AEGEUS

Secure Messaging Blueprint

Secure Means of Sharing Data Using IPFS

V1.0 September 2018

Contents

Introduction

Everybody wants to send information to each other securely these days. We not only have big brother on our backs, but we also have hackers and these are unfortunately ‘our peers’. Mainstream secure messaging is becoming more and more competitive, and more 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 multiples of individuals. The only tech out there left that has got any play, and it’s still in its early days is Interplanetary File System, otherwise known as IPFS.

It is by far the most promising solution available to us today. Similar in structure to the Bit torrent 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.

Using hash identifiers is not secure enough especially for sensitive data so a second layer must be used in order to access the data.

This second layer is a unique encryption process and it makes the whole world of difference! This encryption is 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 client is seeking. So in essence there are two layers of security before you get to the actual file, perhaps three if you look at the actual process up close. This decentralized and distributed method of data distribution and retrieval puts users more in control by far and certainly allows for a substantially richer programmatic interaction.

Secure Messaging Process

John (Sender) wants to send a message to Mary (Recipient), so he creates his message using one of the following data types;

1. Zip Files
2. Audio Files
3. Videos
4. Text
5. Images

Once the message is created, John encrypts it with Mary's public key so only Mary can access it using her key. 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.

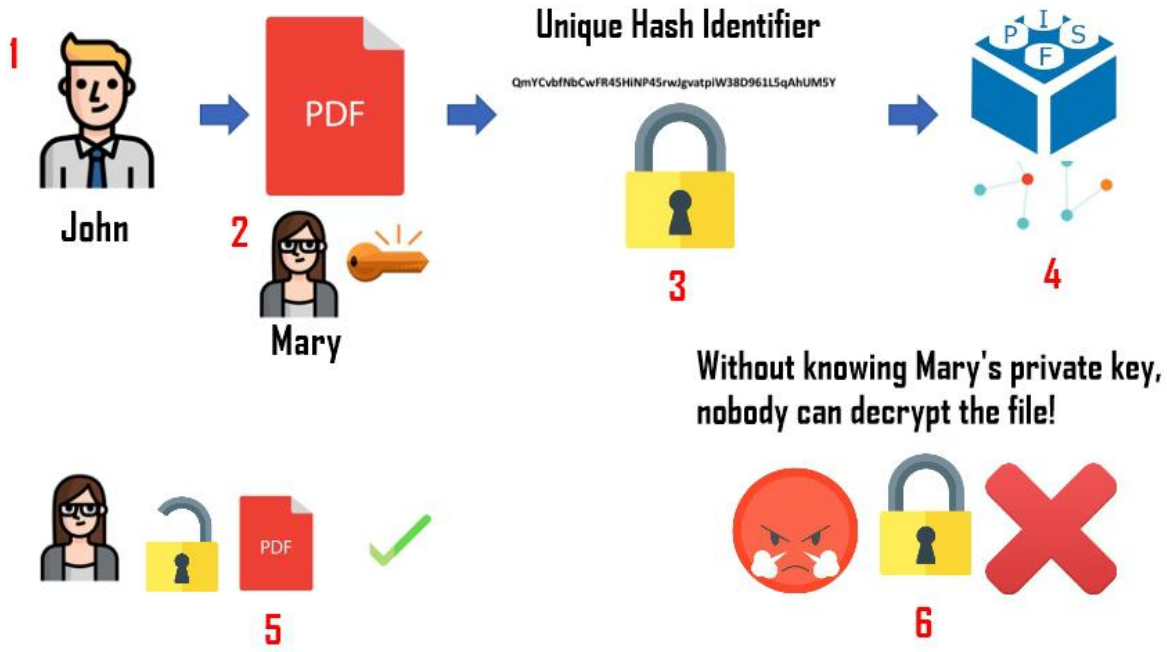
Mary the recipient then proceeds to decrypt the hash file with her private key. Once Mary decrypts the hash file using her private key, John's wallet notifies him that the file has been been downloaded from the IPFS server.

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 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, but will be very soon.

How Secure Messaging Works



Aegeus Secure Messaging using IPFS technology!

Conclusion

Secure messaging through IPFS and asymmetric encryption must be the most secure way of sending and receiving data in existence today, especially over a large network, distance or populous. As per the example above, users can upload any file data to their IPFS directory and select who to give access to.

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

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

This is the beauty of Secure Messaging through IPFS. Decryption cannot happen without this person's private key. Private keys are only generated when public keys are generated. Malicious parties cannot decrypt these files, because they lack the very important 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 in danger over the past few years and are increasingly becoming eroded. IPFS can 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 sometime after its prototype is launched. Thank you for reading this publication. For more information regarding this blueprint, Aegeus, or to speak to one of the team, please visit www.Aegeus.io or email us at contact@aegeus.io

AEGEUS

Secure Messaging Blueprint

Secure Means of Sharing Data Using IPFS

V1.0 September 2018