their computers. While this may appear as a good backup service, ultimately users are sacrificing their privacy to big companies, many of which have been shown to be sharing their data freely with governments, without the knowledge of the users.

As a response to corporate solutions, the crypto industry has been offering a number of alternatives, notably as Storj and Siacoin, which have delivered distributed, anonymous networks.[1] These networks were designed both to resolve privacy issues, and to be more secure than other networks following major data breaches. While these are good alternatives for some users, they are generally hard to use and require more technical knowledge than the average user wants to invest. Other fog and mesh solutions in the cryptosphere have simply failed to deliver at all.

Notably, crypto-based solutions are community owned and managed. While this may be an advantage in the long-term, it does not offer much of an incentive for token holders or investors in these foundation-run organizations, and it does not offer a centrally responsible entity that takes care of the network. While hackers and open source community members may feel comfortable with a foundation or community-owned entity, regular users want to know someone is in charge of the network. Users want to have someone to call when something goes wrong, an enterprise representative if they want custom solutions, etc. For most users, the system has to be seamless to use and offer customer support and accountability for the network.

---

[1] https://medium.com/bitfwd/what-is-decentralised-storage-ipfs-filecoin-sia-storj-swarm-5509e476995f

CHALLENGES

- Security breaches stealing people's personal information are becoming an increasing concern.

- Identity theft is one of the most common malicious uses of identity data, where people's passwords and credit cards are stolen and reused. Any online service provider that retains a database of users is susceptible to such threats.

- Increasingly, identity theft can lead to physical threats, even the dispatch of armed police officers to someone's home or business.

- Large cloud service providers collect information on users, and people are becoming aware that their privacy is important.

- Companies and individuals have the right to keep their information and identities private.

- Crypto-based solutions for file storage are not designed for regular users.

- Regular users shy away from crypto-based solutions because there is no authority to take responsibility for the network.

- The prices for storage are high because of the grip that large companies have on the market. The true price can be dramatically lower.

SOLUTION

PRODUCT

Opacity.io is a cloud storage provider with one major difference: Privacy. Privacy is a basic human right, supported by the US constitution. Yet with the rise of digital property, governments have exercised flexibility in what they consider protected by privacy law, and some people have increasingly been concerned about the security and privacy of materials stored with cloud storage companies such as Dropbox, Google, and others.

Unlike other storage solutions, Opacity relies on client-side encryption to ensure that only the owner of the files has access. Backend services maintain zero knowledge regarding the association between accounts and file uploads, such that a file cannot be associated with an account without the private key.

Small businesses, individuals and others want to keep their data private. Opacity protects people's basic rights and provides cloud storage to anyone through its Opacity token. The token can be purchased on a crypto exchange and then used to purchase data storage plans that are completely private, and can be accessed only by the purchaser with the private key.

Unlike other service providers, Opacity does not require personal identification information. Opacity stores no information on its users, and allows people to store whatever they want, whenever they want, with assurance that their personal data stays personal.

Opacity's code is fully opensource, and a code review license can be found at https://www.opacity.io/code-review-license.

OPACITY CAPABILITIES

Opacity 1.1 is available in the summer of 2019 with the following capabilities:

- Payment privacy via OPQ token
- Account private access via private key
- File sharing via public key
- Client side encryption
- Metadata encryption and privacy
- API for developers

- Folders
- Desktop Sync Application
- Credit card payment

The Architecture section describes these capabilities in detail.

Additional capabilities in the roadmap include:

- Larger storage plans
- Streaming downloads
- File previews
- Multi-file delete
- Multi-file download
- Renew subscription
- Upgrade plan
- Rename files
- File versioning
- File search
- Mobile applications for iOS and Android
- Decentralization

SERVICES

Currently, Opacity provides basic file storage services of 128 GB, 1 TB and 2 TB (coming soon). Over time, Opacity will add other value-added services. These services will increase the utility of the OPQ token, and provide more utility for token holders as they can purchase services privately and securely.

Following are services that Opacity will be able to offer in the near future:

- Geographically-located services, for individuals and companies that prefer to store (or are required to store) files in a particular geography. This may include avoiding a particular geography, as per configuration.
- Custodianship services. By default, the only way to access the file storage is by the individual with the individual's private key / seed passwords. If that is lost, there is no recovery. Custodianship services would allow people to purchase the

ability for Opacity to store another copy of the passcode, accessible with specific proofs by the individual.

- Enterprise storage services, for organizations with larger needs than 1 or 2TB.

- Independence-assured backup and redundancy. This option allows users to purchase redundant systems (backups) that are guaranteed to be with different providers in different geographies. This service ensures users that even in the case of force majeure, their files are stored safely in another location.

- Dedicated servers.

- Shared storage for workgroups and teams.

- Connectivity to business applications (replacing Microsoft or other type of automatic sharing systems).

- Search capabilities.

ZERO KNOWLEDGE

Zero knowledge means that absolutely nobody has access to your data other than you, and that, in fact, nobody even knows or can prove it is yours. When it comes to online cloud services, zero knowledge is a bit tricky. Most people want some form of assurance that they will be able to recover their files in case anything happens, and as a result, most cloud storage providers save the login information somewhere. In other words, that information can be accessed by the cloud service provider, or by someone with the phishing skills to get enough information to pose as the owner of that data.

Moreover, no matter what cloud service provider you use, subscription services require a payment method, and as soon as you give out your credit card information for monthly billing, that information is stored with the cloud provider, plus, of course, your credit card company knows, and as we all know today, credit card data is regularly sold to third parties.

In other words, to get truly private cloud services, it's necessary to pay in a method that can't be traced by anyone, and that doesn't require recording of any of your personal identification information.

In order to accomplish this, the Opacity network uses the OPQ token as a verified payment method. The tokens can be purchased on cryptoasset exchanges and using the token requires absolutely no proof of identity, just like cash payments. Opacity users get a private key (seed passcodes) to unlock their cloud storage, and that's it. The private key is not stored anywhere else, and 100% of the security of that passcode is with the user.

No authority can search the Opacity network, and it's impossible for anyone except the owner with the passcode to unlock the storage. When using the OPQ token, there is no record of the transaction on a credit card or PayPal account. Zero-knowledge, in this case, means that there is no trace of the purchase. Just like purchases made with cash, purchases made with the OPQ token are not attributable to any particular person.

This system is not for everyone. If the passcode is lost, Opacity does not store it and the files can never be recovered.

CLOUD PROVIDER

In the initial phase, Opacity utilizes select major cloud storage providers. Over the coming months, agreements will be implemented with a variety of storage providers, to ensure file storage is not dependent on one entity. To ensure privacy and ensure there are no regulatory issues, Opacity considers it essential to have agreements and file storage with companies in multiple jurisdictions. While most countries recognize people's right to privacy, laws are subject to change and Opacity will ensure that its users have privacy under any circumstances.

Over time, Opacity will expand its file storage capacity to also incorporate server farms that ensure privacy. The Opacity Partner Program will allow service providers to partner with Opacity for provision of storage at private server farms. Partners will be screened for eligibility in the program. This extra layer of private storage will ensure that Opacity is robust and not subject to any one large provider of storage. Users of the Opacity network who choose redundant file storage capabilities will be ensured that their files are backed up on systems that are completely independent of one another.

PAYMENTS AND OPQ TOKEN

The platform launched with the ability to purchase with the OPQ token, which is available on the following exchanges:

- KuCoin
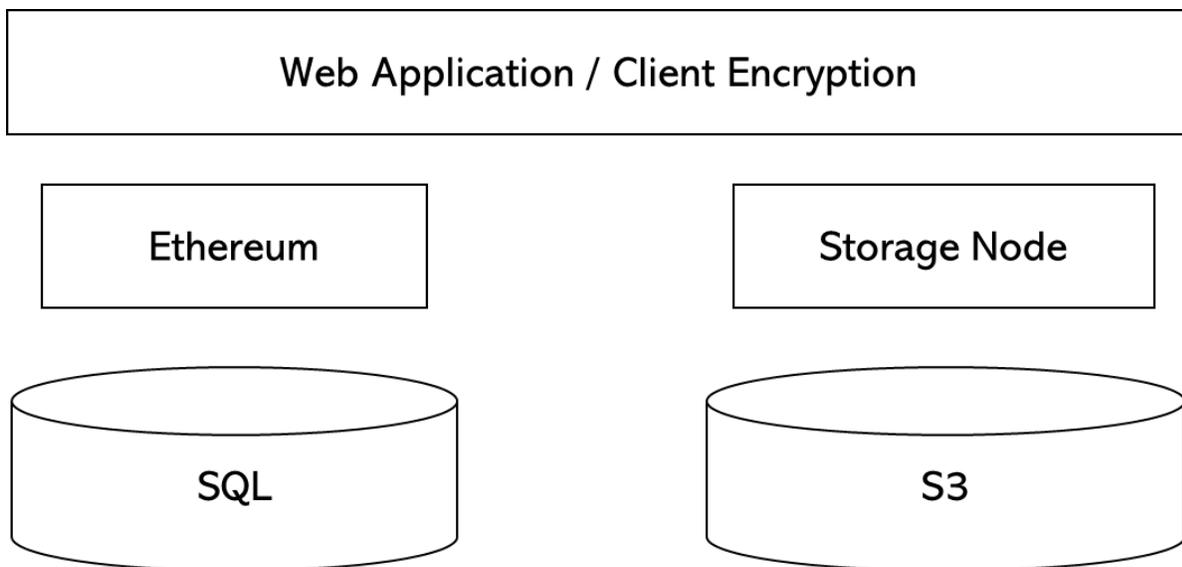- Mercatox
- Other exchanges will follow.

Purchase of file storage is guaranteed at the fixed rate of 1 OPQ per 64 GB of storage. Current models are for 128 GB or 1 TB of storage, and other options will be added.

Under the launch strategy, 1 OPQ purchases 64GB of storage. Based on the current pricing, this makes the Opacity offering much less expensive than others, but that proportion can

change depending on the OPQ price and market changes. Over time, market prices for storage generally decline. To counteract the effect of inflation and maintain a steady token value, Opacity reserves the right to change the storage peg of the OPQ token value to 1 OPQ = 128GB or higher. Initially, the team will be responsible for determining the adjusted storage quantity, but eventually, it is intended to adjust automatically based on network criteria.

Payment by credit card will be available in Q3 2019. Credit card purchase is at the market rates for storage (full price rather than the exchange rate for using OPQ). While we destroy all personal information after the initial payment for the storage, the transaction by credit card means that the purchase is not fully private. Opacity also holds the information for a certain amount of time to prevent fraud.

ARCHITECTURE / TECHNOLOGY

```
┌─────────────────────────────────────────────────────────┐
│          Web Application / Client Encryption             │
└─────────────────────────────────────────────────────────┘

   ┌──────────────────┐          ┌──────────────────┐
   │     Ethereum     │          │   Storage Node   │
   └──────────────────┘          └──────────────────┘

   ⎛                  ⎞          ⎛                  ⎞
   │       SQL        │          │        S3        │
   ⎝                  ⎠          ⎝                  ⎠
```

The Opacity team is made up of a group of technical experts that have designed a system architecture and backend that will ensure both ease of use and a high level of security and privacy for file storage and services.

ACCOUNT CREATION

Account creation is designed to be as simple as possible, and is designed to be fully anonymous. Users are completely responsible for their own private keys, and no private key or mnemonic information is accessible by Opacity.

Users:

- Download their mnemonic 12-word passphrase
- Receive their private key
- Pay with the Opacity token, through a one-time wallet

The one-time wallet is used only for the tokens paid for the storage for that particular wallet. Top-up will be available in the future by using the private key to log in.

Privacy:

- No private keys are stored.
- Opacity uses the SHA-256 Hash function proven for other cryptocurrency projects
- The primary key for the account access is the Account ID, which is derived from the public key of the user's private key, via the sha256 hash function.

PAYMENT PROCESS

As an ERC-20 token, OPQ tokens are fully anonymous and cannot be traced to specific users. When using the OPQ token for payment, the system is 100% private and no user information is available at any time to Opacity. Likewise, because Opacity cannot access any of the user files, there is no way the company can have any clues to the identity of its clients.

If the user chooses to use credit cards for purchase of the Opacity storage, the credit card information is erased following the purchase of the storage, once the payment is fully cleared to prevent fraud. However, the user is not fully private, because the credit card company will have a record of the purchase, as will Stripe, the third-party credit card processor for Opacity. Opacity does not store any information about the credit card or users.

ENCRYPTION

Encryption is enforced on all files, file handles, and metadata about the files. Through use of encryption, it is impossible to access any information about the files or file structure, nor can someone without the private key access the files themselves.

The encrypted files are then stored in chunks, so that each part of the file is separately stored and encrypted.

- Highlighted feature: For streaming video and audio, it is possible to recover each part of the file separately, decrypt the file and stream without downloading the entire file. This feature results in superior performance of streaming video, audio, and game applications, which require retrieval of large files.

Without the private key for the files, none of the parts of the files can be read. Similarly, all file handles, file structures and metadata are encrypted.

Symmetric encryption is used for files, file handles, and read files. Asynchronous encryption is implemented for file modification.

STORAGE

The initial release of the Opacity network is through Amazon's AWS system. Through 2019 and 2020, the team will actively seek additional partners for the distribution of the storage capabilities across multiple cloud storage providers for maximum security and elimination of any possible points of failure or jurisdiction requests of storage clients.

Storage of files is done after the files are divided into 5MB-10MB chunks, which are encrypted and impossible to understand without the private key and the other chunks belonging to the files.

The architecture is designed for decentralized storage and decentralized services. The file system is designed for further decentralization towards the capacity to utilize private storage nodes in the future.

METADATA

All metadata associated with files is stored separately from the files, encrypted and accessible only with the private keys. The key value database is stored on the storage node. Metadata is encrypted as a json file and stored on the storage node database.

The system uses hierarchical deterministic wallet keys. A public key of the derived wallet is used as a key hash. The keys are stored on a separate key value database.

Account metadata stores top-level info about all the uploads to an account and resides in the badger K:V database. File metadata stores information about a specific file and resides with the file in the S3 bucket.

FILE SHARING

File sharing is available for individual files by the issuance of a specific public handle for each uploaded file. Since each uploaded file is assigned an individual public handle, each file handle may be shared with individual people who can access via a separate key and a separate instance for each file uploaded. Through this implementation of file sharing, an account owner could upload the same file more than once, creating a new handle each time, and be able to control access for different individuals or groups who have the different handles. Therefore, it would be possible to give handles with different expirations, or retract public file handles of specific individuals while maintaining access for others.

API

The Opacity API is designed for app developers who want to use Opacity as the backend storage system for their applications.

BUSINESS MODEL

Opacity earns money on the storage provided. The current business is sustainable even at a low price of the Opacity token, because Opacity pays only for utilized storage and bandwidth, and most people use less than 1% of the storage they originally purchase. Opacity will charge full market price for storage services purchased by credit card.

Over time, Opacity will add additional features that are charged with the OPQ token or credit card.

BENEFITS TO CUSTOMERS

- Fully private storage, with no access other than via their own private key.
- Secure storage, knowledge that nobody can read it, including the storage providers themselves.

- Low-cost storage, dramatically lower cost than other cloud providers.

- No need to expose any private information to purchase storage.

- Records of the transactions are private when using the OPQ token. Credit card companies and other financial institutions will have no record of the transaction.

- Reliable organization providing cloud storage. No mysterious distributed network or foundation. The founders and company are reliable and well-known individuals with a US-registered incorporated company.

- Backups and redundant capabilities available.

ORGANIZATION

Opacity is a privately held company, fully owned by the founders.

The OPQ token is a utility token available on public cryptoasset exchanges. OPQ is not a speculative token, and it is not designed for rise in value or investment purposes. The sole purpose of OPQ tokens is to purchase services on the Opacity network.

MARKETING

TARGET MARKET

Opacity is appealing to small businesses, individuals and organizations that want to keep their private data private. The initial offering is through private accounts and SMB-size storage accounts. Enterprise-level accounts will be offered starting in Q3 2019, and other services will provide a higher level of flexibility plus international distribution.

COMPETITIVE LANDSCAPE

	Privacy enabled	Zero Knowledge	Easy to use	Low cost	Crypto and credit card
Opacity	☑	☑	☑	☑	☑
Google			☑		
Box	☑		☑		
DropBox			☑		
Mega Pro	☑		☑		
Sync	☑		☑		
Microsoft			☑		
Apple			☑		
Storj	☑	☑		☑	☑
Sia	☑	☑		☑	

Opacity has been well received in the market, with several hundred customers subscribing in the first month, with limited marketing and publicity beyond the existing token holders. The company has an active Telegram group and social media following. Opacity will be leveraging the existing token-holder group, as well as traditional and social media to promote its services.
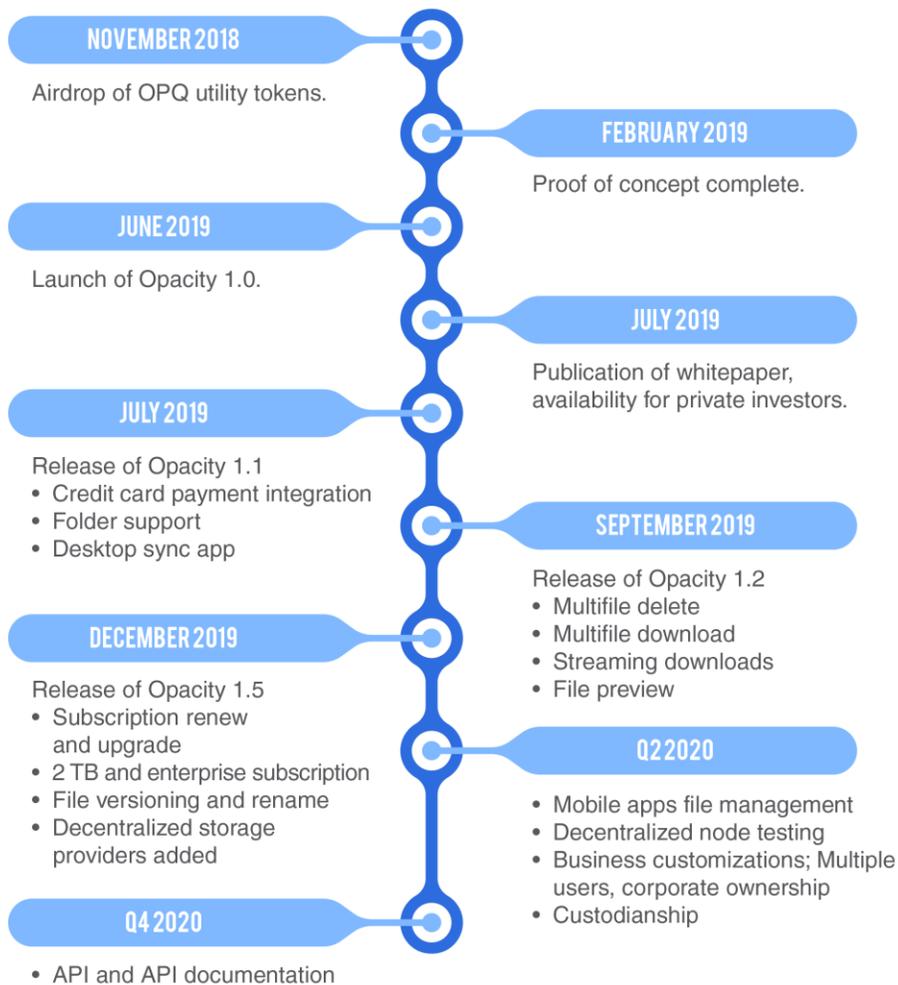
PARTNERSHIPS

Opacity is actively seeking partnerships with organizations that offer products and services directed at people's privacy. As people are increasingly aware of the co-opting of their data by corporations, as well as the threats from hackers of corporate and personal data, the market for privacy is expanding. Through these partnerships, Opacity is developing itself as the storage vendor of choice for a variety of applications requiring fully private cloud storage.

Following are the partners that are available to date, with the launch of the Opacity system:

- QLCChain.Org is partnering with Opacity as part of its service ecosystem. QLCChain is the creator of the Confidant hardware-based private messaging tool. Confidant allows people to send peer-to-peer messages and files from one dedicated hardware node to another. Through the use of their hardware node, people are ensured that their data cannot ever be accessed by anyone other than themselves and the designated recipient. By using Opacity in tangent with Confidant, we provide a true end-to-end privacy solution.

- Flo. The Flo.cash network provides a metadata layer for rapid read-write to the blockchain. The Flo Open Index Protocol is designed for decentralized publishing. The partnership will allow content developers and other dApps on the Flo network to utilize the Opacity storage network for full privacy on the backend, allowing publishers to be fully resistant to censorship.

- BOMB. Opacity is the official zero-knowledge storage platform for BOMB along with the BOMBX incubated companies. The BOMBX Incubator offers entrepreneurs anywhere in the world to launch their idea into the world with zero to minimal upfront capital.

ROADMAP AND MILESTONES

ROADMAP AND MILESTONES

NOVEMBER 2018

Airdrop of OPQ utility tokens.

FEBRUARY 2019

Proof of concept complete.

JUNE 2019

Launch of Opacity 1.0.

JULY 2019

Publication of whitepaper, availability for private investors.

JULY 2019

Release of Opacity 1.1
• Credit card payment integration
• Folder support
• Desktop sync app

SEPTEMBER 2019

Release of Opacity 1.2
• Multifile delete
• Multifile download
• Streaming downloads
• File preview

DECEMBER 2019

Release of Opacity 1.5
• Subscription renew and upgrade
• 2 TB and enterprise subscription
• File versioning and rename
• Decentralized storage providers added

Q2 2020

• Mobile apps file management
• Decentralized node testing
• Business customizations; Multiple users, corporate ownership
• Custodianship

Q4 2020

• API and API documentation

TEAM

JASON COPPOLA, CEO

Jason has 20 years of experience in software product development, working in engineering, product, and executive leadership. He has led organizations to build and deliver highly scalable applications at Fortune 100 and startup companies by applying his experience as an entrepreneur and Agile expert.
https://www.linkedin.com/in/jasoncoppola

ARON HILTZIK, BUSINESS DEVELOPMENT

Aron is a recent student-athlete graduate from University of Illinois with a Bachelor of Arts in Advertising. He founded his first business in 2018, scaling to over $500k in revenue in 6 months. Aron has specializes in marketing, SEO optimization, and brand strategy.
https://www.linkedin.com/in/aronhiltzik/

TIM DEHAAS, COMMUNITY MANAGER

Tim has 2 years of experience in building online communities, and social media management in a variety of platforms. He also performs basic programming and is able to work with highly technical communities. Further, Tim has a B. Sc. in Biochemistry and is currently studying for a Master's degree in Biochemistry and Molecular Biology.
https://github.com/MrRedPandabaer/

WILLIAM HALUNEN, COMMUNITY MANAGER

William has 2 years of experience managing online communities. He has helped organically grow communities totaling over 50,000 members across all social media outlets. He also has a bachelor's degree in computer science.
https://www.linkedin.com/in/william-halunen-080987156/

REBEL FORNEA, TECHNICAL LEAD

Rebel began her software career in the frontend in a hardware company. She got her start in crypto by jointly winning a developer bounty using a language she learned specifically for that prize. She now focuses on backend development, deployments, and design.
https://www.linkedin.com/in/rebel-fornea-7640b8122/

EDMUND MAI, LEAD SOFTWARE ENGINEER

Edmund is an experienced lead developer with experience working for renowned tech startups in NYC. He has founded and built multiple software businesses, one of which was recently acquired.
https://www.linkedin.com/in/edmundmai/

CONNOR HEN, SOFTWARE ENGINEER

Connor has spent the past 5 years in a variety of development roles. He got his programming start in game development making arcade-style games before moving on to generative art and frontend web development. He currently serves as a full-stack developer, including designing and building frontends, library development, and other roles.
https://github.com/CKH4

MARCEL LINDIG, SOFTWARE ENGINEER

Marcel has 10 years of experience developing software, working in everything from front end development to database administration. He has worked with a variety of clients, from individual designers to international corporations, to advise on software needs and deliver custom solutions.
https://github.com/nullpilot

LADISLAV BALON, SOFTWARE ENGINEER

Ladislav is experienced full-stack developer who started programming when he was 13 years old. He has worked on many commercial projects for a variety of clients as well as on his own projects.
https://www.linkedin.com/in/ladislav-balon-00134b54/