HashBox Mail - Blockchain Messaging Protocol

Silvio Guedes Santana
https://mail.hashbox.app/address/0x55555E09bc39767C48Eb02863029Cb0838a80f2B

Abstract

A protocol to exchange messages and files on blockchain in a decentralized way, scalable, cryptographically secure, censorship-resistant, with SPAM prevention mechanisms and active participation of users in its decentralization. Through the use of peer-to-peer encryption, it removes the need for users to provide personal information on websites and online systems where leaking such information could compromise their security. The communication between the sender and the receiver is done through NFTs instead of proprietary APIs, as is done nowadays, using only the wallet address and a common smart contract between them. Protection against SPAM proves to be efficient, as an attack on the user's mailbox becomes costly when it is necessary to make a payment to the receiver. Scalability is achieved by using distributed file storage, while smart contracts are used to generate incentives to keep the network available as long as possible.

Keywords: NFT. Mail. Messages. Files. Cryptography.

Introduction

Due to the nature of the blockchain that all data on it is public, anyone who knows a user's wallet address can know how much money the user has. If it is an exorbitant amount, this information could put that person's safety at risk if a criminal knows where the user lives or goes to.

For this reason, no user should link his personal information (SSN, home address, telephone number or workplace address) to his wallet address. A criminal knowing someone's email address, can easily discover his home address or sensitive information from a resume posted online (usually on LinkedIn [1]).

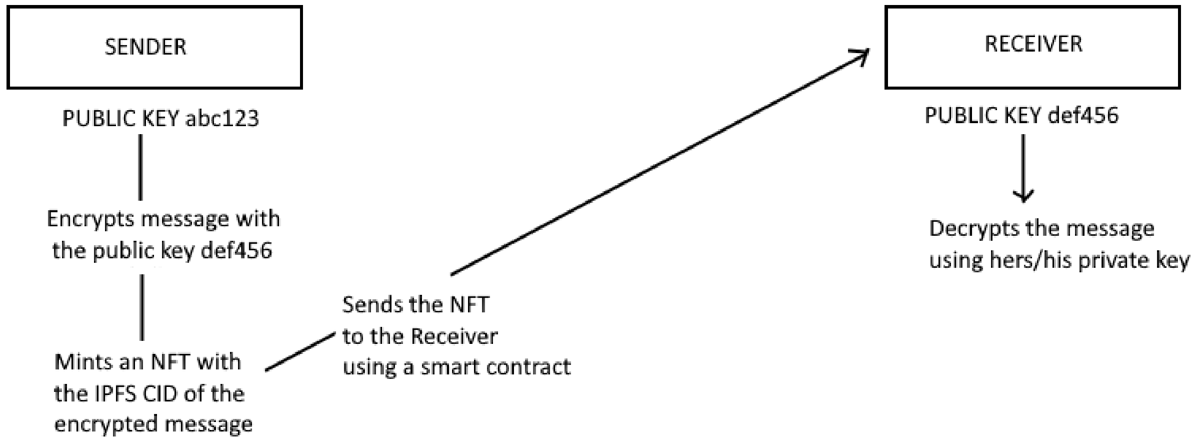
The solution removes this need for the user to expose personal information, using only his wallet address to communicate, to receive information or files from a company or another user. An online platform only needs to know the user's wallet address - if he has the necessary amount or if he has already paid for the product/service offered.

Privacy is an increasingly scarce commodity in online systems today. If user data is the new gold [2], privacy has become the new diamond [3].

How does it solve this problem?

Through the use of NFTs (smart contracts of the ERC-721/ERC-1155 type), blockchain, IPFS (InterPlanetary File System) [4] and encryption (hash algorithms, RSA and AES encryption), in which each message is sent to the receiver via the blockchain.

Each participant in the protocol (sender and receiver) has its wallet address linked to a public key and an RSA private key. The receiver's public key (which is known to everyone) is used by the sender to encrypt the message he is going to send. The receiver, in turn, has a private key (which only he has access to) to decrypt the received message.

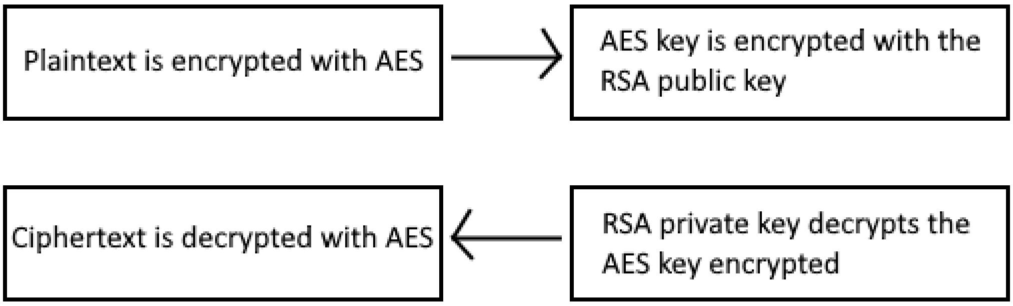

SENDER
PUBLIC KEY abc123
Encrypts message with the public key def456
Mints an NFT with the IPFS CID of the encrypted message
Sends the NFT to the Receiver using a smart contract
RECEIVER
PUBLIC KEY def456
Decrypts the message using hers/his private key

Each user's public keys are stored in a smart contract in which both the sender and the receiver participate, in much the same way as is done in the current artistic NFTs. Messages are also NFTs, having in their metadata information related to the encryption algorithm used, the subject and the body of the email (the last two are encrypted).

Only the receiver can decrypt the received message using their RSA private key. The RSA encryption algorithm uses SHA256 as the hash algorithm and 2048 bits of modulus length (length key) which are currently recommended by IBM [5]. The AES encryption algorithm also uses SHA256 as the hashing algorithm and has a 256-bit key length.

This means that the number of attempts for a conventional computer to break RSA encryption is 2^{2048} - a real eternity. For a quantum computer, it would take 8 hours and would need 20 million imperfect qubits [6], something we are far from having today [7].

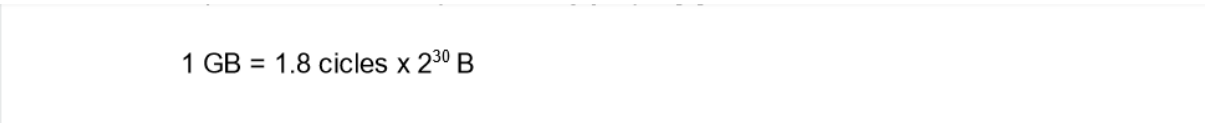
Encryption and decryption is done in a hybrid way [8], in which the asymmetric key (RSA) reveals the symmetric key (AES) that gives access to the original content (plaintext) that was previously encrypted (ciphertext).


Plaintext is encrypted with AES
AES key is encrypted with the RSA public key
Ciphertext is decrypted with AES
RSA private key decrypts the AES key encrypted

In turn, to decrypt a ciphertext using AES 256-bit encryption, a computer equipped with an Intel Core i7 Extreme Edition processor takes about 1.8 iterations (cycles) per byte [9].

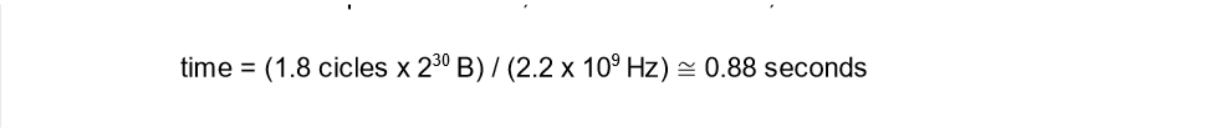
Note: although we are already on the 12th generation of Intel processors, we will use this known value for comparison purposes only.

With this, we have for each gigabyte:



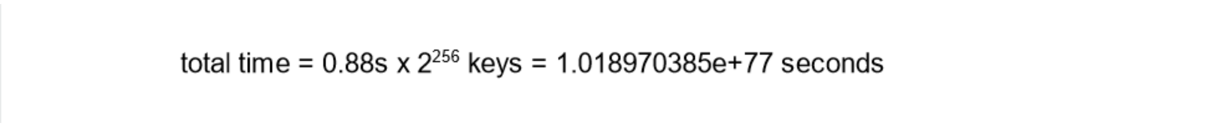
$$1 \text{ GB} = 1.8 \text{ cicles} \times 2^{30} \text{ B}$$

For a computer with 2.2 GHz clock rate per second, we have:



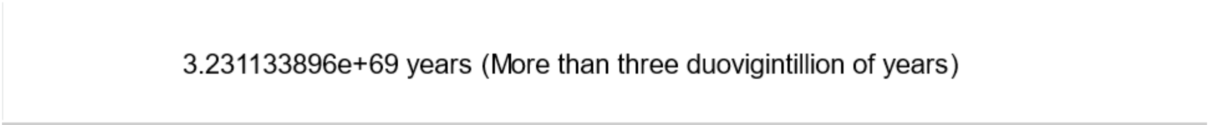
$$\text{time} = (1.8 \text{ cicles} \times 2^{30} \text{ B}) / (2.2 \times 10^{9} \text{ Hz}) \cong 0.88 \text{ seconds}$$

Since the key is 256 bits long, so:



$$\text{total time} = 0.88\text{s} \times 2^{256} \text{ keys} = 1.018970385\text{e+}77 \text{ seconds}$$

Or about:



3.231133896e+69 years (More than three duovigintillion of years)

In short: if someone tries to decrypt a single 1 gigabyte message using brute force in the AES algorithm, for example, that person will take tens of years and will need to spend hundreds of times the energy sources of the Universe [10].

How does this technology differ from most messaging apps?

It allows the receiver user to receive a message only after paying a fee. If the user does not pay, he is unable to contact the owner of the wallet address.

This avoids the famous SPAMs (and scams) from emails or mobile applications such as:

- Nigerian princes who want to donate their fortune [11];
- Foreign women who say they love you but don't know if you're a man or a woman (Dear Mr/Ms);
- That you earned 1 BTC but need to spend $1,000.00 to redeem it;
- That a manager of a big company says that you are approved for a position (without you even having sent your resume) and that you will work part-time from home earning 5 thousand dollars [12].

If the anti-SPAM mechanism is activated, spammers and scammers will always have to pay the receiver user on the first message they send. If the permanent fee mechanism is enabled, anyone will always have to pay the fee to the receiver.

In today's world with so many social networks, businesses, types of entertainment and so much connection with friends and relatives, companies need to fight each other to get users' attention. If the user pays attention, he should be rewarded in some way, as attention is the new currency for businesses and individuals [13].

What are the use cases for this technology?

The use cases are not only in the primary use (messages), but as a basis for several applications that today have supreme owners in Web 2.0:

- For email receiving application such as Gmail;
- For sending emails application, such as SendGrid;
- For file storage, as on Dropbox;
- For a user to order a food in a restaurant, as on Grubhub;
- For a user to send their shopping list to a market, as on Instacart;
- For a user to contact a delivery man, as on Amazon Flex;
- For a user to ask a driver for a ride, as on Uber;
- For a user to contact a home service, as on Thumbtack;
- For a user to get legal advice, as on Fastcase;
- To send documents and rent a car, as on Turo.

For each request made, part of the payment can be sent to the receiver and another part to the company that provided the bridge.

Small/medium businesses and self-employed workers will be able to directly benefit from the crypto economy without going through a payment gateway or trying their luck at daytrade. Getting paid in cryptocurrencies will no longer be a privilege only for cryptocurrency developers, exchanges, miners and digital artists.

It is good to warn that the examples of use cases are endless, the business possibilities are endless, but unfortunately the profit can only be 21 million Bitcoins.

What are the possibilities of this type of communication?

There are uses that are still unknown for a newly created technology. This is often referred to as Deep Tech/Hard Tech [14], where not even the creator has any idea of everything that can be done with their creation.

One of these uses not yet known could be in a metaverse.

Although I think that metaverses have several problems for mass adoption, I believe they are valid for some specific uses, much more as help material to learn some manual profession or as an additional package for games, but not as a social network as it is being speculated.

One of the possibilities is unlocking items in games - where the item's password is sent as an encrypted message to the player's mailbox.

Another would be for communication: more famous avatars need to have an anti-SPAM mechanism, in case the metaverse is blockchain-based and has wallet addresses as a way of identification.

What if I don't have any company, can I still make money from it? How?

Yes. Through IPFS servers that will work as “bridges” between the sender user and the receiver user. The sending user pays a fee in cryptocurrency to use your server and be able to upload the content on the IPFS network, while the receiver user uses the service to obtain the content stored on the IPFS network.

Why wasn't the blockchain itself used to store the email content?

Because a 32-byte word costs 20,000 gas to be stored on the Ethereum blockchain [15]. As the average block size limit (before “The Merge” [16]) is 15 million gas [17], this makes the maximum text that can be stored in a block is 750 words, i.e. , about 24 KB.

In addition to being an inappropriate size for the storage of most files today, this would be costly when taking into account that the value of gas on the Ethereum network is costing 10 gwei and 1 ether costs US$ 1,600.00 in August 2022 (approximated values).

For a 24 KB file, the cost would be US$ 240.00 (not counting the transaction amount).

Because IPFS storage is efficient, censorship resistant, free and can be used to generate community participation in the protocol, for these and other characteristics it was chosen. But nothing prevents another storage protocol from being used instead.

Is it too expensive to send a HashBox Mail?

If it's on the Ethereum network before “The Merge”, yes. Currently, it would be more advantageous to use a Layer 2 or Ethereum Sidechain with lower rates, such as Polygon (MATIC) or BSC (Binance Smart Chain). These two were the ones tested, there are other networks that use EVM and have low transaction values like Fantom and Harmony.

On Polygon's testnet, the value per email is no more than 2 cents:
https://mumbai.polygonscan.com/tx/0xea2ba4c5029377d400d8f7e9b0c81c9ec068e06fe3f668d18aee5511c97036be

Is it possible to use this protocol on another blockchain?

Yes. Just convert the code from Solidity to Haskell (if your app runs on Cardano blockchain), from Solidity to Rust (if your app runs on Solana blockchain), or from Solidity to any other language of any other blockchain that supports smart contracts.

For blockchains that use EVM (Ethereum Virtual Machine), the code, theoretically, is already adapted for them. But I recommend that you test on a testnet before deploying to the mainnet.

Why did you barely comment the code?

For three reasons:

a) Because much of the code is self-explanatory - e.g., the getUtils() function, is for getting the Utils instance;
b) Because in this way I force interested companies hire my consulting service to understand the entire protocol;
c) To make my webmail code useful as soon as it is ready - I will be providing paid consulting through HashBox Mail.

Note: I only commented parts of the code where even I have difficulty understanding what I did.

Can I collaborate on the code?

Yes, you can. But I will pay more attention to issues related to the security of the protocol. Feel free to create issues and forks.

Can I reuse your code?

Yes. The license is MIT, do whatever you want with the code in your fork.

Features and Tokenomics

- Fixed total of 10 billion tokens (HBM);
- Starting fixed price of 0.008 MATIC (Polygon Network);
- Any email (except Feed) must spend 1 token to be sent;
- Every token spent to send an email goes back to the protocol;
- Any user can buy a token in the protocol (permissionless);
- Any user can sell a token in the protocol (swaps);
- No tokens will be created after launch;
- The price in MATIC will not be changed after launch.

Final considerations

If you liked the project and want to contribute, there are several possibilities to do:

a) Testing the project using the testnet version;
b) Listing an issue related to the code security on the project's GitHub;
c) Being an IPFS server (and getting paid for it), helping with the decentralization;
d) Converting Solidity code to other languages;
e) Creating some of the possible solutions listed and including my wallet address as a receiver of part of the fees;
f) Donating some ethers to my wallet address.

My wallet address: 0x55555E09bc39767C48Eb02863029Cb0838a80f2B.

References

[1] PALMER, Danny. Phishing emails targeting LinkedIn accounts are on the rise. Here's what to watch out for. **ZDNet**, 2022. Available at: <https://www.zdnet.com/article/phishing-emails-targeting-linkedin-accounts-are-on-the-rise-heres-what-to-watch-out-for/>. Accessed on 1st August 2022.

[2] OLANO, Gabriel. Data is the new gold. **Insurance Business Mag**, 2022. Available at: <https://www.insurancebusinessmag.com/us/risk-management/news/data-is-the-new-gold-325916.aspx>. Accessed on 1st August 2022.

[3] LESWING, Kif. Apple is turning privacy into a business advantage, not just a marketing slogan. **CNBC**, 2021. Available at: <https://www.cnbc.com/2021/06/07/apple-is-turning-privacy-into-a-business -advantage.html>. Accessed on 1st August 2022.

[4] WHAT is IPFS? **IPFS**, [s.d]. Available at: <https://docs.ipfs.tech/concepts/what-is-ipfs/>. Accessed on 1st August 2022.

[5] SIZE considerations for public and private keys. **IBM**, 2021. Available at: https://www.ibm.com/docs/en/zos/2.2.0?topic=certificates-size-considerations-public-private-keys>. Accessed on 1st August 2022.

[6] GIDNEY, Craig; EKERA, Martin. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. **ARXIV**, 2021. Available at: <https://arxiv.org/abs/1905.09749>. Accessed on 1st August 2022.

[7] HACKETT, Robert. IBM plans a huge leap in superfast quantum computing by 2023. **FORTUNE**, 2020. Available at: <https://fortune.com/2020/09/15/ibm-quantum-computer-1-million-qubits-by-2030/>. Accessed on 1st August 2022.

[8] GURU, Abhishek; AMBHAIKAR, Asha. AES and RSA-based hybrid algorithms for message encryption & decryption. **IT IN INDUSTRY**, 2021. Available at: <https://it-in-industry.org/index.php/itii/article/download/129/114>. Accessed on 1st August 2022.

[9] AKDEMIR, Kahraman et al. Breakthrough AES Performance with Intel AES New Instructions. **INTEL**, 2010, 5p. Available at: <https://software.intel.com/sites/default/files/m/d/4/1/d/8/10TB24_Breakthrough_AES_Performance_with_Intel_AES_New_Instructions.final.secure.pdf>. Accessed on 1st August 2022.

[10] SCHNEIER, Bruce, APPLIED CRYPTOGRAPHY: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996. 157-158p.

[11] LEONHARDT, Megan. Nigerian prince' email scams still rake in over $700,000 a year—here's how to protect yourself. **CNBC**, 2019. Available at: <https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html>. Accessed on 1st August 2022.

[12] LALLJEE, Jason. Job switchers beware: Some high-paying, remote jobs are scams. **BUSINESS INSIDER**, 2022. Available at: <https://www.businessinsider.com/job-scams-high-paying-remote-work-walmart-amazon-bbb-warning-2022-1>. Accessed on 1st August 2022.

[13] DAVENPORT, Thomas H.; BECK, John C. THE ATTENTION ECONOMY: Understanding the New Currency of Business. Harvard Business Press, 2001. 3p.

[14] WHAT Is Deep Tech Anyway? A Guide to Deep Tech Startups in CEE. **WOLVES SUMMIT**, c2018. Available at: <https://www.wolvessummit.com/blog/deep-tech-startups-in-cee>. Accessed on 1st August 2022.

[15] Dr. WOOD, Gavin, Ethereum: A secure decentralised generalised transaction ledger. **GITHUB**, 2022. 27p. Available at: <https://ethereum.github.io/yellowpaper/paper.pdf>. Accessed on 1st August 2022.

[16] What is The Merge? **ETHEREUM**, 2022. Available at: <https://ethereum.org/en/upgrades/merge/#what-is-the-merge>. Accessed on 1st August 2022.

[17] Block Size. **ETHEREUM**, 2022. Available at: <https://ethereum.org/en/developers/docs/blocks/#block-size>. Accessed on 1st August 2022.