Block Labs publications
Type: Whitepaper
Status: Published
Updated: 21.10.2022
Luxembourg 2022
https://4thtech.io/

Web3 Secured W2W dMail & dChat Communication Infrastructure --4thTech Whitepaper--

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 and security. Instead of providing a safe environment for online communication, the internet evolved into a system of centralized intermediaries which enable mass surveillance and data mining to enforce intrusive ad campaigns or sell our data as they see fit. Furthermore, current Web2 services established models that prevent users to own their data or their identities. Now more than ever secure online communication, privacy and data ownership are becoming more and more important as we depend on them every day. Enters 4thTech (i.e. 4thpillar Technologies) with Web3s first L1-secured W2W (i.e. wallet-to-wallet) E2EE (i.e. end-to-end encrypted) dMail & dChat communication infrastructure powered by dedicated SDKs. The initiative strives to enable a self-sovereign framework of on-chain data exchange and ownership representation while leveraging the power of blockchain to facilitate true Web3 security. This whitepaper was written as a hybrid addressing the *4thTech* protocol benefits and solutions.**

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

Keywords: *digital transformation, blockchain technology, decentralization, Web3, peer-to-peer, online trust, online security, online privacy, 4thtech, dmail, dchat, wallet to wallet, encryption, l1, multi chain*

1. INTRODUCTION

Blockchain always offered the promise of enabling secure, immutable W2W communication, while retaining data and identity ownership, it is by design the perfect security tool. However, it could never really take off due to the scalability and cost constraints of early-generation blockchains. With the rise of new generation blockchains, privacy awareness, and coming Web3 mobile and Web3 adoption in general, the on-chain W2W email & messaging could become the dominant communication and as such will be the future of secure online communication.

4thTech addressed this issue already in 2017 when the R&D started; (1) 2017 initial research and concept development of Ethereum-based W2W E2EE FOURdx Protocol with dMail & data file exchange use cases; (2) 2018 FOURdx Protocol EVM-based SC (i.e. smart contact) deployment on Ethereum MainNet; (3) 2018 Beta infrastructure development (i.e. UI platform, wallet); (4) 2020 FOURdx Protocol EVM-based SC SI-Chain deployment with decentralized eDelivery use case; (5) 2020 FOURns Protocol deployment with dNotary use case; (6) 2020 X.509-to-Web3 dID TestNet deployment; (7) 2021 FOURdx Protocol Substrate-based SC Edgeware MainNet deployment with dMail & data file exchange use cases; (8) 2022 FOURdx Protocol Solana-based Program MainNet deployment with dMail & data file exchange use cases; (9) 2022 FOURim Protocol Solana-based Program MainNet deployment with dChat use case; (10) 2022 dMail & dChat JavaScript EVM SDKs development; (11) 2023 FOURdx Protocol EVM-based SC Tron & BTT MainNet deployment with dMail & data file exchange use cases, and; (12) 2023 FOURim Protocol EVM-based SC Tron & BTT MainNet deployment with dChat use cases. With core fundations build, there is still a lot to do with the roadmap stretching to the next 4 years.

****Read more:*** *https://4thtech.io/roadmap/*

Blockchain; The superiority of blockchain technology and its unique tamper-proof features was confirmed, 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) blockchain ensures tamper-proof digital transactions through the use of cryptographic technology and automated consensus. In the case of 4thTech, blockchain transactions are used for on-chain message exchange as one message (i.e. email or short message) represents one L1 transaction. This is how communication immutability is achieved. Blockchain provides a decentralized and secure shared digital ledger, which gives participating parties a way of validating information related to a transaction. Blockchain is made from a trail of validated facts. These facts can be anything from money to information. 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 and information. 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. The need for immutable, unmodifiable E2EE dMail and dChat is imminent. Current systems or other Web2 data exchange services are not private or secure and do not fulfil the task in question. Furthermore, current Web2 services established models that prevent users from owning their data, so now more than ever secure online communication, privacy and data ownership are becoming more and more important as we depend on them every day.

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 version 2.0, the *4thTech* stack enters the adoption phase and becomes globally interoperable, available as a L1 communication standard on the majority of public blockchains.

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 4THPILLAR Blockchain platform. (*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* (*HolaChain, Web3 Secured W2W Communication Infrastructure | Devpost,* n.d.) *and so forth.*

2. 4THTECH

Build as a Web3 infrastructure technology occupying L1, protocol, SDK and encryption layers, the project aims to; (1) enable permissionless multi-chain (i.e. 20+ L1) communication standard that enables 1000s of dMail & dChat dApps to evolve on Web3, via TypeScript/JavaScript SDKs & White-labels, while its core Web3 primitive; one message = one L1 transaction utilises L1s security to enable immutable E2EE W2W on-chain communication; (2) develop dMail & dChat communication-specific L1; (3) contribute to the next Web3 adoption wave, and; (5) pioneer the future of encrypted, immutable and decentralized on-chain communication.

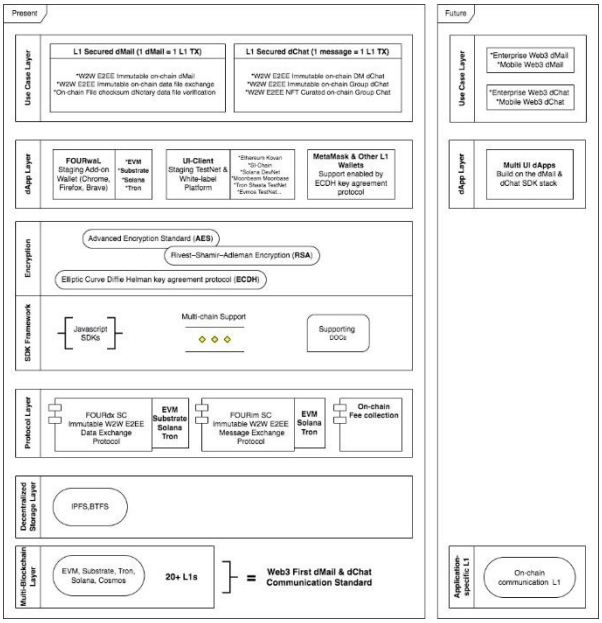
Core Primitives; (1) One Email/Message = One L1 Transaction. The dChat W2W message exchange happens on-chain, as one short message represents one L1 transaction. As dMail is data heavier, lite encrypted JSON files are created to hold dMail metadata (i.e. subject, content & attachment location) while the link to this JSON metadata & checksum (i.e. dMail content structure SHA-256 hash) are recorded on-chain in the form of an L1 transaction. Again, the core primitive "one email/message = one L1 transaction" applies;

(2) Not Your Keys = Not Your Email/Message. Every wallet becomes an on-chain identity & message data vault, accessible/decrypted only with users' private keys;

(3) L1 security + Encryption + Decentralized storage = Web3 Secured W2W dMail & dChat Communication. True dMail & dChat security is achieved by utilising L1s security, encryption-hashing cocktail (i.e. AES, RSA, SHA-256, ECDH) and decentralized storage.

4thTech brand; According to many, there are three fundamental technological developments in human history; (1) the invention of electricity; (2) the invention of the microprocessor, and; (3) the invention of the internet. We are certain, that the invention of blockchain technology is the fourth fundamental technology pillar, which revolutionary applications will yet be revealed to the world.

Infrastructure by layers; To be able to establish Web3s first dMail & dChat communication standard, the solution will be available on 20+ L1s. To support enterprise and mobile on-chain communication in the future, the deployment of application-specific L1 is needed and a part of project roadmap. Decentralized storage is needed to manage dMail & dChat attachments (e.g. media files, data files ...). The core solution consists of two smart contacts; (1) FOURdx Protocol, and; (2) FOURim Protocol. Developed as multi-chain interoperable, the smart contacts support EVM, Substrate, Solana, Tron frameworks and will support Cosmos stack in the future. Build on top of the protocol stack, the dMail & dChat TypeScript/JavaScript plug-and-play SDKs stand ready for security-enabled multi-UI/use case social scaling in the multi-chain universe. Besides using L1 security to enable true immutability, the encryption-hashing cocktail (i.e. AES, RSA, SHA-256, ECDH) provides the final lego of protection. The project's main focus is directed to infrastructural protocols & SDK development, so 1000s of dMail & dChat dApps could evolve easier and faster forming unique use cases and UIs supporting the ever-growing demand.



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

3. MULTI-CHAIN LAYER

One way to achieve immutability of internet communication is to put it on-chain (i.e. one message = one transaction). Blockchain always offered the promise of enabling secure, immutable W2W communication, while retaining data and identity ownership, it is by design the perfect security tool. On-chain communication should provide sufficient security, assuming the underlying protocol is decentralised enough. However, it could never really take off due to the stability, scalability and cost constraints of early-generation blockchains *(Block Labs research 2017 – 2021)*. Extensive research is being currently conducted on new-gen blockchains including factors such as decentralization, performance, microtransaction cost and transaction time to finality. Based on the findings, 20+ networks will be chosen to host the future 4thTech dMail and dChat communication standard. As a multi-chain EVM, Substrate, Solana and Tron framework, the protocols currently enable the dMail & dChat interoperability with Ethereum, Edgeware, Moonbeam, Solana, Tron, BTT, Evmos chains with more coming with every progressing month.

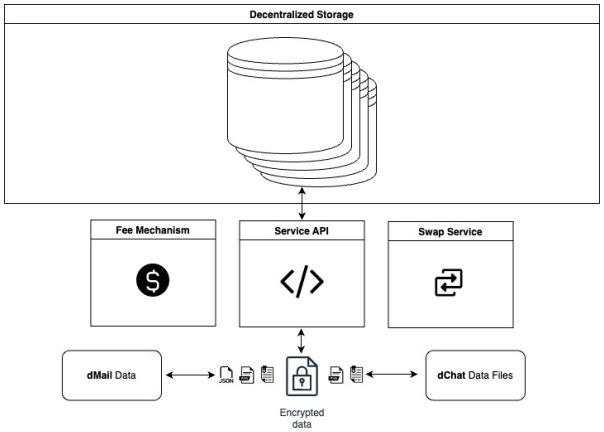
To be able to support future communication also on mobile and to offer on-chain communication to the enterprise sector, an application-specific blockchain is needed. A blockchain that will be used only for its one and only purpose, processing communication transactions. New modern blockchains bring

new scaling models such as Tron SideChains, Avalanche Subnets, Polkadot Substrates or Cosmos Interchains. Designed to be application-specific, these new sub-blockchain technologies could be the answer that we are looking to support dMail & dChat fast finality and low-cost transactions (i.e. one message = one transaction).

4. STORAGE LAYER

There are four storage data bases forming within the framework; (1) blockchain is used to store; (a) a link to the dMail JSON metadata, timestamp, checksum & sender address; (b) dChat encrypted message, timestamp & sender address. The overall security of the blockchain network depends on its decentralization, while access security depends on the user's private key safety measures; (2) decentralized storage is used for the temporary or permanent storage of encrypted data files, media and JSON files (i.e. dMail, subject & content attachment location) that are exchanged between wallets in the dMail or dChat process. The decryption and access to the data files are possible only with a private key of the user; (3) to comply with GDPR, the data file cloud repository is also an option that is used for the temporary 7-day storage of encrypted data, media and JSON files (i.e. dMail subject, content attachment location) that are exchanged between wallets in the dMail or dChat process. The decryption of the data files is possible only with a private key of the user. The data file cloud repository is protected by a firewall and other safety measures provided by cloud provider. In the case of a user request, it is possible to delete any user-related data to comply with GDPR, and; (4) user local storage is used to storing; (a) wallet private keys; (b) dMail & dChat content cache, and; (3) user-initiated backup of conversations, data files and reports. The security of local storage is in the user's domain.

To overcome the multi-chain challenge of enabling the usage of the same decentralized storage (e.g. BTFS) for all supported chains, the unique solution is being developed. The BTFS as a service, will enable any adopter or end user to communicate with BTFS no matter their native chain. While the native BTFS service payments are settled in BTT, the underlying swap will enable the storage payments in the token of the user's choice. The BTFS as a service will also act as a stand-alone solution providing service APIs to any project in need. As projects develops more details will be revealed.



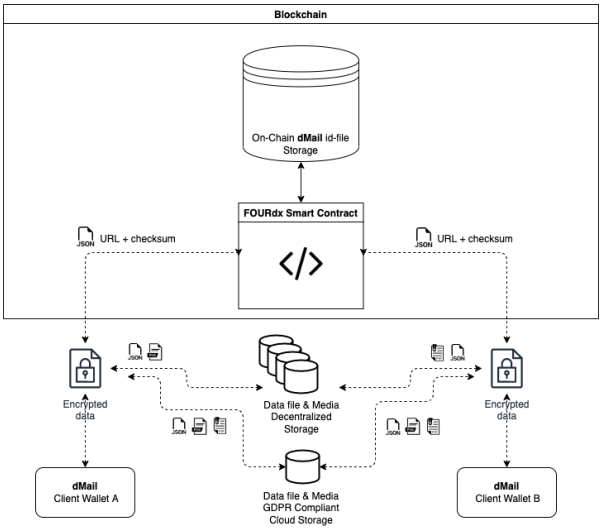
BTFS as a service structure diagram

5. PROTOCOL LAYER

There are two smart contracts forming the core solution protocol layer; (1) FOURdx Protocol, and; (2) FOURim Protocol. Developed as multi-chain interoperable, the smart contracts support EVM, Substrate, Solana, Tron frameworks and will support Cosmos stack in the future. Additional protocol and services such as; (1) FOURid Protocol, and; (2) FOURns Protocol were developed as the framework evolved.

5.1. FOURdx PROTOCOL

The protocol leverages trust sourced from the blockchain L1 to enable E2EE, immutable W2W data exchange in the form of; (1) dMail (i.e. decentralized email); (2) data file exchange (e.g. media or data files), and; (3) dNotary (i.e. data file on-chain file checksum verification). Deployed on public blockchains, the protocol SDKs empower any projects to connect and enable their users to communicate in a secure and decentralised manner. Compared to the FOURim Protocol (i.e. immutable W2W E2EE message exchange), where W2W message exchange happens on-chain, the FOURdx is data heavier due to attachments and sizable content. The key was combining L1 security with decentralized storage where lite encrypted JSON files are stored to hold dMail metadata while link to dMail JSON metadata and checksum are recorded on-chain in the form of an L1 transaction. Supported by a TypeScript/JavaScript SDKs and plug-and-play white-labels, the protocol is made ready for security-enabled social scaling in the multi-chain universe.



dMail structure diagram

FOURdx architecture & process; (1) JSON metadata file is created that included dMail sender subject, content, attachment name, attachment URL, calculated hash (i.e., checksum) of data file content and Client B address; (2) in the form of JSON metadata file, dMail send from Client Wallet A gets encrypted with a public key of the receiver (i.e. applies in RSA encryption and is not applicable in ECDH case) Client B; (3) JSON metadata file URL & checksum are sent to the chosen L1 FOURdx Smart Contract; (4) received Client B dMail is decrypted with Client B private key (i.e. applies in RSA encryption and is not applicable in ECDH case); (5) attachments in the form of media & data files from Client A are encrypted with the public key (i.e. applies in RSA encryption and is not applicable in ECDH case) of Client B; (6) encrypted attachments files are sent to either temporary GDPR compliant cloud storage or decentralized storage, and; (7) received Client B attachments files are decrypted with Client B private key (i.e. applies in RSA encryption and is not applicable in ECDH case).

```
// Symmetric encrypt
const symKey = crypto.randomBytes(32);
```

```
const iv = crypto.randomBytes(16);
const cipher = crypto.createCipheriv('aes-256-
cbc', symKey, iv);
const symEncrypted = Buffer.concat([
  cipher.update(fileData),
  cipher.final(),
]).toString(
    'base64',
);

// Asymmetric encrypt - encrypt just symmetric
key & iv const key = new NodeRSA();
key.importKey(publicKey, 'pkcs8-public');
const symPrefix =
`${symKey.toString('base64')}:${iv.toString('base
64')}`;

const encrypted = key.encrypt(symPrefix,
'base64');

// Join asymmetric and symmetric part
const data =
Buffer.from(`${encrypted}:${symEncrypted}`);
```

File Encryption Example (i.e. applies in RSA encryption and is not applicable in ECDH case)

Attachments; Attachment media & data are stored on decentralized storage. The dMail recipient is provided with the "link" of the saved location of the JSON metadata file. The JSON metadata file link/location that includes the link of the attachments is sent to the blockchain, and the dMail recipient can download the data file and decrypt it with his private key (i.e. applies in RSA encryption and is not applicable in ECDH case).

GDPR compliant; As a result of extensive three years of legal and procedural GDPR research, the FOURdx protocol can be recognised also as a GDPR compliant application as no personal data is stored on-chain.

***Note:** The current staging data exchange file size is limited to 20MB. All exchanged files are deleted after 7-days.*

***FOURdx Protocol Smart Contacts**:*
https://wiki.4thtech.io/intro/discover.html#the-fourdx-smart-contracts

More *FOURdx-related information:*
https://wiki.the4thpillar.com/intro/discover.html#fourdx-data-exchange-protocol

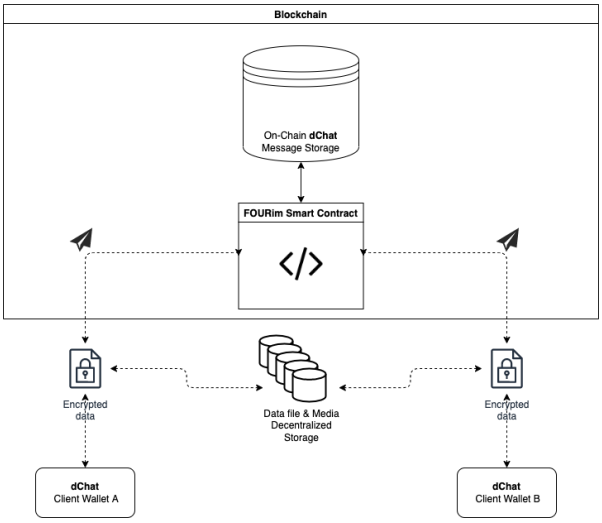
***Quote;** "I see amazing possibilities in 4THPILLAR TECHNOLOGIES products. The FOURdx, electronic data and documents exchange serves as a system for sensitive document distribution between organizations and individuals and is based on blockchain technology. A truly innovative and amazing solution."*

Igor Zorko, ZZi

5.2. FOURim PROTOCOL

The protocol leverages trust sourced from the blockchain L1 to enable E2EE, immutable W2W message exchange in the form of; (1) on-chain DM dChat (i.e. W2W E2EE direct messaging); (2) on-chain Group dChat (i.e. W2W E2EE group messaging), and; (3) NFT or token curated on-chain Group Chat (*4THPILLAR TECHNOLOGIES Layer 1 Blockchain Instant Messaging (i.e. FOURim) Light Paper*, n.d.).

So far the FOURim Protocol is developed as Solana, Rust-based and EVM-based framework. Due to fast transaction finality (i.e. 0.89s), the protocol was first developed for the Solana ecosystem, following deployments on Tron and Bittorrent Chains. The L1 serves as an immutable blockchain ledger exchanging short encrypted messages from wallet address A to wallet address B in the form of a transaction (i.e. one message = one L1 transaction). To achieve the security of decentralization, 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. The FOURim framework is supported by a TypeScript/JavaScript SDKs and plug-and-play white-labels made ready for security enabled social scaling in the multi-chain universe.



dChat structure diagram

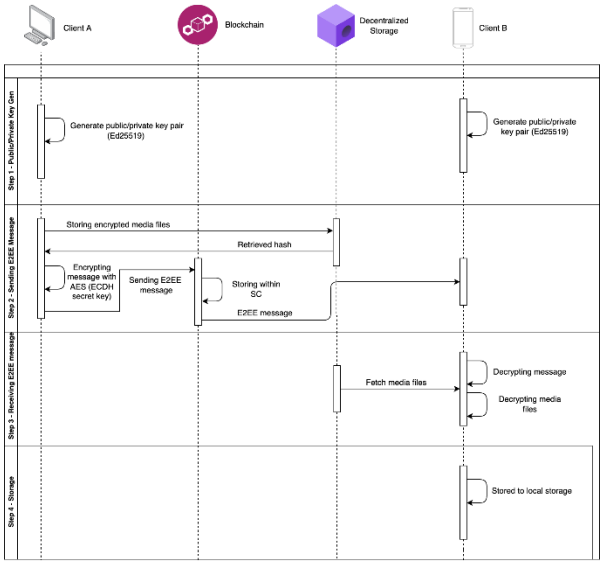
Messaging Process; the messaging process itself is pretty straightforward. Let's take an example of Alice and Bob;

(Step 1) public and private key pairs are created for Alice & Bob. Alice creates a message along with a picture or data file attachment she wants to send to Bob;

(Step 2) the send message is encrypted with Advanced Encryption Standard (AES), while Elliptic-Curve Diffie-Hellman (ECDH) key agreement protocol is used for generating the secret key (used in AES encryption). At the final stage of step 2, encrypted message is written on the TRON blockchain. Just to clarify, this message is stored on-chain, while attachments are stored on decentralized storage;

(Step 3) Bob receives and decrypts the message and attachment sent by Alice with his secret key generated by ECDH key agreement protocol between Alice and Bob, and;

(Step 4) the message and its attachments are stored in Bob's local storage.



dChat process diagram

Message Encryption
Message is encrypted with AES algorithm Secret key for AES algorithm is shared between Client A and Client B with ECDH algorithm **Client A and Client B agree on a curve with starting point P** **Client A has a private key a and public key A = a * P** **Client B has a private key b and public key B = b * P** **a * B = a * b * P = b * A** **So a * b * P ends up being the shared secret** ECDH: Elliptic Curve Diffie Hellman Key-sharing algorithm used for asymmetric encryption AES: Advanced Encryption Standard Ed25519: Edwards Curve 25519 The most commonly used Edwards Curve

dChat encryption table

FOURim Protocol Smart Contract;
https://wiki.4thtech.io/intro/discover.html#the-fourim-smart-contracts-in-production
More FOURim-related information;
https://wiki.the4thpillar.com/intro/discover.html#fourim-4thtech-instant-messaging-protocol

5.3. FOURid PROTOCOL

The Web2 reality as we know it did not prove sustainable, as personal data manipulation by the corporate giants is just not acceptable. Unlike Web2 where our identities are disclosed and locked by the intermediaries, the decentralised Web3 on-chain identities (i.e. dID) need no third party, are portable and completely anonymous until and if the users decide to tie them to the off-chain identity. Web3 identities 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. Wallet core infrastructure enables anonymous identity as a default. Due to specific development requirements of the 4thTech W2W communication protocols (i.e. dMail, dChat, dNotary) where data is being exchanged and confirmed between wallets, a custom wallet framework had to be developed which enables the usage of the UI-staging platform. Staging users can transact and communicate using the same wallet account across multiple dApps (i.e. dMail, dChat, dNotary) as their on-chain identity is seamlessly transferable between them.

Solution; FOURid Protocol connects entities, organizations, and individuals in a decentralized internet. The protocol connects wallets when data is exchanged. At the same time, the protocol provides wallet address verification of an individual or an organisation by creating a link between an X.509 user's online identity and blockchain wallet address. It enables a self-sovereign framework of data (i.e., data files and metadata) authorisation and ownership representation. All ID 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.

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

dID for organisations; Opposite to permissionless identity used by end-users in a decentralised Web3 environment, organisations need a connection between off-chain and on-chain identity. If using decentralised blockchain technology, organisations need to be able to identify and verify the recipients of the sent data or assets. 4thTech approached this issue by enabling the connection of the off-chain X.509 digital identity with on-chain dID. The 4thTech on-chain identity can now be verified using users' off-chain X.509 digital identity certificate. The connection process is executed off-chain and managed by the organisation admin, so it complies with existing online regulations.

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 name, last name and tax number; (3) FOURid mechanism 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 FOURid between the user's X.509 digital certificate and its 4thTech wallet address.

More FOURid-related information;
https://wiki.the4thpillar.com/intro/discover.html#fourid-4thtech-digital-identity-protocol

5.4. FOURns PROTOCOL

Blockchain data verification or notarisation can be described as a fraud prevention process that enables *dMail* 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. *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 from wallet A to wallet B, 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 dNotary framework is supported white-label solutions.

Solution; As a by-product of data exchange protocol (i.e., FOURdx), the FOURns Protocol can leverage the power of blockchain to facilitate source and time confirmation for any data files exchanged within the 4thTech ecosystem. dNotary 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.

**More FOURns related information;*
https://wiki.the4thpillar.com/intro/discover.html#fourns-4thtech-data-source-and-time-stamp-verification-service

6. SDK LAYER

Build on top of the protocol stack, the dMail & dChat TypeScript/JavaScript plug-and-play SDKs stand ready for security-enabled social scaling in the multi-chain universe. More information will be revealed as the SDKs are being developed.

7. ENCRYPTION LAYER

True dMail & dChat security and immutability is achieved by utilising L1s decentralization, encryption-hashing cocktail (i.e. AES, RSA, SHA-256, ECDH) and decentralized storage. Decentralized storage is used to store encrypted data. The decryption and access to the data files are possible only with a private key. In the case of the FOURim Protocol, message is encrypted with Advanced Encryption Standard (AES), while Elliptic-Curve Diffie-Hellman (ECDH) key agreement protocol is used for generating a secret key (i.e. used in AES encryption). ECDH also enables interoperability with popular wallets such as MetaMask, TronLink and others. The group chat encryption is solved by random generation of the secret key, that is used to encrypt/decrypt messages. The secret key is distributed to all group members and separately encrypted with Advanced Encryption Standard (i.e. AES) over the Elliptic-Curve Diffie-Hellman (i.e. ECDH) key agreement protocol.

8. dApp LAYER

While the project goal is to support permissionless onboarding of multi-chain dMail and dChat UIs via SDKs, specific staging dApps like data exchange dedicated multi-chain wallet and dMail and dChat UI had to be developed.

8.1. FOURwaL

W2W messaging and data exchange dedicated wallet framework serves as a gateway connecting users with on-chain dMail & dChat services. As a non-custodial gas wallet, it also manages RSA public and private keys. It provides a secure way to connect to the 4thTech blockchain protocols (i.e., FOURid, FOURdx, FOURns, FOURim) as it contains a pair of public and private cryptographic keys. The FOURwaL is fully operational within the ecosystem of Chromium, Firefox and Brave browsers and performs tech-specific features needed for services staging execution. FOURwaL utilises advanced encryption standards (i.e. AES), with a combination of RSA encryption and hash algorithm 256 (i.e. SHA 256) to secure immutable data exchange. Furthermore, the 4thTech wallet framework (i.e. FOURwaL) supports multi-chain accounts and serves as a dID on Ethereum, Tolar HashNet, Edgeware, Solana, Moonbeam, Tron, Bittorent Chain & Evmos.

FOURwaL main functions; (1) to serve as a gateway connecting the user with on-chain services; (2) to enable on-chain digital identity; (3) to enable wallet-to-wallet data exchange and communication; (4) to act as an on-chain data file and message exchange transaction signing tool; (5) to be used as a cryptographic token (i.e. FOUR, ETH, TOL, EDG, SOL, TRX, BTT, EVMOS…) gas wallet; (6) to manage the public and private keys, and; (7) to be used for private keys backup.

**Quote; "We build the 4thTech add-on from the ground-up. The challenge was to build the ADD-ON with a unique blockchain document exchange feature. I can say with certainty that the 4thTech add-on code is unique and the first of its kind! "*

Denis Jazbec, 4thtech CTO

****More FOURwaL-related information;***
https://wiki.the4thpillar.com/intro/discover.html#fourwal-4thtech-multi-chain-client-app-wallet

8.2. UI-PLATFORM CLIENT

The 4thTech UI-platform serves as an onboarding staging hub accessed by the user via Chromium and Firefox browsers with an installed FOURwaL blockchain wallet add-on. It serves as a staging and white-label framework enabling use case testing and further protocols development. It connects and hosts all the 4thTech protocols and services in one ecosystem, giving the user all-in-one access to; (1) powerful multi-chain wallet; (2) FOURid, on-chain digital identity; (3) FOURdx, E2EE dMail; (4) FOURns, dNotary verification protocol, and; (5) FOURim, wallet-to-wallet E2EE on-chain dChat.

UI-platform Build; As a part of the 2.0 update, the 4thTech UI-platform codebase was rewritten with TypeScript and has overgone the crucial performance upgrade from Vue 2 to Vue 3. New features and functions are embedded, so the user experience can be as intuitive as possible. The 2.0 update includes an automatic dNotary system, while the blockchain network address recognition system simplifies the dMail process.

**Note; To log in to the 4thTech UI-platform, please follow this link. https://app.4thtech.io/*

8.3. UI-STAGING

Usually staging is set up to replicate the production environment, test code or updates to ensure quality under a production-like environment before application deployment. In most cases, Staging is not open to the public domain. This was also the case for 4thTech, but with the emerging online privacy needs dID, dMail, dNotary & dChat are now open for public testing and available in 4thTech UI-staging. Even though the 4thTech Staging environment is a replica of the production environment, there are still some key differences such as; (1)

different UI-platform access links (staging.4thtech.io instead of app.4thtech.io); (2) the production environment uses public MainNet blockchains, while Staging uses TestNets and pilot DLT network SI-Chain, and; (3) production environment transactions use valuable MainNet tokens for gas, as Staging uses free TestNet tokens. In a non-production multi-chain environment, 4thTech Staging supports; (1) Ethereum TestNet Kovan; (2) HashNet protocol-based SI-Chain (i.e. Slovenian national blockchain testing infrastructure); (3) Edgeware TestNet; (4) Solana DevNet; (5) Moonbeam TestNet Moonbase; (6) Tron test nets Shasta & Nile; (7) Bittorrent Chain TestNet, and; (8) Evmos TestNet.

Staging Storage; Very similar to production, Staging storage different itself only in on-chain storage, where it saves the needed protocol data on TestNets instead of on MainNets. four data storages are forming in the 4thTech Staging system;

(1) Blockchain is used to store; (a) a link to the dMail JSON metadata, timestamp, checksum & sender address; (b) dChat encrypted message, timestamp & sender address. The overall security of the blockchain network depends on its decentralization, while access security depends on the user's private key safety measures;

(2) Decentralized storage (in development) is used for the temporary or permanent storage of encrypted data files, media and JSON files (i.e. dMail, subject & content attachment location) that are exchanged between wallets in the dMail or dChat process. The decryption and access to the data files are possible only with a private key of the user;

(3) To comply with GDPR, the data file cloud repository is also an option that is used for the temporary 7-day storage of encrypted data, media and JSON files (i.e. dMail subject, content attachment location) that are exchanged between wallets in the dMail or dChat process. The decryption of the data files is possible only with a private key of the user. The data file cloud repository is protected by a firewall. In the case of a user request, it is possible to delete any user-related data to comply with GDPR;

(4) User local storage is used to storing; (a) wallet private keys; (b) dMail & dChat content, and; (c) user-initiated backup of conversations, data files and reports. The security of local storage is in the user's domain.

**__Note:__ To log in to the 4thTech UI-staging, please follow this link. https://staging.4thtech.io/*

**__More__ client UI-platform-related information: https://wiki.the4thpillar.com/intro/discover.html#_4thtech-client-app-web-platform*

9. USE CASES

The need for permissionless, immutable and secure digital data exchange is imminent. Current centralised email and messaging systems are not secure and do not provide any protection before cyber-attacks and ever-growing spam. Did you know that nearly 85% of all emails are spam? According to Dataprot statistics that 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.

The dMail and dChat multi-chain protocol deployment accompanied by plug-and-play SDKs will enable 1000s of dMail and dChat dApps to Blum on Web3, creating various use cases with some of them being long overdue, such as;

(1) UI that will enable user-friendly UX to immutable dMail & dChat on-chain communication that is resistant by design to identity theft, data theft, email spoofing, span and social engineering;

(2) the Bloomberg like dChat that will enable privacy and security in trading-based conversation groups that can be accessed based on a specific asset;

(3) the dNotary UI, which can be also described as a digital notary of the decentralized world and with its main solution enables sensitive data files time-stamp and origin verification using L1s as a "trust" source, and;

(4) data file exchange dedicated UI, that enables anyone to harness the L1 security and enable immutable end-to-end encrypted data file exchange between wallets.

10. 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 FOURdx Protocol is designed and built according to the EU and GDPR guidelines with main GDPR compliance features; (1) transaction is authorized by the user; (2) blockchain network is used for transactions that Include link to encrypted dMail, 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 dMail 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 4thTech dMail 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.*

11. CONCLUSION

Privacy, data ownership and secure online communication are fundamental rights of every person. With the help of advanced Web3 blockchain protocols as an underlying infrastructure, 4thTech leads the way in R&D towards secure and private internet communication. As online communication represents one of the biggest use cases needed to be solved by the Web3, there are also other projects trying to solve the same issue, each with its own proposed approach. According to competitor analysis (*4thTech DMail & DChat Competitors Comparison Tables*, n.d.), 4thTech's "one message = one transaction" approach is unique, but also 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 venerable, 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.

12. DISCLAIMER

All content provided herein, including but not limited to text, graphics, logos, and images (the "Content"), is the property of Block Labs Luxembourg S.a r.l., a legal entity established under the laws of the Grand Duchy of Luxembourg, registered with R.C.S. Luxembourg under N B263508 at the following address: 41, rue du Puits Romain, z.a. Bourmicht (Atrium Business Park), L-8070 Bertrange, Luxembourg (the "Company" or "we"). It is protected by copyright and other laws that protect intellectual property and proprietary rights. You are granted a non-exclusive, non-transferable, revocable license to access and use the Content for the sole purpose of obtaining information about the 4thTech technology and other educational purposes. We have done our best to ensure that the Content is accurate, updated, complete, and provides valuable information, but neither do we guarantee nor take any responsibility for its accuracy and/or completeness. The Content is not intended as, and shall not be understood or construed as legal, financial, tax, or any other professional advice, sale or offer for sale of any securities, and/or crypto-assets. The Company is not engaged in rending of and/or is not licensed to render any of the crypto-asset services and/or financial services, such as investment or brokerage services, capital raising, fund management, or investment advice.

**__Note;__ Prepared and updated with care by the 4thTech team*

References

4THPILLAR TECHNOLOGIES Layer 1 blockchain instant messaging (i.e. FOURim) Light Paper. (n.d.).

4thTech dMail & dChat Competitors Comparison Tables. (n.d.). Retrieved October 23, 2022, from https://4thtech.io/comparison-tables/

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/

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*.

HolaChain, Web3 Secured W2W Communication Infrastructure | Devpost. (n.d.). Retrieved September 25, 2022, from https://devpost.com/software/4thtech-privacy-enabled-w2w-communication-infrastructure

HOPR | Blockchain Data Protection and Privacy. (n.d.). Retrieved October 23, 2022, from https://hoprnet.org/

Solana on Twitter: "Decentralized, encrypted messaging, built on #Solana" / Twitter. (n.d.). Retrieved September 25, 2022, from https://twitter.com/solana/status/1482045683364511759?s=20&t=qJGMObZxxNynIhzXPJAhLQ