Block Labs publications
Type: Whitepaper
Status: Published
Updated: 25.09.2022
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 Web3 first L1 secured E2EE dMail & dChat W2W on-chain communication infrastructure. 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. The protocols in its core prevent ads, tracking and data mining! This whitepaper was written as a hybrid addressing the *4thTech* product benefits and solutions.**

Dr. Tali Rezun, head of *4thTech* R&D

Keywords: 4thpillar, 4thtech, dID, dMail, dChat, dNotary, FOURdx, FOURid, FOURns, FOURim, digital transformation, blockchain technology, decentralization, peer-to-peer, online trust, online security, online privacy, DLT

I. INTRODUCTION

Secure exchange of digital data in the form of emails, messages, data files or media should be as easy and available to all. 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. We believe that 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 private online communication. The security native to Web3 is just too good to be overlooked.

4thTech addressed this issue already in 2017 and started to develop a secure blockchain-based solution, which leverages encryption and trust provided by the L1 to enable immutable *dMail* and W2W data file exchange (i.e. FOURdx Protocol). On-chain digital identity, the *4thTech dID* (i.e. FOURim Protocol) was later added in 2018. Data verification protocol (i.e. FOURns Protocol) was built in 2020 that acts as an essential part of the *4thTech* ecosystem and enables unique *dNotary* data timestamp and file checksum authenticity verification solution. As the last Web3 communication building block, dChat was constructed in 2021 and enables the first true on-chain messaging.

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 (i.e. one message = one L1 transaction). Blockchain provides a decentralized and secure shared digital ledger, which gives participating parties a way of validating information related to a transaction. In doing so, it speeds up the process and cuts out intermediaries and costs. 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 both values and events. 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. Blockchain technology is one of the most promising developments in the information technology (i.e., IT) domain. According to (*Blockchain Technology Market Size, Share | Industry Report, 2019-2025*, n.d.), the global blockchain technology market size was valued at 1,590.9 million in 2018 and is expected to grow at a CAGR of 69.4% from 2019 to 2025. The article from The Economist ("The Second Half of the Internet," 2019) predicts that billion new internet users will be joining the rest of us soon, there are countries such as Mauritius that are skipping centralized digitalization and want to adopt blockchain technology directly. According to (*Time For Trust: How Blockchain Will Transform Business and the Economy - PwC*, n.d.), blockchain has the potential to boost global domestic product (i.e. GDP) by 1.76 trillion dollars over the next decade and hit the mainstream by 2030. PwC report also points out that some 60% of CEOs are placing digital transformations among their top three priorities and that organisations have recognised the value of online trust and cybersecurity between

their business partners and customers. As data value grows exponentially, so does its privacy. 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 three years of *4thTech MVP* (i.e., minimum viable product) early adopter testing and refinement according to European standards, the technical feasibility and its practical potential have been proven, with that PoC (i.e., proof of concept) was confirmed. Moving to version 2.0, *4thTech* enters the adoption phase and becomes globally interoperable and ready to use.

In May 2018 Adriatic council awarded Dr. Tali Rezun 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 acknowledgement followed such as Solana FOURim Protocol endorsement* (*Solana on Twitter: "Decentralized, Encrypted Messaging, Built on #Solana" / Twitter*, n.d.) *and Tron Hackathon win* (*HolaChain, Web3 Secured W2W Communication Infrastructure | Devpost*, n.d.).

II. 4THTECH

4thTech utilises Web3 to enable secure communication within on-chain W2W E2EE dMail, dChat & data file exchange, which is currently non-existing in traditional Web2 applications. Behind the scenes, 4thTech enables any project to integrate the dMail & dChat layers into their platform UIs or wallets using SDK framework, while its multi-chain interoperability and deployment pave the way towards the first Web3 communication standard.

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. So again the core primitive "one email/message = one L1 transaction" applies;

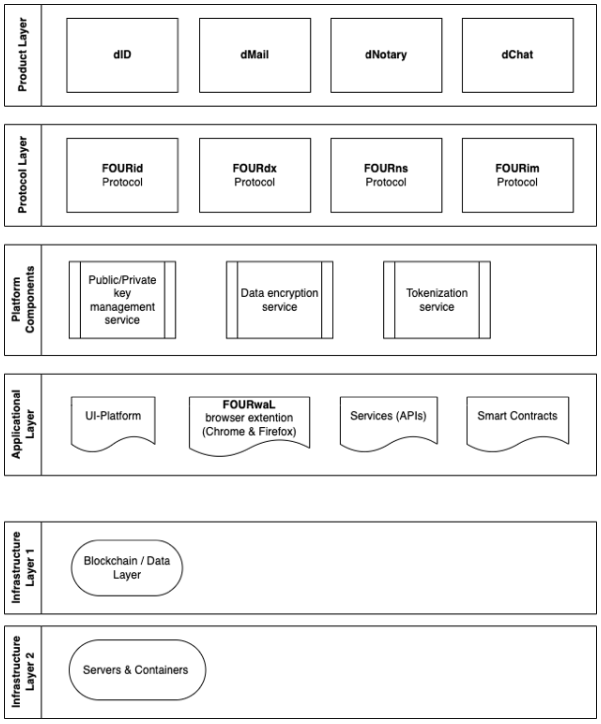
(2) Not Your Keys = Not Your Email/Message. Every wallet becomes an on-chain identity & message data vault, accessible/decrypted only with users' private keys!;

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

The aim and project objective are to enable; (1) a secure affordable encrypted dMail and dChat with no ads, no data mining and no tracking; (2) wider adoption of blockchain technology, and; (3) to pioneer the future of encrypted decentralized on-chain communication. With massive communities emerging surrounding popular DeFi, NFT, Gaming and DAO platforms the need for social communication is increasing. Messaging is at the top of the list regarding social interaction. But in the decentralized ecosystem, you need a decentralized communication solution. 4thTech is not only an end-user dMail & dChat dApp, but a permissionless dMail & dChat protocol standard that enables 1000s of W2W communication dApps Blum on Web3, via our SDKs & White labels.

4thTech brand--According to many, there are three fundamental technology 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.

Layer infrastructure; (1) product layer defines all project products including SDKs (i.e. dID, dMail, dNotary, dChat); (2) protocol layer defines all the project protocols (i.e. FOURid, FOURdx, FOURns, FOURim); (3) the third layer defines the platform components (i.e. public/private key management service, data encryption service and tokenization service; (4) the fourth layer defines the applications (i.e. UI-platform, browser extension wallet, API services and smart contracts), and; (5) infrastructural layers are defining capabilities and connectivity's to blockchain networks and hardware and scalability tools.



4thTech layers diagram

III. FOURid PROTOCOL, DECENTRALIZED DIGITAL IDENTITY

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 KPI core infrastructure enables anonymous identity as a default. Due to specific requirements of 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 UI-platform, UI-staging and White-labels UIs access. Users can transact and communicate using the same wallet account across multiple dApps (i.e. dMail, dChat, dNotary) as their anonymous on-chain identity is seamlessly transferable between them. Every wallet becomes a user on-chain identity and data vault that only the user controls. 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 & Evmos.

***dID Solution**--4thTech's* digital identity protocol FOURid connects entities, organizations, and individuals in a decentralized internet. The *dID* connects wallets when data is exchanged. It serves as the public key exchange point between users. 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. dID 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.*

***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).

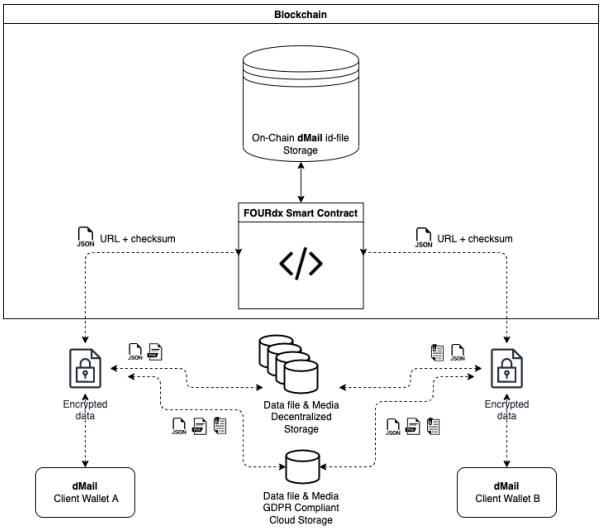
X.509 connection process; (1) the user selects the X.509 standard qualified digital certificate, associated with an individual or organisation; (2) a simple KYC form is completed with the certificate holder's name, last name and tax number; (3) FOURid mechanism prepares and sends WSDL request in a SOAP 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*

IV. FOURdx PROTOCOL, W2W E2EE dMail

The need for permissionless, immutable, private digital data exchange is imminent. Current centralised eMail systems or other web2 data exchange services are not secure and do enable any privacy whatsoever. 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.

***dMail solution**--*FOURdx protocol leverages trust sourced from the blockchain L1 and enables E2EE, immutable wallet-to-wallet dMail. The dMail (i.e. decentralized email) framework is built on public or DLT blockchains, enabling organizations and individuals to collaborate and exchange data in a secure and decentralised manner. Compared to dChat, where W2W message exchange happens on-chain, the dMail 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. 4thTech's dMail can also be defined as a decentralized network framework that supports text, data file or media exchange between wallet addresses of supported blockchain frameworks (i.e. EVM, Substrates and Solana). Supported by a modern intuitive UI-platform and thanks to multi-chain support, 4thTech dMail is accessible and affordable to all users.



dMail structure diagram

dMail 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 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; (5) attachments in the form of media & data files from Client A are encrypted with the public key of Client B; (6) encrypted attachments files are sent to either 4thTech temporary GDPR compliant cloud storage or decentralized storage (i.e. in development), and; (7) received Client B attachments files are decrypted with Client B private key.

dMail Attachments--Attachment media & data are stored in the 7-day temporary repository (i.e. currently limited to 20 MB file size). The dMail recipient is provided with the "link" of the saved location JSON metadata file. The JSON metadata file that includes the link is sent to the blockchain, and the dMail recipient can download the data file and decrypt it with his private key saved in the browser's 4thTech wallet (FOURwaL).

GDPR compliant--As a result of extensive three years of legal and procedural GDPR research, the FOURdx protocol can be recognised as a GDPR compliant application as no personal data is stored on-chain but resides off-chain. FOURdx records links to encrypted files and hashes of the encrypted content on the blockchain.

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

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

V. FOURns PROTOCOL, ON-CHAIN dNotary

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 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.

dNotary solution--As a by-product of data exchange protocol (i.e., FOURdx), the FOURns 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.

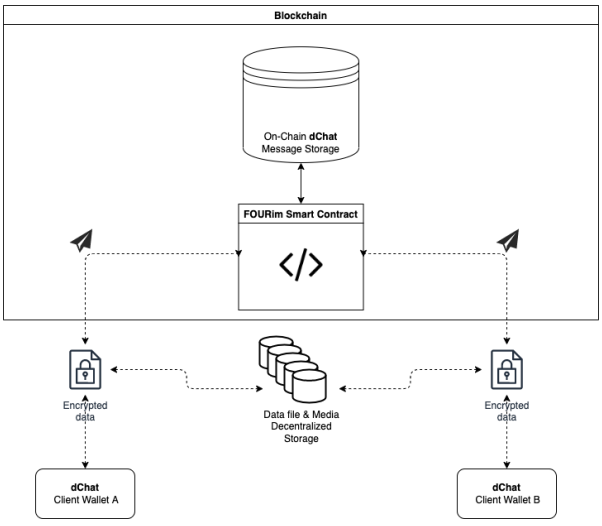
Data verification process; (1) user account creation within the FOURwaL; (2) user account verification using 4thTech dID within the UI-platform (option); (3) on-chain checksum and timestamp verification of the received data file, using 4thTech dNotary within the 4thTech UI-platform.

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

VI. FOURim PROTOCOL, W2W E2EE dChat

Up to now, on-chain instant messaging deployment would be hard to achieve due to slow blockchain network speed, congestion and transaction cost. With the arrival of the new-gen blockchains on-chain, instant messaging is becoming a reality. To address this issue the 4thTech developed the dChat, which leverages blockchain L1 security to provide E2EE immutable on-chain W2W messaging.

dChat solution--The FOURim Protocol leverages the underlying L1 to enable true security and first on-chain W2W communication (*4THPILLAR TECHNOLOGIES Layer 1 Blockchain Instant Messaging (i.e. FOURim) Light Paper*, n.d.). Due to extremely fast transaction finality (i.e. 0.89s), the protocol was first developed on Solana. It connects to the Solana blockchain node using JSON-RPC protocol. Solana serves as an immutable L1 blockchain ledger exchanging short encrypted messages from SOL wallet address A to SOL wallet address B in the form of a transaction (i.e. one message = one L1 transaction). The 4thTech dID is used to connect both the wallet of the message sender and the wallet of the message receiver and serves as the public key exchange point between both users (i.e. the sender needs a public key of the receiver). To achieve the security of decentralization, the messages are not stored on a company centralised server but are temporarily stored on the L1 itself and deleted after 7-days. Solana programs (i.e. smart contracts) are used to facilitate two unique requirements; (1) saving dChat instant messages from the sender, and; (2) retrieving dChat instant messages from receivers. An EVM FOURim Protocol version is currently in development and will enable the protocol deployment also on EVM-based L1s.



dChat structure diagram

Solana dChat PDA accounts*;* All data on the Solana blockchain is saved in the PDA accounts. PDA accounts are owned by the FOURim Protocol program (i.e. smart contract). FOURim Protocol uses five different types of accounts; (1) user account

holds conversation counter data; (2) conversation account holds message counter; (3) user conversation account holds conversation address; (4) message account holds message data (sender, message type, content, timestamp), and; (5) conversation encryption info-account holds data of the encryption conversation. Initialization of conversation between two wallets consists of; (1) creating a user account for sender and receiver; (2) creating a conversation account; (3) creating two user conversation accounts, one for the sender and the second for the receiver; (4) creating a message account, and; (5) creating a conversation encryption account. When the already created conversation continues a new message account is created and the message counter in the conversation account is increased.

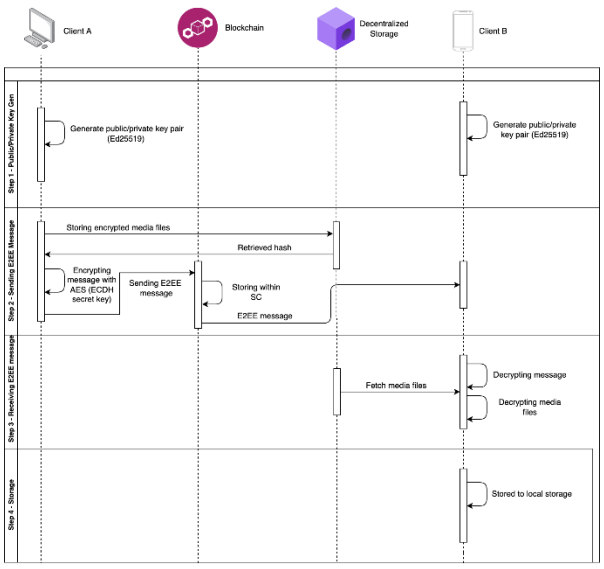
Messaging Process—the messaging process itself is pretty straightforward. Let's take an example of Alice and Bob:

(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, the message hash is written on the TRON blockchain. Just to clarify, this message is temporarily 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 private key;

(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

User control--With FOURim Protocol, the dChat users gain control over their messages, the messages are end-to-end encrypted and stored on the L1 itself. Messages are not stored on a company server! Every message is signed with the receiver's public key. Your wallet address serves as your on-chain identity. When the 4thTech UI-platform reaches full decentralization, it will not matter if the project is here or not, all control will be in the user's hands. There are no ads, no tracking or data mining and never will be!

Pre-transaction message snapshot--Due to a short dChat send message delay on behalf of the encryption and network transaction execution, a pre-transaction dChat message snapshot is created, that displays the send a message in light colour before the colour changes to darker which represents the final on-chain message execution.

Speed & transaction pricing testing results--After significant testing on Solana DevNet and MainNet, we have concluded that the send or receive message speed depends on the message length, encryption (decryption) and transaction finality as it varies between 1 to 5 seconds. As every message represents its on-chain confirmed transaction and needs to be encrypted and decrypted this is still a good result and it is as "instant" as it can get with a current framework. Hopefully, the execution time will improve with further network developments and protocol tweaks. Further testing will be done to produce more accurate results. Currently, only Solana TX cost is being charged in $SOL with a possibility of a small protocol service fee to be added in the future. Overall, there are currently three cost variants to be considered in the messaging process;

(1) Initialization of a conversation between two wallets usually takes more time to be established as five accounts need to be created (we are adding a progress window in future updates). Testing produced the following TX cost: 0,006845503 SOL "Hi :D"

(2) When the conversation is established between two wallets, sending and receiving messages takes less time averaging between 1 and 5 seconds. Testing sending a short message produced the following TX cost: 0,000039503 SOL "ooo :)"

(3) The TX cost depends on message length. Testing sending a longer message produced the following TX cost: 0,00006219

SOL "Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book."

**__Testing timeframe:__ Results were measured on 21.12.2021 with SOL price at 190$, while TestNet and MainNet testing was performed over 6 months.*

*__*FOURim Protocol__ Program: https://explorer.solana.com/address/Hk5f9Xw9PdaQ9GEg8TPVFusojLA9otDpUkziXw1hAVE5*

**__More__ FOURim-related information: https://wiki.the4thpillar.com/intro/discover.html#fourim-4thtech-instant-messaging-protocol*

VII. FOURwaL, MULTI-CHAIN ADD-ON WALLET

According to (*Cryptocurrency Wallet - Wikipedia*, n.d.), a cryptocurrency wallet is a device, program or service which stores the public and/or private keys and can be used to track ownership, receive or spend cryptocurrencies. As all cryptocurrencies run on blockchains, cryptocurrency wallets can be referred also as blockchain wallets. Up to now, blockchain wallets was mostly used for cryptocurrency asset holding and exchange.

Solution--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 public and private keys. It provides a secure way to connect to the 4thTech blockchain protocols (i.e., FOURid, FOURdx, FOURns, FOURim) and products (i.e. dID, dMail, dChat, dNotary) as it contains a pair of public and private cryptographic keys. A public key allows for other wallets to execute 4thTech services to the desired wallet's address, whereas a private key enables the decryption of communication such as data files and short messages from the sender address. The FOURwaL is fully operational within the ecosystem of Chromium and Firefox browsers and performs tech-specific features needed for services 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. FOURwaL contains a pair of public and private cryptographic keys. A public key allows for other wallets to execute data communication to the desired wallet's address, whereas a private key enables the decryption of data from that address.

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, 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 and it took four engineers over a year to do it. 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*

VIII. UI-PLATFORM CLIENT

The 4thTech UI-platform serves as an onboarding hub accessed by the user via Chromium or Firefox browsers with an installed FOURwaL blockchain wallet add-on. 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. With over four years in development, the UI platform focuses on user onboarding UX, availability of accustomed email and messaging features and high-end crypto design. The coming 3.0 update will enable light or dark mode with contrast colours predominating the interface, inspiring the users with simplicity, step-by-step onboarding and reassurance while executing complicated transactions in the background. The design is made also for white-label solutions and can merge with the brand just by tweaking the brand logo and UI colours.

Main UI-platform services & solutions; (1) dID - FOURid Web3 Identity Protocol (status: in production); (2) dMail - FOURdx Data Exchange Protocol (status: in production); (3) dChat - FOURim Instant Messaging Protocol (status: in production); (4) dNotary - FOURns Verification Protocol (status: in production); (5) data encryption service (status: in production); (6) off-chain database and repository (status: in production); (7) JSON metadata schema (status: in production), and; (8) transaction fee mechanism (status: in production).

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/*

IX. 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 Test Net Kovan; (2) HashNet protocol-based SI-Chain (i.e. Slovenian national blockchain testing infrastructure); (3) Edgeware TestNet, and; (4) Solana DevNet.

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. 4 databases 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*

X. STORAGE

(1) Blockchain is used to store; (1) a link to the dMail JSON metadata, timestamp, checksum & sender address; (2) 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. 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; (1) wallet private keys; (2) dMail & dChat content, and; (3) user-initiated backup of conversations, data files and reports. The security of local storage is in the user's domain.

XI. MULTI-BLOCKCHAIN INTEROPERABILITY

Multi-blockchain support enables transaction cost and speed choice, which is especially important when dealing with public blockchains. Next, to already supported Ethereum, two additional blockchain frameworks Substrate and Solana were added, both chosen based on their uniqueness and overall standard usage. Different EVM L1 variations were also added based on the testing demand. The support for HashNet protocol was added already in July 2020, while Edgeware, a Polkadot Substrate was added in v2.0. HashNet DLT is a ground platform we find essential to building an application that can handle a high volume of transactions that are furthermore, fairly recorded and immutable, while the platform ensures valid, scalable usage which makes it perfect for Enterprise applications. Edgeware is a high-performance, self-upgrading WASM smart contract platform, in the Polkadot ecosystem. It is a Substrate based blockchain built using the Rust programming language. Smart contracts are written in Ink! programming language. Ink! is a Rust-based eDSL for writing Wasm smart contracts specifically for the Contracts module. Special logic was added into programming, which enables us to add additional blockchain support when needed. Solana blockchain support was added in Q2 2021 to enable a secure affordable L1 instant messaging solution. To enable the first dMail and dChat multi-chain framework standard, the protocols would need to be deployed on all suitable L1s. In 2022 the support for Moonbeam, Tron and Evmos was added.

Special logic was added into UI programming, which enables us to add additional blockchain support when needed. There are several strategic advantages to multi-blockchain application interoperability; (1) the option to choose based on the network transaction price; (2) the option to choose based on the transaction speed; (3) the option to choose based on the network governance; (4) the option to choose based on the network congestion; (5) the option to choose based on the network interoperability; (6) the option to choose based on the network immutability, and (7) the option to choose based on the network infrastructure type.

**__Note:__ 4thTech uses hosted Ethereum node on Infura over JSON-RPC protocol, to connect to the Ethereum node. In the case of HashNet protocol, 4thTech uses Tolar Gateway which transforms JSON-RPC calls to gRPC (i.e. universal RPC framework) calls to connect to the HashNet node. In the case of connecting to the Polkadot/Edgeware and Solana node, 4thTech uses JSON-RPC protocol.*

XII. SECURITY PROTOCOLS

True dMail & dChat security is achieved by utilising L1s security, encryption cocktail (AES, RSA, SHA-256, ECDH) and decentralized storage. Decentralized storage is used to store encrypted data files, media files and JSON files (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 In the case of the FOURdx Protocol (dMail), the protocol uses an advanced encryption standard (i.e., AES), with a combination of RSA encryption and hash algorithm 256 (i.e., SHA 256) to secure immutable W2W E2EE dMail & data file exchange. In the case of the FOURim Protocol (dChat), message is encrypted with Advanced Encryption Standard (AES), while Elliptic-Curve Diffie-Hellman (ECDH) key agreement protocol

is used for generating a secret key (used in AES encryption). 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.

XII. 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 interoperability, *4thTech* dMail 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 encrypted dMail link, that only the receiver can open using his or her private key; (2) no personal information is located in the blockchain transaction; (3) 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; (4) 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; (5) 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.*

XIII. 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 enables a suitable E2EE dApp & SDK toolbox (i.e. dID, dMail, dChat, dNotary), helping individuals and organizations on their way towards secure and private online communication. At its core, 4thTech prevents identity theft, data tracking or data mining, while it's impervious to invasive ad campaigns and user content surveillance. 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.

XIV. DISCLAIMER

**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.).

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/

Blockchain Technology Market Size, Share | Industry Report, 2019-2025. (n.d.). Retrieved March 8, 2020, from https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

Cryptocurrency wallet - Wikipedia. (n.d.). Retrieved March 7, 2020, from https://en.wikipedia.org/wiki/Cryptocurrency_wallet

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

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

The second half of the internet. (2019). *The Economist*, *431*, 21–25.

Time For Trust: How blockchain will transform business and the economy - PwC. (n.d.). Retrieved December 31, 2020, from https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html