myMessage Whitepaper 0.9.1

About myMessage

Many people continue to wonder how they could store files, documents, pictures, or videos, permanently. Various techniques have been adopted by people to keep their precious files for generations to come. These techniques include the use of pen drives, SSD hard disk, cloud storage, and even multiple PCs as forms of storage. Moreover, people have also embraced the use of paper or hardcopy storage, CD, DVD, and many more.

“Moreover, people believe that storing copies of an original document at different distant locations may help solve the problem of loss of the original to threats such as theft, fire or earthquake. More so, some people feel most secure when their document is stored at three distant locations." [1]

It is true that information stored using the above techniques may last long, however, they tend to get misplaced or spoilt after a long time. Furthermore, a pen drive, SSD hard disk, physical storage, or DVD could get damaged, lost in transit, or stolen. More so, a proven fact is that “condensation from high temperatures or high humidity can lead to the shortening of circuit boards or corrosion of contacts.” [2]

“Recordable CD-RWs may seem to be durable and secure, and optimists have estimated that they could last for 20 to 30 years. However, real life experiences have proven otherwise as manufacturers began introducing discs of variable quality to the market, some of which would not endure up to a year.” [1]

What about cloud storage such as Dropbox, Google Cloud, Apple iCloud, and Microsoft Cloud? They may seem reliable but are very prone to hacking: It happened in the past, and it would happen in the future. Furthermore, your information stored in the cloud storage can be lost, modified, hacked, or deleted if it is inactive for years. Therefore, they cannot be classified as permanent storage. [3].

“However, the biggest cause of concern for Cloud storage is not hacked data, it is lost data. For instance, Dropbox recently had a glitch in their sync system, and it left many subscribers with lost files. For those who only had their files hosted on Dropbox, there was no possible way to retrieve them.” [4]

Because of this, this project aims to create a means of storing information permanently for decades at a low cost. The proposed storage technique for myMessage is the use of blockchain, which is immutable, undeletable, secure, and timestamped. With blockchain, you can store your information forever, and no one

would be able to delete, modify, or steal your information. Moreover, if you want your information to be kept private, you can encrypt it, hence no one would be able to see your information without having the secret key.

Unlike cloud storage that requires you to pay yearly, myMessage only costs approximately $0.1 per message. However, the cost of the message to be stored is highly dependent on the size. With the use of blockchain, you can view or retrieve your information anytime for free.

What information can you store?

Anything classified as digital can be stored on blockchain. These include

- ASCII Text Art,
- encrypted messages for sensitive information,
- pass messages between parties,
- lover vouch/declaration - like a lover lock,
- valentine message board,
- a verified message from a verified source,
- a will or testament*,
- a will inheritance of crypto assets,
- patents, music rhythm, songs, ideas,
- shout out to commend employee/staffs/co-workers,
- appreciation/thank you note, etc.

Legal Documents

Lawyers encrypt and store legal documents on myMessage, such that if a fire or natural disaster (e.g. an earthquake) breaks out, the documents remain in blockchain, undeletable and immutable.

“The transparent, immutable, and secure nature of the blockchain allows lawyers to record and solve various types of legal matters. From property records to court records, chains of custody, UCC filings, funds transfers, legal opinions, and contracts, there can be a wide range of ledger-based activities in the legal industry.” [5]

Can Wills and Testaments be stored in blockchain?

“According to the Wall Street Blockchain Alliance, the legal industry is one of the fastest-growing sectors when it comes to blockchain. Blockchain, being unhackable, makes it attractive for storing wills and testaments. The ‘Proof of existence’ acts as a public notary that demonstrates data ownership and examines the integrity of the document, therefore making verification easier. Lawyers are freed from trivial tasks and hence, can leverage more time on legal insights. It helps them draft contracts, store data on transactions and make authentication easier.” [6]

Timestamp your documents, design, and ideas

myMessage can be used to timestamp your documents, ideas, design or a piece of original artwork at a very early stage. Blockchain cannot fake a timestamp nor can the date and time be modified/changed; therefore, it can be used as timestamp proof in the future. However, we do not know if this can be used in a legal case as evidence or not. Kindly consult your lawyer if you intend to use this service as proof of evidence.

Moreover, timestamping with myMessage is very cost-effective compared with other platforms that provide timestamping services. For example, Draw (https://www.drawy.eu/protect/) provides timestamping services for EUR8.90 per timestamp. Moreover, Draw is much more complicated and time-consuming than using myMessage. To make use of myMessage timestamping services, simply attach your file and pay a small fee.

Entertainment/Leisure Purpose

You can store your pictures as attachments in the blockchain permanently*.
Alternatively, you can convert your pictures to ASCII Art using freeware such as Alternate’s ASCII Artist, and store it as text ASCII art.

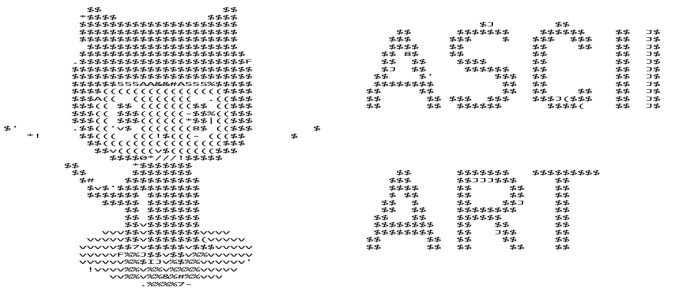

Figure 1: ASCII ART sample

Meeting Minutes

Your company's meeting minutes can be stored in the blockchain and encrypted if necessary; so that the public won't be able to see your content. To store your meeting minutes, use tags such as

#Company_ABC

#meeting minute 26 March 2021

#memo: 2011566

Subsequently, you can just search all the company's meeting minutes using the keyword/tag "Company_ABC." You don’t even need to remember the txid.

How does it work?

A smart contract is deployed in the Zilliqa network; and a front-end dApp is used to interact with the smart contract. Afterward, you type your message or attach a file, encrypt it if necessary, and then send it to the network. You'll be required to pay the network fee and the commission fee of myMessage.

How do I retrieve my message?

We offer many ways to search your messages stored on blockchain. You can search by txid, the sender address, keywords/tags and/or using the range of date.

Moreover, you can search for encrypted messages only, or messages with attachments only.

How secure is the encryption?

Storing sensitive and secret messages/files for many years requires very strong protection against hacking. To make sure your encryption is as secure as possible, we require you to use strong secret keys where a combination of alphabets, numeric, and symbols is definitely a must. Furthermore, the secret keys are made lengthy so that a hacker will not be able to guess or use brute-force to break open your secret messages or documents.

However, there are speculations that brute-force using quantum computers is very possible; therefore, brute-force encryption algorithms like RSA are not safe against quantum computer attacks [ ]. According to [ ], AES 256 is very strong against quantum computer attacks, thus myMessage uses AES256 as the encryption algorithm to support. If you still worry about quantum computer attacks, you can encrypt your files using PeaZip (windows version available), a free utility similar to Zip that can compress and encrypt your files using strong encryption techniques such as AES256, Serpent256, or Twofish256, which are quantum computer resistant algorithms. Therefore, you can perform double encryption: One on your file using Twofish256 or Serpent256, and the other with AES256 (the encryption algorithm that myMessage uses) when sending it to the blockchain. Therefore, you will have two secret keys: you need the AES secret key to download the file from blockchain. Afterward, you will need the second secret key to decrypt the file. This will ensure maximum security.

A comparative study of AES, Blowfish, Twofish, and serpent cryptography algorithms. Debasish Roy, Saptarshi Paul and Sanju Das Computer Science Department, Assam University, Silchar, India.

The encryption is very secure with the AES encryption algorithm. “AES256 is virtually impenetrable using brute-force methods. While a 56-bit DES key can be cracked in less than a day, AES would take billions of years to break using current computing technology. Hackers would be foolish to even attempt this type of attack.” [7]

AES encryption is one of the five most common encryption methods that is considered unbreakable [8]. According to Wikipedia, AES is one of the post-quantum computer-resistant encryption. “Provided one uses sufficiently large key sizes, the symmetric key cryptographic systems like AES and SNOW 3G are already resistant to attack by a quantum computer.” [9]

Quantum Computer Threat

Since this is a permanent message storage solution, the information might be stored for many years or decades, and quantum computers might become available by then. Quantum computer threat might be an issue if you would like to store sensitive data for decades.

Using normal encryption which is not threatened by our classical computer will not be sufficient if one intends to store information for a long time. Therefore, we use a quantum-resistant encryption algorithm; we use AES encryption as our encryption algorithm; specifically, we use AES256.

What is AES?

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity, and electronic data protection [10].

The National Institute of Standards and Technology selected three “flavors” of AES: 128-bit, 192-bit, and 256-bit. Each type uses 128-bit blocks. The difference lies in the length of the key. Being the longest, the 256-bit key provides the strongest level of encryption. With a 256-bit key, a hacker would need to try 2256 different combinations to ensure the right one is included. This number is astronomically large, landing at 78 digits in total. It is exponentially greater than the number of atoms in the observable universe [11]. AES 128 uses 10 rounds, AES 192 uses 12 rounds, and AES 256 uses 14 rounds. The more rounds, the more complex the encryption, making AES 256 the most secure AES implementation.

For securing data using symmetric key cryptography, Advanced Encryption Standard (AES) is one of the trusted cryptographic algorithms, which can resist conventional computers as well as quantum computers [12].

Multiple Levels of Security

AES encryption is very strong and can resist quantum computer attacks. However, if anyone knows your secret key, he/she can view your secret files irrespective of how strong the encryption is. Therefore, never reveal your secret key!

However, if you really need to share your secret key with someone, you can still add more security to your file. You can use the same secret key to encrypt all your files

when sending to myMessage, but a different secret key for each file. Encrypt each file before attaching and sending it to myMessage. Use strong encryption like AES, Blowfish, or Twofish, which are also resistant to quantum attacks. Using this method will provide extra security to your most sensitive information which will be stored on blockchain. However, you need to remember all your secret keys: if you lose/forget one of the secret keys, you will permanently lose access to that important information forever, and no one would be able to help you.

Why myMessage chose ZILLIQA blockchain?

To send information permanently on blockchain, we need some criteria:

1) Speed: The confirmation speed must be reasonably fast. If it takes too long to confirm, our users will feel annoyed. We put our criteria for confirmation time to be less than or equal to 5 minutes.
2) Throughput: We need high throughput blockchain. Many users will use our services, and we can't afford our blockchain to have low TPS, and network congestion which results in delays in confirmation. Our minimum is 2000 TPS.
3) Fee: This is our main criteria. If the network fee is high, no one will use our service. The fee must be low and affordable for all. Therefore, the maximum fee for an average message (1 kB message) should be less than $0.1.
4) Technical support: We prefer good technical support from the team so that our technical team can have good support if any issue arises.
5) Decentralization: We want a blockchain that has good decentralization.

The list above shows the criteria any blockchain must fulfill before myMessage would run on it. We found that the ZILLIQA blockchain fulfilled all our criteria, and thus we select the ZILLIQA blockchain to build on. We also apply for a development grant.

Contact Us

You can reach us via several methods as shown below:
Email: contact@mymessage.io
Official website: https://myMessage.io
Official telegram: https://t.me/myMessageio
Github: https://github.com/daynight97/myzilliqawallet
(Repo still in private now)

DISCLAIMER

This material is provided on an "as is" basis and to the fullest extent permitted by law is without warranty of any kind whatsoever, whether express or implied, including without limitation to any implied warranties of merchantability, fitness for use, fitness for a particular purpose and/or non-infringement of third-party rights. In addition, any warranties, whether express or implied, statutory or otherwise, in relation to use, access, operation, availability, continuity, or non-interruption of this material are hereby excluded to the fullest extent, permitted by law. While the information and content on this material are believed to be accurate, it may contain errors or inaccuracies.

Reference

[1] https://www.ifla.org/node/93091
[2] https://www.datarecovery.net/newsletters/what-kills-flash-drive.aspx
[3] https://www.bbc.com/news/technology-29237469
[4] https://blog.cloudhq.net/5-safety-concerns-with-cloud-data-storage-answered/
[5] https://www.leewayhertz.com/blockchain-in-legal-industry/
[6] https://medium.com/@vishnu_3187/wills-and-testaments-on-the-blockchain-crypto-wills-9d2be9171a7d
[7] https://www.solarwindsmsp.com/blog/aes-256-encryption-algorithm
[8] https://blog.storagecraft.com/5-common-encryption-algorithms
[9] https://en.wikipedia.org/wiki/Post-quantum_cryptography
[10] https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
[11] https://www.solarwindsmsp.com/blog/aes-256-encryption-algorithm
[12] The AES-256 Cryptosystem Resists Quantum Attacks, International Journal of Advanced Computer Research.

Notes

*Do note, however, due to the limitation of the Zilliqa blockchain, you cannot store any file larger than 200kB. We are working on a solution to extend this.