AEGEUS.

Secure Messaging Blueprint

Secure Means of Sharing Data Using IPFS

V2.0 November 2018

CONTENTS

AEGEUS.

01. Introduction

Everybody wants to send information to each other securely these days. We not only have big brother on our backs, we are also chased by hackers and they unfortunately are ‘our peers’. Mainstream secure messaging is becoming more competitive and more technological advances allow hackers to compromise these advances.

Blockchain systems are highly secure, but regrettably are not able to cater for unlimited data encryption, storage, and distribution from one party to another or between multiple users. The only tech out there that can mitigate these problems is IPFS (InterPlanetary File System). However, it is still in its early days.

IPFS is by far the most promising solution available today. Similar in structure to the Bittorrent model, IPFS is a peer-to-peer protocol where each node stores a collection of hashed files. A user who wishes to retrieve a file must go through highly secure layers to access this data.

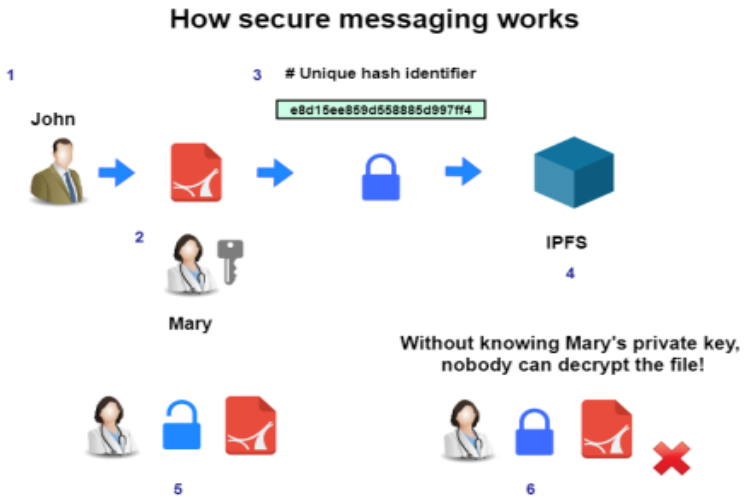
Since using hash identifiers is not secure enough, especially for sensitive data, a second layer must be used in order to access the data. This second layer is a unique encryption process linked to a particular hash file which represents an actual data file.

IPFS is used to search through the network of nodes to find the file that the user is seeking. So in essence, there are two layers of security before one gets to the actual file, perhaps three if one looks at the actual process up close. This decentralized method of data distribution and retrieval provides more control to the users in terms of security and anonymity.

02. Secure Messaging Process

John (sender) wants to send a message to Mary (recipient), so he creates a message using one of the following data types:

1. Zip Files
2. Audio Files
3. Video Files
4. Texts
5. Images



Once the message is created, John encrypts it with Mary's public key so only Mary can access it using her privatekey. This message is then sent (uploaded) on the IPFS network. John then proceeds to send Mary the hash of that file which can only be encrypted with the public key of the recipient which in this case is Mary.

Mary, the recipient, then proceeds to decrypt the hash file with her private key. Once Mary decrypts the hash file using her private key, John's wallet notifies him that the file has been been downloaded from the IPFS server. For an extra layer of security, the content will

not be displayed without the user unlocking their wallet for either that session or per-message.

All file types can be transmitted, and there is no limitation to data size. However, large data types are encouraged to use compressed (zip) files as it makes the whole messaging process more efficient. Nodes that participate in storing data will receive a percentage of the fee charged for carrying out this secure messaging feature. This is to ensure that all participating nodes are rewarded for enabling this service on the IPFS network.

So every time a storage node serves up content, it will receive a fee that will come from the message users wallets. These fees are yet to be established by Aegeus but will be released very soon once our public Prototype is completed and released.

03. Conclusion

Secure messaging through IPFS and asymmetric encryption is the most secure way of sending and receiving data, especially over a large network or long distance. As per the example above, users can upload any file data to their IPFS directory and give access to whom the user chooses.

Once users know whom they wish to provide access to, they can encrypt the file with that person's public key. Once the file is encrypted, it is assigned a hash and is stored on the IPFS network. Only the person whose public key was used to encrypt the file can access that specific file using their personal private key.

If the file needs to be accessed by more than one person, there is an option to select multiple recipients from the directory, prior to encrypting and sending.

This is the beauty of Secure Messaging through IPFS. Decryption cannot happen without the recipients' private keys. Private keys are only generated when public keys are generated. These files cannot be decrypted without the relevant private key.

Although this technology is relatively new, the organic need for such features is rising every single day as more and more sensitive data is being compromised.

Businesses and personal interactions have become more vulnerable to attacks over the past few years. IPFS can help put data sharing, secure messaging, and collaboration on the map again in a new, fresh and exciting way.

Aegeus will roll out its secure messaging feature once the public prototype is launched. Thank you for reading this publication. For more information regarding this blueprint, Aegeus, or to speak to a team member, please visit “https://aegeus.io” or email us at “contact@aegeus.io”.


AEGEUS.