ePigeon Whitepaper

Have you ever wanted to reach out to someone with a specific wallet address on the blockchain? A smart contract owner or an NFT holder? Are you looking for a fully decentralized but encrypted solution for messaging?

Now you can send messages with ePigeon's courier pigeons. Everyone with an existing wallet address is automatically a user and can be reached with our pigeons.

Pigeons can be owned and traded. They can also have a valuable payload to attract the recipient's attention.

Fully decentralized messaging

ePigeon is a set of smart contracts that create fully decentralized messaging solutions. ePigeon empowers anyone to create and make use of different applications.

Applications are represented by ownable smart contracts that are minted by smart contract factories. These smart contracts can be tokenized into NFTs and put on sale if the owner would want to transfer ownership.

There is an unlimited number of new possible applications. New factories can be set up any time. Applications can represent one-to-one encrypted messaging, subscribed private groups, bulletin boards, advertisement solutions, etc.

Example: a simple ePigeon application is just like a real-life courier pigeon. You can own a pigeon and send it with a message to any address on the blockchain. Only the recipient can reply and send the pigeon back to you. You can send a value payload to the recipient as well. All of these "functionalities" are provided by an ePigeon contract. The contract is owned by a wallet address (sender) and it is only the owner who can trigger transactions (set destination wallet address, write a message, attach payload, etc.). Some functions can be triggered exclusively by the recipient. These include replying and accepting the pigeon's payload.

Encrypted communication

Since the blockchain is a transparent environment, a special smart contract is in place to enable encrypted one-on-one communication. The NameAndPublicKeyDirectory contract enables the storage of public keys for encrypted one-on-one messaging. Public keys are expected to be ECDH P-384 public keys in JWK (JSON Web Key) format to enable client interoperability.

ECDH key pairs can be generated outside of the blockchain (or by the dApp). The private key of one party and the public key of the other party can be used to generate a shared secret code which can be used to implement AES encryption on any message and with this making them private on the public blockchain.

The key generation and the encryption standard are deliberately chosen to be publicly known and are available to anyone. Our dApp offers easy keypair generation, encryption and decryption.

Attention tokens

ePigeon can send a message to anyone with an existing wallet address. However, recipients of such ‘cold messages’ need to be made aware that they have something new in their wallet. Such awareness is achieved with the Attention Token solution, the Lockable Coin. The Lockable Coin can be bundled with the message and serves as an incentive for the recipient: the recipient receives the Lockable Coin only after reading the message.

Lockable Coin is an ERC777 token connected to another (interim) ERC777 token called Locked Coin. The combination and interaction of these two coins offer a technical solution for sending a Lockable Coin to a wallet conditionally. Since transactions on the blockchain are not reversible the conditionality is achieved through executing two separate transactions whereas the Locked Coin is used as an interim token. In the first transaction the Lockable Coin is blocked from further transactions (escrow function) and its linked Locked Coin with a message is transferred to the recipient. Once the recipient opens the message, the second part of the transaction is triggered: the Lockable Coin is transferred to the recipient while the linked Locked Coin is burnt. If the recipient fails to open the message within a pre-defined time period, the Lockable Coin is unblocked and its linked Locked Coin is burnt. This way the original conditions are restored as if no transactions had happened at all.

Smart contracts as NFTs

All ePigeon smart contract applications can be tokenized into ePigeon NFTs. ePigeon NFTs are linked to a unique smart contract that makes the applications tradable on NFT markets. These can be sold with or without their message and payloads (contents). This reduces unnecessary contract creation and enables the applications’ users to recover their initial investment into minting the token.

Verified smart contract addresses

Smart contracts are live and verified on both Ethereum MainNet and Polygon. The addresses are the same on both blockchains for:

Lockable Token:	0x41A7E62e231BAd6026B82952C78FaB6e61D96958
LockedCoin:	0x258B53983EE9Bd315a281382aa4c1f84351F113f
Coinbank:	0x33A2c56186E76103E29539e6fC8816e5D36148eD
Epigeon:	0xA89D7d236f518bBC93355e7754AAbe32Ec0485ef
EpigeonNFT:	0xe9b4Bc4E8D1a4a3b8A94956C0771526916c526C5
NameAndKeyDirectory:	0xf473037A55520D35765321F22cc989A54C6038CA
DestinationDirectory:	0x77eEaFd371709f1E946C338b83aC0a8507D561Fc
Chat:	0x1b9ec769445Aeb3b294A8F45100B64f976c4e10E
SharedPigeon:	0xB7c9D0B25A78bA692BdaEF585214b3407718f17D
Pigeon by LimitedPigeonFactory:	0x4264F03eb34Ee8Bd1cFBD8568e1ECd415D770177