Block Labs publications
Type: Whitepaper
First published: January 2018
Last update: 06.11.2023
Luxembourg 2023
https://4thtech.io/

# “on-chain” communication technology framework --4thTech Project Whitepaper--

Dr. Tali Režun & Denis Jazbec

***Abstract;*** **The internet changed the way we live, it opened the highway to unlimited communication and revolutionized access to information, but it failed greatly regarding our digital freedom. Instead of providing a safe environment for online communication (i.e. emailing, messaging, data exchange) that we depend on every day, the internet evolved into a system of centralized intermediaries which trade the ease of access for mass surveillance and user data mining. While the majority of users have no problems accessing legacy email, messaging, or data file-sharing platforms, the “permissioned access” issue remains. Enforced usually based on censorship misbehaviour, de-platforming cases are well known leading to various cases of access restrictions. The fact remains, that the current legacy communication platforms are designed to grant permission for every email or message that we send based on pre-approval mechanics. There is also the matter of data ownership. Did you know that the moment you attach any data file to an email attachment or share it via any “free” messaging service or data file-sharing app there is a big data ownership loss possibility? Blockchain always offered the promise of enabling permissionless, secure, non-custodial, immutable communication with uninterrupted up-time, while retaining data and identity ownership, it is by design the right tool for the job. 4thTech addressed this issue already in 2017 when the “on-chain” communication R&D started. The solution presented itself in the form of an OCC (i.e. on-chain communication) framework accompanied by a dedicated SDK (i.e. software development kit).**

Dr. Tali Režun, head of *Block Labs* R&D

***Keywords:*** *blockchain technology, decentralization, encryption, immutability, on-chain communication, permissionless communication, peer-to-peer communication, peer-to-peer communication wallet-to-wallet communication, non-custodial communication, encrypted communication*

## 1. CONTEXT

In the past decade, digital communication has become most relevant as digital data has become extremely valuable. Communication in the form of emailing, messaging and data file sharing forms personal and business relations. Humankind has grown a dependency on digital communication as it relies on and depends on it to be confidential, private, secure, or even intimate.

To understand the root of the problem, one must grasp the state of digital communication platforms which are currently used and, in most cases, based on ad/surveillance data mining models typical for Web2 applications. Users trade/pay the ease of access for their data, that has been created within the communication or interaction process. It’s more than obvious that users are paying dearly, but not just with metadata. The users are paying in; sharing behaviour; history; content, and; their digital lives in general. (*From Online to On-Chain, the Evolution of Digital Communication | by Dr. Tali Rezun | /4thtech | Oct, 2023 | Medium*, n.d.). While some messaging platforms offer end-to-end encryption, the metadata of the conversation and interactions are still being mined. According to (*(1) Iara on X: “Little Morning Tip: Get off Facebook & WhatsApp 💯 Https://T.Co/ASCvHpiWWs” / X*, n.d.), WhatsApp and Facebook together mine over 50 data points.

Legacy communication applications (i.e. email, messaging, data file transfers) are custodial by nature, meaning the platform holds custody over user communication and data, which brings the issue of access. While the majority of users have no problems accessing legacy email, messaging, or data file-sharing platforms, the “permissioned access” issue remains. Enforced usually based on censorship misbehaviour, de-platforming cases are well known leading to various cases of access restrictions. The fact remains, that the current legacy communication platforms are designed to grant permission for every email or message that we send based on pre-approval mechanics.

There is also the matter of data ownership. *Did you know that the moment you attach any data file to an email attachment or share it via any “free” messaging service or data file-sharing app there is a big data ownership loss possibility?*

Due to its current framework, legacy email and messaging platforms are less secure and do not provide any protection before cyber-attacks and ever-growing spam. According to Dataprot (*What’s On the Other Side of Your Inbox - 20 SPAM Statistics for 2023*, n.d.) nearly 85% of all emails are spam which translates into an average daily volume of 122.33 billion messages globally. Tessian research (*Email Security Resources - Research, Datasheets, Whitepapers - Tessian*, n.d.) suggests that throughout 2020, 1 in every 4,200 emails was a phishing email. Keeping your email un-infected and out of the millions of subscription services is close to impossible these days and cleaning the inbox has become a daily time-consuming task.

## 2. SOLUTION

The superiority of blockchain technology and its unique tamper-proof features was confirmed long ago and it is no longer considered a hype tech. According to (*Economic Commission for Europe Executive Committee Centre for Trade*

*Facilitation and Electronic Business Blockchain in Trade Facilitation: Sectoral Challenges and Examples*, 2019) blockchains ensure tamper-proof digital transactions through the use of cryptographic technology and automated consensus. Blockchain is made from a trail of validated facts. These facts can be anything from money, information or communication. As part of this digital system of record-keeping, each transaction and its details are validated and then recorded across a network of computers. Everyone who has access to the distributed ledger receives this information and the parties agree on the accuracy before the block is replicated, shared and synchronized among the entities. A Blockchain is virtually impossible to tamper with since each block of information references the block before it. In an age when trust is both elusive and held at a high premium, Blockchain presents a way to confirm, validate and authenticate values, events, information and communication. Smart contracts are codes or rules written into a digital program, which determine what happens when digital assets come in or when certain conditions are met. As data value grows exponentially, so does its privacy and the need for security.

Blockchain always offered the promise of enabling permissionless, secure, non-custodial, immutable communication with uninterrupted up-time, while retaining data and identity ownership, it is by design the right tool for the job. However, it could never really take off due to the scalability and cost constraints of early-generation blockchains. With the rise of the new generation blockchains, easier block space access, growing privacy awareness and coming Web3 mobile and Web3 adoption in general, the concept of "on-chain" communication could become a reality. The exclusive features native to Web3 are just too good to be overlooked.

***Web3;*** *According to (Web3 - Wikipedia, n.d.), Web3 also known as Web 3.0 is an idea for a new iteration of the World Wide Web which incorporates concepts such as decentralization, blockchain technologies, and token-based economics. Some technologists and journalists have contrasted it with Web 2.0, wherein they say data and content are centralized in a small group of companies sometimes referred to as "Big Tech". The term "Web3" was coined in 2014 by Ethereum co-founder Gavin Wood, and the idea gained interest in 2021 from cryptocurrency enthusiasts, large technology companies, and venture capital firms.*

*4thTech* addressed this issue already in 2017 when the "on-chain" communication R&D started. Due to the core principle; 1 email/message/data-exch = 1 L1/L2-TX in place, the right fit needed to be found between the protocol mechanics and underlaying L1s/L2s. Blockchain transactions are used for "on-chain" data and message exchange as one communication package (i.e. email, short message or data file transfer) represents one L1/L2 transaction. Blockchain acts as an underlying network infrastructure enabling immutability and transparency of the communication transactions executed by the *4thTech* protocols. Many protocol iterations and other deployments followed that resulted in the production version available today;

(1) 2017 genesis R&D of EVM [Mails] protocol; (2) 2018 [Mails] protocol deployment on Ethereum TestNet enabled first dMail & data file transfer use cases; (3) 2018 dedicated wallet and UI client development; (4) 2020 [Mails] protocol deployment on SI-Chain enabled decentralized eID, eDelivery and eNotary use cases; (5) 2020 X.509-to-Web3 dID framework; (6) 2021 [Mails] protocol deployment on Edgeware TestNet enabled first dMail & data file transfer use cases in the substrate ecosystem; (7) 2022 [Mails] protocol deployment on Solana TestNet enabled first dMail & data file transfer use cases in the Solana ecosystem; (8) 2021 [Chat] protocol deployment on Solana TestNet enabled first dChat use cases in the Solana ecosystem; (9) 2022 Encryptor Extension development enabled OCC encryption layer currently not supported in major wallets; (10) 2023 OCC SDKs development, and; (11) 2023 OCC white-label UI framework development.

***Validation:*** *After four years of 4thTech MVP (i.e., minimum viable product) early adopter testing and refinement, the technical feasibility and its practical potential have been proven, with that PoC (i.e., proof of concept) confirmed. Moving to production, the 4thTech framework enters the adoption phase offering an open-source SDK framework accompanied by a set of OCC white-labels. In May 2018 Adriatic Council awarded Dr Tali Režun with the Beyond 4.0 award for his dedication, promotion and accomplishment in the field of science, new technologies and innovation for the 4thTech blockchain concept (Adriatic Council | BEYOND 4.0 – LJUBLJANA, 25.05.2018. KRISTALNA PALAČA (BTC), n.d.). Other acknowledgements followed such as Solana FOURim Protocol endorsement following MainNet deployment (Solana on Twitter: "Decentralized, Encrypted Messaging, Built on #Solana" / Twitter, n.d.), Tron Hackathon wins (TRON Grand Hackathon 2022: Accelerate the Future - Devpost, n.d.) and so forth.*

*4thTech* spent the last five years developing foundations for Web3's first on-chain communication infrastructure. It manifested in the form of the OCC (i.e. on-chain communication) Framework. The technology utilises; smart contacts; blockchain networks; encryption, and; decentralized storage, to retain data ownership and enable OCC use cases.

***Core Primitives:*** *While various use cases are possible, let's use dMail and dChat as examples. The dChat W2W message exchange happens "on-chain" as one short message represents one L1 or L2 blockchain transaction. As dMail is data heavier, lite encrypted JSON objects are created to hold dMail metadata. The link to this metadata and checksum is recorded on the chain as a blockchain transaction. The same goes for W2W data file transfers where; 1 data file package transfer = 1 L1/L2-TX. So again, the core primitive described by the formula below applies.*

**💡1 email/message/data-exch = 1 L1/L2-TX**

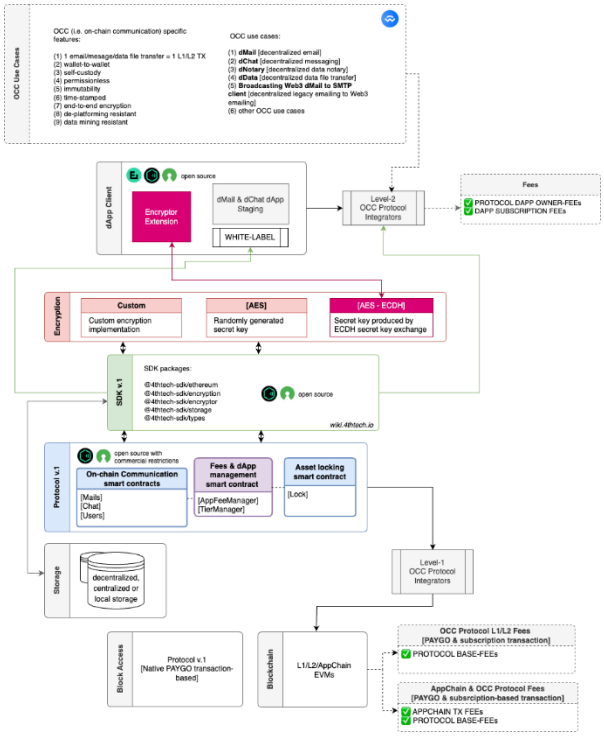
*Every wallet becomes an "on-chain" identity, and the message or data vault can be accessible (i.e. decrypted) only with users' private keys! There are three encryption options available within the protocol; (1) custom encryption; (2) AES-randomly generated secret key (i.e. Advanced Encryption Standard), and; (3) AES secret key produced by ECDH (i.e. Elliptic-Curve Diffie-Hellman).*

**💡not your keys = not your email/message/data**

## 3. INFRASTRUCTURE BY LAYERS

Zooming out, the architecture is quite straightforward. There are UI clients built on top of the OCC SDK, powered by protocols, encryption, storage, and blockchain networks. The OCC framework architecture was designed to be as lightweight and modular as possible while retaining core decentralization primitives. No personal data whatsoever is collected, and the only party with access to communication data is the user himself. Code is law principle applies! Connected by the OCC SDK, four main legos complete the on-chain communication framework; (1) OCC Protocol; (2) blockchain network; (3) encryption, and; (4) decentralized storage.

To be able to establish Web3's first on-chain communication standard, the OCC Protocol will need to be available for many L1s and L2s. To support "on-chain" communication at scale, the deployment of on-chain communication-specific AppChain would be needed in the future.




*Infrastructure by layers: https://github.com/4thtech/static-assets/raw/main/pdf/infrastructure_by_layers.pdf*

### 3.1. BLOCKCHAIN LAYER

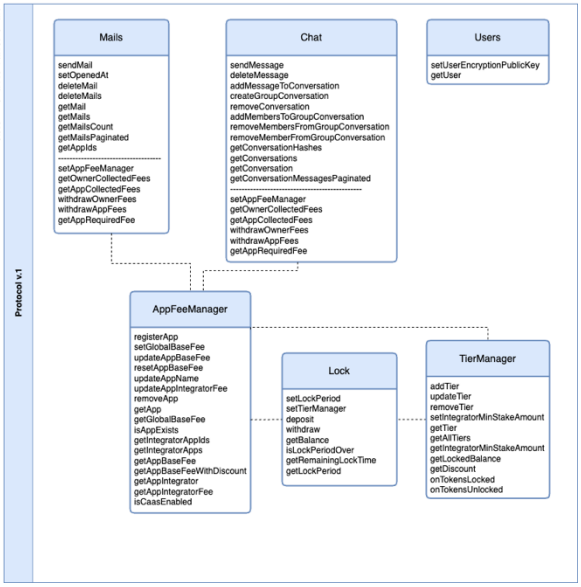
The OCC Protocol is EVM-based and out-of-the-box interoperable with the majority of EVM (i.e. Ethereum virtual machine) L1/L2 blockchain networks. The OCC Protocol deployment is under the domain of the *4thTech* Level-1 integrators. To enable "true" usable decentralized communication there are three factors to consider; (1) network decentralization; (2) network transaction time to finality (i.e. faster the finality, faster the on-chain communication), and; (3) network transaction cost.

### 3.2. STORAGE LAYER

Four storage databases are forming within the OCC framework; (1) if we take a look at the dMail and dChat as an example, blockchain is used to store; (1.1) a link to the dMail JSON metadata, timestamp, checksum & sender address; (1.2) dChat encrypted message, timestamp & sender address; (2) decentralized storage is used for the temporary or permanent storage of encrypted communication, data files and JSON files (i.e. dMail, subject & content attachment location); (3) integrators can also opt for more centralised storage such as cloud storage; (4) user local storage is used to storing; (4.1) wallet private keys; (4.2) dMail & dChat content hash, and; (4.3) user-initiated backup of conversations, data files and reports.

### 3.3. PROTOCOL LAYER

With many iterations behind, the six smart contracts crystalized and are forming the core OCC Protocol layer, enabling "on-chain" communication at scale; (1) Mails; (2) Chat; (3) Users; (4) AppFeeManager; (5) Lock, and (6) TierManager.




*Protocol v.1 smart contract schematic: https://github.com/4thtech/static-assets/raw/main/pdf/protocol-structure.pdf*

Two main smart contracts are enabling the main use cases; (1) Mails, and; (2) Chat. While [Mails] smart contract is used for data exchange over the blockchain, the [Chat] is a smart contract used for decentralized, encrypted short message exchange over the blockchain.

[Mails] smart contract is implementing the following methods;

(1) sendMail: self-explanatory
(2) setOpenedAt: recipient can mark read mail timestamp
(3) deleteMail: self-explanatory
(4) deleteMails: self-explanatory
(5) getMail: self-explanatory
(6) getMails: self-explanatory
(7) getMailsCount: returns the number of received mails
(8) getMailsPaginated: self-explanatory
(9) getAppIds: self-explanatory

[Chat] smart contract is implementing the following methods;

(1) sendMessage: self-explanatory
(2) deleteMessage: self-explanatory
(3) addMessageToConversation: self-explanatory
(4) createGroupConversation: self-explanatory
(5) deleteGroupConversation: self-explanatory
(6) addMembersToGroupConversation: self-explanatory
(7) removeMembersToGroupConversation: self-explanatory
(8) getConversationHashes: each conversation has its own hash, this method returns an array of user-participation-conversation hashes
(9) getConversations: self-explanatory
(10) getConversation: self-explanatory
(11) getConversationMessagesPaginated: self-explanatory

***More Protocol-related information:***
*https://github.com/4thtech/smart-contracts*

### 3.4. SDK LAYER

Built on top of the protocol stack, the OCC TypeScript/JavaScript plug-and-play SDKs stand ready for

security-enabled social communication scaling in the multi-chain universe. The OCC SDK consists from five packages; (1) @4thtech-sdk/ethereum; (2) @4thtech-sdk/encryption; (3) @4thtech-sdk/encryptor; (4) @4thtech-sdk/storage, and; (5) @4thtech-sdk/types.

***More SDK-related information:***
*https://github.com/4thtech/sdk-js*

### 3.5. ENCRYPTION LAYER

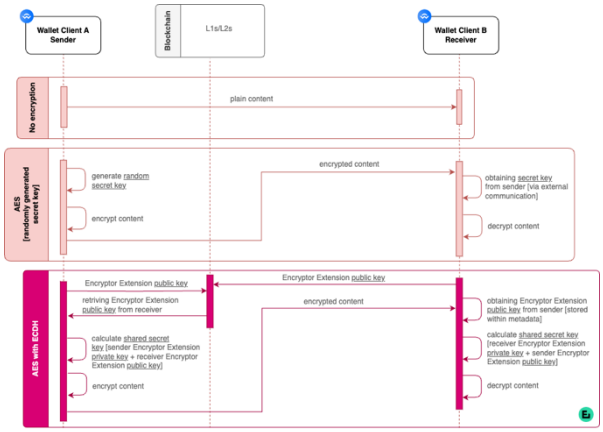
To enable various use cases there are several communication encryption options available; (1) no encryption, where plain unencrypted content is shared between wallet client A (i.e. sender) and wallet client B (i.e. receiver); (2) custom encryption where integrators have the option to develop their specific encryption implementations, and; (3) AES (symmetric, secret key encryption);

(3.1) randomly generated secret key;

a random secret key is generated to encrypt content, which is shared between wallet client A (i.e. sender) and wallet client B (i.e. receiver). Content is encrypted with AES encryption. The receiver obtains the secret key from a sender using external communication (i.e. email, chat...) to decrypt the content.

(3.2) secret key produced by ECDH secret key exchange using Encryptor extension;

the secret key is produced with ECDH secret key exchange. The sender needs the wallet client B (i.e. receiver) "Encryptor Extension" public key to be recorded on the blockchain. "Encryptor Extension" is used to calculate the shared secret key.




*Protocol v.1 smart contract schematic: https://github.com/4thtech/static-assets/raw/main/pdf/4thTech-encryption-schematic.pdf*

***Note:** Natively AES-256-GCM is used for the encryption algorithm.

### 3.6. APPLICATION LAYER

*4thTech's* goal is to support permissionless Level-2 integrator onboarding of on-chain communication dApps via the OCC SDK. To achieve this, some unexisting infrastructural legos had to be developed to enable out-of-the-box onboarding; (1) FOURwaL, TestNet multi-chain wallet; (2) Encyptor Extension, which adds a communication encryption layer currently not supported in major wallets, and; (3) OCC UI white-lable framework.

#### 3.6.1. FOURwaL EXTENSION

While the OCC framework now enables and supports interoperability with all major wallets (e.g. MetaMask), use case-specific wallet had to be developed in the early days of the project. OCC dedicated TestNet wallet framework served as a gateway connecting pioneer users with dID, dMail, dChat and dNotary UI back in years 2018 to 2020. As a non-custodial gas wallet, it also manages RSA public and private keys. FOURwaL utilises advanced encryption standards (i.e. AES), with a combination of RSA encryption and hash algorithm 256 (i.e. SHA 256) to secure permissionless, non-custodial and immutable communication and data exchange. Furthermore, the FOURwaL supports multi-chain accounts and serves as a dID on Ethereum, Tolar HashNet, Edgeware, Solana, Moonbeam, Tron, Bittorent Chain and Evmos and is still being used in a TestNet environment, while serving as a white-label wallet framework powering many projects.

***Quote;** *"We build the FOURwaL add-on from the ground up. The challenge was to build the extension with a unique blockchain data exchange feature. I can say with certainty that the FOURwaL extension code is unique and the first of its kind! "*

*Denis Jazbec, 4thTech*

***More FOURwaL-related information:***
*https://github.com/4thtech/four-wal*

#### 3.6.2. ENCRYPTOR EXTENSION

Encryption and decryption of the communication or shared data files is possible with the Encryptor Extension. Used to enable ECDH key agreement protocol, the Encryptor Extension adds the "on-chain" communication encryption layer currently not supported in major wallets. It creates an elliptic curve key pair and computation of the shared secret key of the receiver/sender.

***More Encryptor-related information;***
*https://github.com/4thtech/encryptor-extension*

#### 3.6.3. OCC UI WHITE-LABEL

The OCC white-label framework enables fast and easy builds of dApps such as decentralized email, messaging or data file transfers. White-label-based modern minimalistic design style emphasizes simplicity with a simple intuitive but effective navigation and setup system. A simple user interface has been developed to offer a step-by-step setup enabling the best possible user experience.

***More White-label-related information:***
*https://github.com/4thtech/white-label-client*

## 4. USE CASES

With Web3 social on the rise, on-chain communication remains one of the last undiscovered frontiers. Until now, there was no permissionless developer-friendly infrastructure to enable out-of-the-box on-chain communication application development. Hopefully, with that out of the way, the developer community can now focus on building communication applications with Crypto-specific features and use cases. The OCC SDK enables various use case iterations. Arthera chain for example, is exploring possibilities of integrating the on-chain messaging as a part of their native wallet, enabling Web3's first on-chain messaging subscription (*Arthera*, n.d.). There is also work being done on integrating on-chain messaging into a decentralized

OTC platform. While many interesting OCC use cases are being explored, the main focus of pioneer integrators goes to; dMail; dChat, and; data file transfers dApps.

We can refer to dMail and dChat as decentralized, self-custodial, E2E encrypted, immutable, and permissionless on-chain email and messaging applications (*IMMU3, DMail & DChat Technology Integrator*, n.d.). Build with the OCC SDK and based on the OCC Protocol v.1, Encryptor Extension, PollinationX decentralized storage, white-label framework, and powered by blockchain networks, the Immu3 dMail & dChat UIs showcase the UI/UX for future on-chain communication. 4P is another project building on top of the OCC infrastructure. They are introducing a set of smart contracts on top of the dMail & dChat framework that will enable different right-to-access models and propose enhanced functionalities for their native FOUR token holders. W3XShare changes the way large and sensitive data is transferred (*W3XShare*, n.d.). It leverages OCC Protocol v.1, encryption framework, PollinationX decentralized storage, and blockchain networks to provide a secure and self-custodial solution for encrypted data file transfer between wallets.

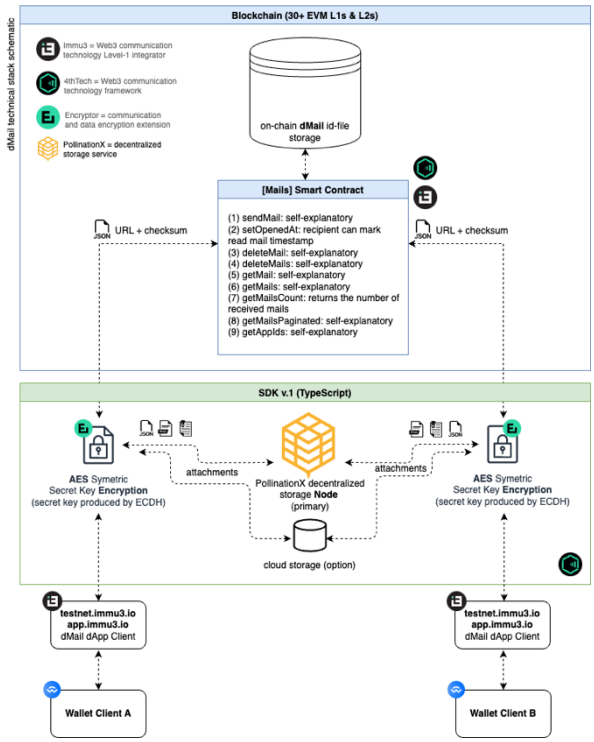
These are all crypto-native use cases designed for crypto-native users. To bridge the gap, R&D is in progress towards a stand-alone desktop application that would enable users to send or receive E2E encrypted emails via an underlying blockchain network using their existing traditional email client applications such as Microsoft Outlook or Apple Mail. We call it a "Broadcasting Web3 dMail to SMTP client". Built with the OCC SDK, the desktop client is designed to add blockchain and encryption layers to the legacy email enabling blockchain decentralization, immutability, and security while users pay for the transaction packages using a credit card.

*4thTech* framework can enable 1000s of "on-chain" communication dApps to Blum on Web3, creating various use cases. With protocol Lego in place, it's just a matter of finding the right market and product fit.

### 4.1. DMAIL

dMail refers to decentralized email. Composed of; (1) subject; (2) content, and; (3) attachment, the dMail can be from a few kilobytes to 20 megabytes in size (i.e. dMail attachment size is limited to 20 megabytes). Based on the *4thTech* [Mails] smart contract, SDKs and white-label framework, the Level-1 integrator *Immu3's* dMail UI showcases the UI/UX for future on-chain communication. As the first white-label iteration, the *Immu3* dApp reveals the dMail UI/UX and acts as a sandbox for this new "on-chain" communication technology.

Compared to dChat, where all messaging happens "on-chain", the dMail is data heavier due to attachments and sizable content. Encrypted JSON files are stored on decentralized storage to hold the dMail metadata while a link pointing to the file along with file checksum is recorded on-chain in the form of an L1 transaction. So again, the core primitive; 1 email = 1 L1 TX applies.




*dMail schematic: https://github.com/immu3-io/static-assets/raw/main/pdf/dMail_technical_schematic.pdf*

***Phases within dMail:*** (1) to enable end-to-end encryption, both sender and receiver need to install and run "Encryptor Extension"; (2) dMails are encrypted with AES while ECDH key agreement protocol is used for generating the secret key (i.e. used in AES encryption); (3) all encrypted attachments are stored on decentralized storage via PollinationX; (4) JSON metadata file is created that includes sender and recipient details, dMail subject, content, and attachment details (i.e. name, stored location, and checksum); (5) JSON metadata file is encrypted with AES encryption and stored on decentralized storage; (6) JSON metadata file URL and checksum are sent to L1 or L2 [Mails] smart contract, and; (7) after transaction finality, the receiver loads and decrypts a JSON metadata file and loads and decrypts all the attachments.

***Note:** "Encryptor Extension" generates EC (i.e. Elliptic Curve) keypairs and stores the public key for its ETH address on a smart contract.*

***More dMail-related information:***
*https://wiki.immu3.io/dapps-and-clients/intro-to-dmail*

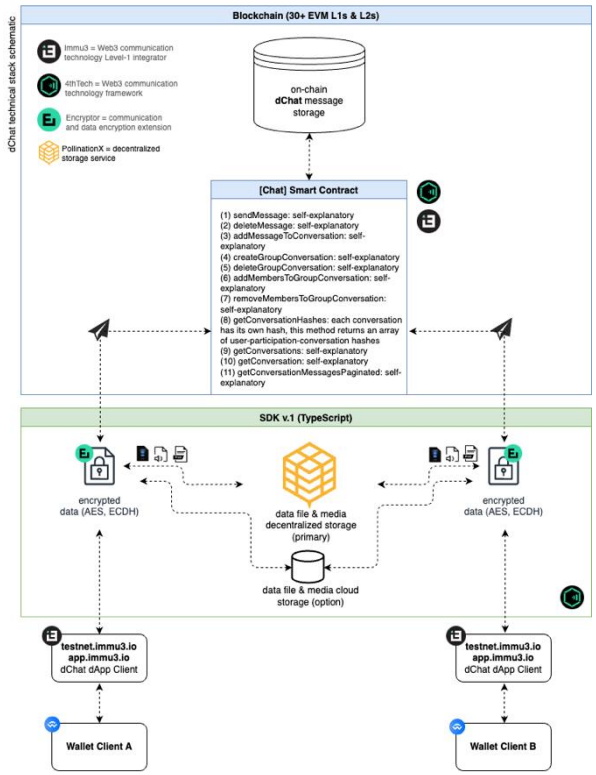
### 4.2. DCHAT

dChat refers to decentralized messaging. Composed from; (1) content, and; (2) possible data files (i.e. media files, photos...), the individual message can be from a few kilobytes to 20 megabytes in size (i.e. message data file size is limited to 20 megabytes). Based on the [Chat] smart contract, SDKs and white-label framework, the Level-1 integrator *Immu3's* dChat UI showcases the UI/UX for future on-chain communication. As the first white-label iteration, the *Immu3* dApp reveals the dMail UI/UX and acts as a sandbox for this new on-chain communication technology.

The OCC Protocol leverages trust sourced from the blockchain to enable E2EE W2W message exchange in the form of; (1) "on-

chain" direct messaging; (2) "on-chain" group chat, and; (3) NFT or token-curated "on-chain" chats.

Due to fast transaction finality (i.e. 0.89s), the dChat as [Chat] protocol and the UI were first developed for the Solana VM (i.e. virtual machine). The L1 serves as an immutable network exchanging short encrypted messages between wallet addresses; 1 message = 1 L1-TX. The messages are not stored on any centralised server but are temporarily stored on the L1 itself and in the case of the Solana blockchain deleted after 7 days. Smart contracts are used to facilitate two unique requirements; (1) saving instant messages from the sender, and; (2) retrieving the instant messages from receivers.




*dChat schematic: https://github.com/immu3-io/static-assets/raw/main/pdf/dChat_technical_schematic.pdf*

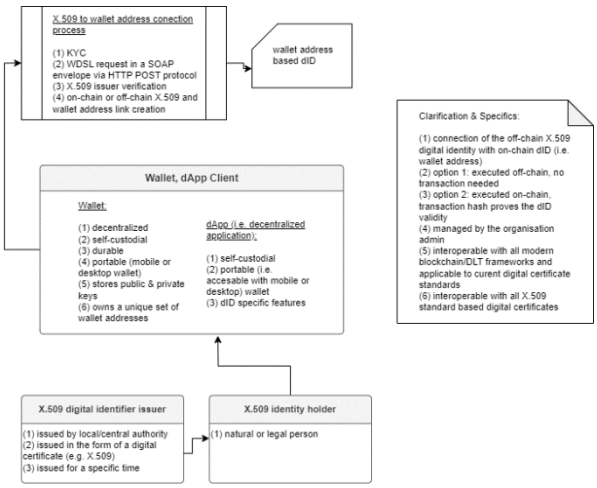
***Phases within dChat:*** *(1) to enable end-to-end encryption, both sender and receiver need to install and run Encryptor extension; (2) dChat messages are encrypted with AES (i.e. Advanced Encryption Standard) while ECDH (i.e. Elliptic-Curve Diffie-Hellman) key agreement protocol is used for generating the secret key (i.e. used in AES encryption); (3) all encrypted attachments are stored on decentralized storage; (4) message data is sent to L1 or L2 [Chat] smart contract, and; (5) after transaction finality, the receiver decrypts message content.*

***Note:** At the final stage, the message hash is written on the blockchain. While the message is temporarily stored on-chain, attachments are stored on decentralized storage.*

### 4.3. dID (i.e. decentralized digital identity)

Digital identity is a crucial part of any online communication solution. Unlike Web2 where our identities are disclosed and locked by the intermediaries, the decentralised Web3 "on-chain" identities (i.e. dIDs) need no third party, are portable and completely anonymous until and if the users decide to tie them to the off-chain identity. Web3 dIDs are born with the creation of a wallet account that represents the user's decentralised identifier. Users can interact with permissionless Web3 "on-chain" systems using the same wallet account without revealing their physical identifiers like phone numbers or email addresses. As the "on-chain" communication becomes more adopted, there will be specific use cases where users will need an "off-chain" identity verification connected to their "on-chain" identity.

*4thTech* approaches this challenge by utilising the X.509 digital identity standard. By connecting the "off-chain" X.509 digital identity issued by the verified issuer with the *4thTech* dID service the bridge is formed between the "off-chain" identity and "on-chain" wallet address. Each user owns their wallet address accessible only with his or her private key. Wallet address acts as a verifiable credential (i.e. VC), which is robust, non-transferable and can be verified/linked to the verifiable X.509 "off-chain data". The process enables a self-sovereign framework of data (i.e., data files and metadata) authorisation and ownership representation. All dID processes are fully automated and decentralized by their design, thereby enabling users to have full control and ownership of any data that may be connected with them. Attached with a specific blockchain wallet address the data can now be verified, while the X.509 digital certificate standard provides the off-chain connection with individuals and organizations.




*dID schematic: https://github.com/4thtech/static-assets/raw/main/pdf/4thTech-dID.pdf*

****Note:** The 4thTech dID framework is compatible with all the Ethereum-based addresses, additionally it supports Substrates, Solana & Tron.*

**X.509 standard:** Digital certificate standard X.509 Public Key Infrastructure can be used for data encryption, notarization of signed data, digital signature, digital identity verification and timestamp. With various European Union certificate publications, the X.509 standard is widely used and as such appropriate for blockchain digital identity integration. The X509 Public Key Infrastructure is also approved by eIDAS (i.e., electronic IDentification, Authentication and Trust Services).

***X.509 connection process:*** *(1) the user selects the X.509 standard qualified digital certificate, associated with an individual or organisation; (2) a simple KYC form is completed with the certificate holder's information; (3) dID service prepares and sends WSDL request in a SOAP envelope via HTTP POST protocol to the government managed automated service (i.e., the issuer of the X.509 certificate), which replies with the verification. If the user's tax number corresponds with the qualified digital certificate serial number, the user is successfully verified; (4) A link is created by the*

*dID between the user's X.509 digital certificate and its 4thTech wallet address.*

### 4.4. DNOTARY (on-chain document notarisation)

Blockchain data verification or notarisation can be described as a fraud prevention process that enables data authenticity and guarantees that the data has not been changed in the course of a transaction between blockchain wallets. Usually, the physical notary acts as an intermediary and provides the needed trust factor between parties, but in the case of *4thTech dNotary*, the system sources the needed trust directly from the underlying L1 blockchain.

***Solution:*** *4thTech dNotary* can be also described as a digital notary of the decentralized world as it provides sensitive data file timestamp and origin verification. During the exchange between wallets, the data file hash/checksum is stored on the blockchain. In the case of future disputes over the data file authenticity, the user can match the data exchange transaction hash stored on the blockchain ledger. The service is capable of; (1) timestamping digital data files; (2) providing the file checksum verification of the digital data authenticity, and; (3) providing access and review of the received data file details.

## 5. BLOCK SPACE ACCESS

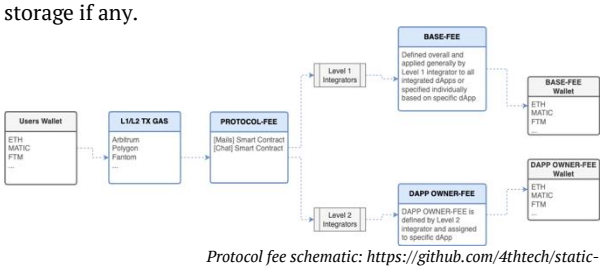
Every message, email or another form of "on-chain" communication bears the cost of a blockchain transaction, which needs gas to be confirmed. Compared with Web2 solutions that offer "free" online communication this barrier to entry looks quite steep. Deeper research reveals that Web2 communication is far from "free". Compared with Web3 which settles transactions in L1/L2 assets, Web2 charges communication transactions with user data.

L1/L2 transaction gas is currently the biggest cost factor of "on-chain" communication, but use cases are already emerging where transaction gas is being shared with dApps, which could result in lower end-user costs. Tron, for example, already enables users to stake TRX and in return offer free bandwidth with practically gasless transactions.

We are still very early and block space subscription is still evolving. It may look complicated and costly to access block space now but it will become more accessible. It's the same as with internet access, we don't think any more about the MBs cost, we just use it. The same will be with block space, as blockchain evolves, access will become more organic, easy and accessible.

## 6. FEES

Parallel to the underlying L1/L2 transaction gas cost, the PROTOCOL-FEE is determined by the protocol integrator and also settled on the smart contract level (i.e. applicable for every communication transaction). Total user cost equals the sum of the L1/L2 transaction gas, the PROTOCOL-FEE and the cost of storage if any.




*Protocol fee schematic: https://github.com/4thtech/static-assets/raw/main/pdf/4thTech-protocol-fees-schematic.pdf*

Protocol build-in monetisation layers enable independent out-of-the-box integrator economics, permitting developers to focus on application UI/UX features.

***Note:*** Level-1 integrators can set the desired protocol BASE-FEEs, while Level-2 integrators can set their protocol DAPP OWNER-FEEs.

## 7. INTEGRATOR LICENCING

There are two integrator licences available within the ecosystem; (1) Level-1 integrator licence and; (2) Level-2 integrator licence.

Level-1 integrator licence or so-called "Enterprise" integrator licence is available via *Block Labs* [*4thTech*] and is meant for traditional businesses or offices, L1s, wallets, and existing applications. A permissionless Level-2 integrator licence is available via *Immu3* and is perfect for teams wanting to build their own "on-chain" communication dApps.

## 8. BLOCKCHAIN, GDPR & LEGAL INTEROPERABILITY

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). The GDPR mandates that EU visitors be given several data disclosures. General Data Protection Regulation ("GDPR") compliance is not about the technology, it is about how the technology is used. There are many tensions between the GDPR and blockchain technology, but they are due to two overarching factors; (1) the first is that the GDPR requires an identifiable controller against whom data subjects can enforce their legal rights under EU data protection law, and; (2) the GDPR requires that data can be modified or erased where necessary to comply with legal requirements. Sending personal data through the blockchain presents quite a big legal challenge. GDPR demands responsibility for ensuring compliance, which can become demanding, especially in the permissionless public blockchain network. GDPR allows personal data processing only in the case of explicit authorization by the subject. To achieve legal technology compliance, the *4thTech* protocol is designed and built according to the EU and GDPR guidelines with the main GDPR compliance features; (1) transaction is authorized by the user; (2) blockchain network is used for transactions that Include link to encrypted communication package, that only the receiver can open using his or her private key; (3) no personal information is located in the blockchain transaction; (4) send encrypted communication package data are stored in the off-chain data repository (i.e. data repository of user choice and control) and can be erased on the user request; (5) the protocol records only links to encrypted files and hashes of the encrypted content on the blockchain, what safeguards the rights of individuals to confidentiality and privacy, and; (6) the sender and the receiver jointly assume responsibility for complying with the GDPR and establishing a lawful basis. According to (Fridgen Nikolas Guggenberger Thomas Hoeren Wolfgang Prinz Nils Urbach Johannes Baur et al., n.d.), this GDPR-blockchain solution falls under the "pseudonymization" approach in which, data on the blockchain is pseudonymized so that it only qualifies as personal data about those participants who possess certain additional information that allows attribution of the data to a natural person.

**__Note:__ The [Mails] protocol does not store any personal data on the blockchain. The data is stored "off-chain". The protocol records links to encrypted files and hashes of the encrypted content on the blockchain. The hashing of exchange data enables GDPR compliance, for example, if there were a request to delete some data (i.e., attached documents), the network controller would be able to delete the requested data from off-chain storage, leaving what would then become an empty hash "on-chain".*

## 9. CONCLUSION

Access to secure, self-custodial, P2P communication should be accessible and available. As digital communication is one of the biggest use cases that need to be solved by Web3, other projects are trying to solve the same challenges, each with its specific approach. According to the competitor's analysis, *4thTech's* "1 email/message/data-exch = 1 L1/L2-TX" approach is unique, but also the most challenging to develop.

At its core, *4thTech* prevents identity theft, Web2 data tracking or data mining, while it's impervious to invasive ad campaigns and user content surveillance. The metadata created between the user wallet and the dApp is still vulnerable, but with the development of mixnets, such as HOPR this issue is also being resolved (*HOPR | Blockchain Data Protection and Privacy*, n.d.). Despite the current industry-specific adoption challenges, early blockchain technology adopters will be able to secure a considerable advantage regarding technology understanding and tailored use-case solutions. Blockchain technology adoption is here with technology-specific advanced solutions that will change the digital landscape as we know it.

## 10. DISCLAIMER



References;

*(1) iara on X: "Little morning tip: Get off Facebook & WhatsApp 💯 https://t.co/ASCvHpiWWs" / X*. (n.d.). Retrieved November 7, 2023, from https://twitter.com/iara_modarelli/status/1709574369788252500?s=20

*Adriatic Council | BEYOND 4.0 – LJUBLJANA, 25.05.2018. KRISTALNA PALAČA (BTC)*. (n.d.). Retrieved March 28, 2020, from http://adriatic-council.eu/beyond-4-0-ljubljana-2018/

*Arthera*. (n.d.). Retrieved November 8, 2023, from https://www.arthera.net/

*Economic Commission for Europe Executive Committee Centre for Trade Facilitation and Electronic Business Blockchain in Trade Facilitation: Sectoral challenges and examples*. (2019).

*Email Security Resources - Research, Datasheets, Whitepapers - Tessian*. (n.d.). Retrieved September 25, 2022, from https://www.tessian.com/resources/

Fridgen Nikolas Guggenberger Thomas Hoeren Wolfgang Prinz Nils Urbach Johannes Baur, G., Brockmeyer, H., Gräther, W., Rabovskaja, E., Schlatt, V., Schweizer, A., Sedlmeir, J., Wederhake, L., Babel, M., Brennecke, M., Camus, P., Drasch, B., Guggenberger, T., Lämmermann, L., Lockl, J., Radszuwill, S., Rieger, A., Schmidt, M., Thanner, N., … Dlt, V. (n.d.). *E WA NDT E I NF ORM AT I O NST EC H NI K FI T*.

*From online to on-chain, the evolution of digital communication | by Dr. Tali Rezun | /4thtech | Oct, 2023 | Medium*. (n.d.). Retrieved November 6, 2023, from https://medium.com/4thtech/from-online-to-on-chain-the-evolution-of-digital-communication-0fb201f98df1

*IMMU3, dMail & dChat Technology Integrator*. (n.d.). Retrieved November 8, 2023, from https://immu3.io/

*Solana on Twitter: "Decentralized, encrypted messaging, built on #Solana" / Twitter*. (n.d.). Retrieved October 21, 2022, from https://twitter.com/solana/status/1482045683364511759

*TRON Grand Hackathon 2022: Accelerate the Future - Devpost*. (n.d.). Retrieved October 21, 2022, from https://tron.devpost.com/project-gallery

*W3XShare*. (n.d.). Retrieved November 8, 2023, from https://w3xshare.com/

*Web3 - Wikipedia*. (n.d.). Retrieved November 6, 2023, from https://en.wikipedia.org/wiki/Web3

*What's On the Other Side of Your Inbox - 20 SPAM Statistics for 2023*. (n.d.). Retrieved November 6, 2023, from https://dataprot.net/statistics/spam-statistics/