

Web3-Enabled E2EE dID, dMail, dChat & dNotary --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. 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 is becoming more and more important as we depend on it every day. To address this issue, 4thTech enables E2EE (i.e. end-to-end encrypted) Web3 communication & data management in the form of dID, dMail, dChat & dNotary. 4thTech initiative strives to enable a self-sovereign framework of data authorization and ownership representation and leverages the power of blockchain to facilitate data source and time confirmation. The protocols in its core prevent ads, tracking and data mining! This whitepaper was written as a hybrid addressing the *4thpillar Technologies* product benefits and solutions.

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

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

I. INTRODUCTION

Privately exchanging digital data in the form of emails data files or media should be as easy and available to all. 4thpillar Technologies (i.e., 4thTech), addressed this issue in 2017 and developed a private, multi blockchain-based solution, which leverages E2EE (i.e. end-to-end encryption) and trust provided by the blockchain to enable secure, immutable dMail (i.e. FOURdx Protocol). To enable on-chain digital identity, the 4thTech dID (i.e. FOURim Protocol) was later constructed in 2018. Data verification protocol (i.e. FOURns Protocol) was added 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 piece, dChat was constructed in 2022 that enables E2EE, private, on-chain instant messaging. The superiority of blockchain 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 ensure tamper-proof digital transactions through the use of cryptographic technology and automated consensus. 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 determines 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 grow 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 is becoming more and more important as we depend on it every day.

Validation--After two 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.

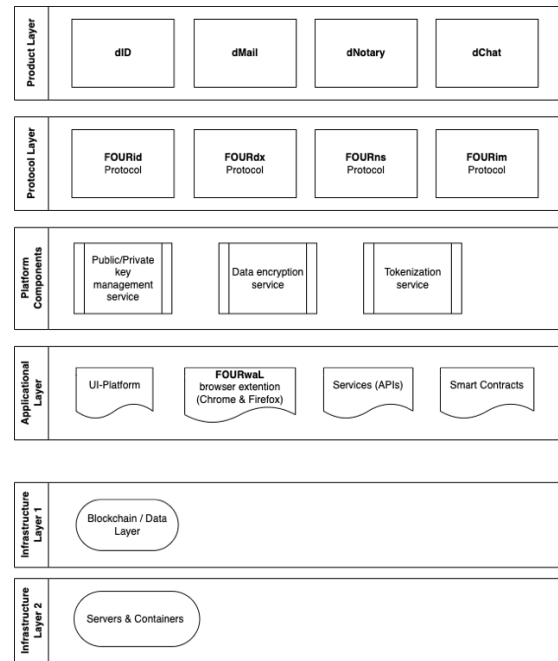
In May 2018 Adriatic council awarded Dr. Tali Rezun with the Beyond 4.0 award for his dedication, promotion and accomplishment in the field of science, new technologies and innovation for the 4THPILLAR Blockchain platform. (Adriatic Council | BEYOND 4.0 – LJUBLJANA, 25.05.2018. KRISTALNA PALAČA (BTC), n.d.)

II. 4THTECH

4thpillar Technologies or short 4thTech is the next-gen multi-chain platform that enables E2EE (i.e. end-to-end encrypted) Web3 communication & data management in the form of dID, dMail, dChat & dNotary. With a charter to establish a foundation for decentralized; (1) digital identity (i.e. dID); (2) multi-chain data exchange (i.e. dMail); (3) data verification (i.e. dNotary); (4) instant messaging (i.e. dChat), and; (5) decentralization of cloud storage, 4thTech strives to enable a self-sovereign framework of data authorization and ownership representation and leverages the power of blockchain to facilitate data source and time confirmation. The aim and project objective is to enable; (1) a secure affordable encrypted dMail and on-chain 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 data exchange.

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 to be revealed to the world.

Layer infrastructure; (1) product layer defines all project products (i.e. dID, dMail, dNotary, dChat); (2) use cases layer defines all the project protocols (i.e. FOURid, FOURdx, FOURns, FOURim); (3) the second layer defines the platform components (i.e. public/private key management service, data encryption service and tokenization service); (4) the third 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.



III. dID, FOURID WEB3 IDENTITY PROTOCOL

With is a constant need for online identity verification, and despite the move towards digital transactions, there is still the need to use physical identity documents. 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 holds promise in this regard and could be used to create and verify digital identities, for individuals and organizations. Trusted identities of blockchain participants are crucial to any operational success and can enable complex transactions and reduce risk. The verified identity of any partner in the business process or a network builds a core foundation for any business or blockchain endeavour. According to (*Blockchain-for-Digital-Identity*, n.d.) blockchain has facilitated the so-called self-sovereign identity, which is inherently unalterable and more secure than traditional identity systems, which has the potential to completely change the way we use identities to connect to different online services. Individuals or organizations can now leverage the 4thTech digital identity solution to map their blockchain wallets with their established online digital identities, enabling the use of blockchain technology in regulated sectors and industries.

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 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 Tolar, Edgeware & Solana.

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 individual or organisation; (2) simple KYC form is completed with certificate holder 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. dMAIL, FOURDX DATA EXCHANGE PROTOCOL

The need for immutable, unmodifiable digital data file exchange is imminent. Current centralised eMail systems or other Web2 data exchange services are not secure and do enable any privacy whatsoever. 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 is becoming more and more important as we depend on it every day. To address this issue, 4thTech enables E2EE (i.e. end-to-end encrypted) Web3 dMail.

dMail solution--FOURdx open-source protocol leverages trust sourced from the blockchain 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. The protocol records only links to encrypted JSON metadata files and checksum of the encrypted JSON metadata file on the blockchain, which safeguards the rights of individuals to confidentiality and privacy, while complying with GDPR. 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 blockchains (i.e. Ethereum, HashNet, 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.

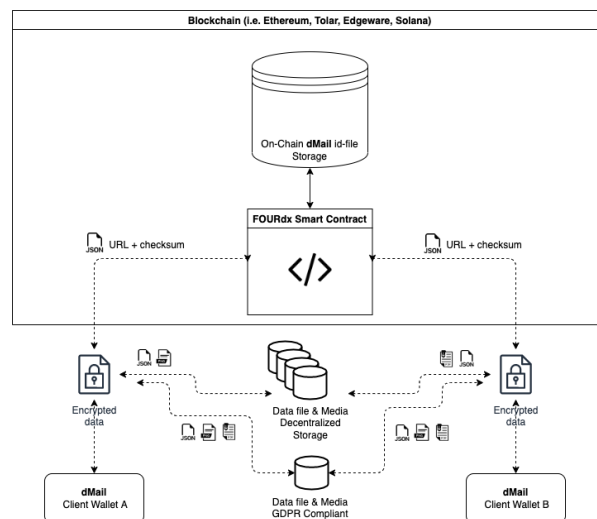
GDPR compliant--As a result of extensive three years of legal and procedural GDPR research, the FOURdx protocol can be recognised as a GDPR compliant application as no personal data is stored on-chain but resides off-chain. FOURdx records links to encrypted files and hashes of the encrypted content on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

dMail architecture and 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 Ethereum, Tolar, Edgeware or Solana 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 permanent 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).

***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. dNOTARY, FOURNS DATA VERIFICATION 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 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 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. dCHAT, FOURIM INSTANT MESSAGING PROTOCOL

Privacy in online communication is a fundamental right of every person. Exchanging private E2EE instant messages securely over the internet without data mining, ads or tracking should be easy and accessible to all. Blockchain technology proposes the ideal foundation to enable this solution. 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 Solana blockchain on-chain, instant messaging is becoming a reality. To address this issue the 4thTech developed a Solana-based dChat, which leverages blockchain trust to provide end-to-end encrypted immutable on-chain messaging.

dChat solution--The FOURim Protocol leverages the Solana blockchain to serve as an immutable ledger exchanging E2EE on-chain messages from FOURwaL wallet SOL address A to FOURwaL wallet SOL address B. (*4THPILLAR TECHNOLOGIES Layer 1 Blockchain Instant Messaging (i.e. FOURim) Light Paper*, n.d.). The FOURim protocol connects to the Solana blockchain node using JSON-RPC protocol. The FOURim protocol connects to the Solana blockchain node using JSON-RPC protocol. Solana serves as an immutable Layer 1 blockchain ledger exchanging short encrypted messages from FOURwaL SOL wallet address A to FOURwaL SOL wallet address B. The 4thTech dID connects 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 (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 Solana blockchain 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.

dChat user control--With FOURim Protocol, the dChat users gain control over their messages, the messages are end-to-end encrypted and stored on the Solana Blockchain. Messages are not stored on a company server! Every message is signed with the receiver's public key. Your Solana 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!

dChat Encryption--FOURim dChat Protocol utilises RSA encryption to secure immutable blockchain message exchange. The dChat messages are end-to-end encrypted with the asymmetric algorithm (i.e., RSA), which is used to encrypt the message with the public key of the receiver. This design does not allow an attacker to infer relationships between segments of the encrypted message. To speed up the message loading process, caching was enabled to prevent repeatedly loading all data from a blockchain that was already retrieved in the past.

dChat 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. All data on the Solana blockchain is saved in the PDA accounts. PDA accounts are owned by the FOURim Protocol program.

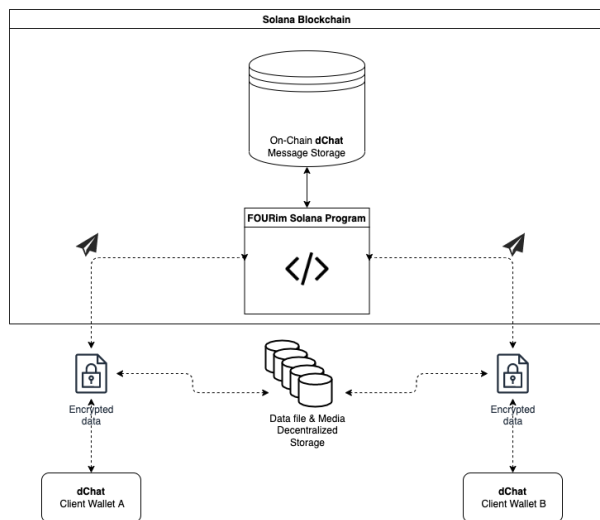
Speed and transaction pricing testing results--After significant testing on DevNet and MainNet, we have concluded that the send or receive message speed depends on the message length, encryption (decryption) and transaction finality as it varies between 1 to 5 seconds. As every message represents its 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."

Architecture & dChat process; (1) dChat message from Client A gets encrypted with a public key; (2) dChat message is sent to Solana FOURim Protocol Program; (3) dChat message is temporarily stored on-chain (i.e. 7-days); (4) dChat message of Client B is decrypted with the private key; (5) Media & data files from Client A are encrypted with a public key; (6) Encrypted media & data files are sent to decentralized storage (i.e. in development), and; (7) Media & data files of Client B are decrypted with the private key



Solana technical--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.

***Note;** Messages are temporarily stored on-chain for 7-days, after 7-days the messages are deleted. Please backup your conversations regularly if needed.

***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. MULTI-CHAIN CLIENT APP WALLET (i.e., FOURwaL)

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--With a single purpose, the 4thTech wallet (i.e., FOURwaL) serves as a blockchain gateway, a tool for 4thTech UI-platform access. 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) 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.

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. The 4thTech UI-platform 2.0 enables users to solve important technical blockchain challenges within a niche sector of data exchange while supporting Ethereum, HashNet and Substrate public and private chains.

***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) 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) MySQL database is used to store; (1) user nicknames; (2) platform settings; (3) user wallets, and; (4) RSA public key for data encryption. Data exchange within the MySQL database is protected with an HTTPS connection and a firewall. In the case of a user request, it is possible to delete any user-related data to comply with GDPR; (2) data file cloud repository is used for the temporary 7-days storage of encrypted data files that are exchanged between wallets in the dMail process. The decryption of the data files is possible only with a private key of the user. 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; (3) local storage is used to store; (1) FOURwaL private keys; (2) dChat short messages, and; (3) user-initiated backup of conversations, data files and reports. The security of local storage is in the user's domain, and; (4) blockchain (i.e. Kovan, SI-Chain, Edgeware TestNet, Solana TestNet) is used to store; (1) a link to the encrypted metadata file and timestamp (i.e. dMail); (2) encrypted message, timestamp and sender address (i.e. dChat). The overall security of the blockchain network depends on its decentralization, while access security depends on the user's private key safety measures.

***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. FOUR-TOKEN, ECOSYSTEM NATIVE MULTI-CHAIN ASSET

A multi-chain non-dilutive asset, a technical component that enables 4thTech tokenization with staking and transaction discounts. Developed and deployed in 2018, FOUR acted as one of the technical components needed for the 4thTech ecosystem tokenization on Ethereum network, combining three technical utility features; (1) embedded TTS interface (i.e., token teleportation-service); (2) MTO (i.e., multiple-transfer option), and; (3) GAS feature. Due to Ethereum gas prices increase, the

ERC-20 FOUR had to evolve to become a multiverse asset occupying the space of multi-chains, while being used as the primary means to enable 4thTech services, services discounts, incentivize participants and provide a default mechanism to store and exchange value. The 4thTech economy utilises FOUR as a unit of value on the web platform that enables token holders with the right to access applications and earn services discounts by staking FOUR in the ecosystem. 4thTech token (i.e., FOUR) is the ecosystem native utility token, used as the primary means to enable services, incentivize participants. It represents a unit of value with the right to stake, right to signal, right to @Member Discord role and access to dMail & dChat TX discounts while enabling ecosystem tokenization.

Technical erc-20 FOUR information;

- (1) Ethereum ERC-20 FOUR;
- (2) name: The 4th Pillar Token;
- (3) symbol: FOUR; (4) token smart contract address: 0x4730fb1463a6f1f44aeb45f6c5c422427f37f4d0;
- (5) ticker colour: black, grey, 4thTech blue;
- (6) decimals: 18;
- (7) blockchain explorer: <https://etherscan.io/token/0x4730fb1463a6f1f44aeb45f6c5c422427f37f4d0>;
- (8) utility: TTS, MTO, GAS, right to stake, right to dMail & dChat TX discount, right to features access, right to signal, right to @Member Discord role

Multi-chain asset--Cross-chain interoperability of ERC-20 FOUR with other blockchains essentially increases the decentralisation of liquidity and unlocks a universe of possibilities for further development. The users instantly benefit from lower fees and the native DeFi economy of the bridged blockchain. With an unchanged total and circulating token supply, the FOUR ERC-20 currently exists on its native Ethereum blockchain, while a wrapped synthetic version exists on the bridged blockchains; (1) Binance Smart Chain; (2) Polygon, and; (3) Solana blockchain.

***More token related information:**
<https://wiki.the4thpillar.com/intro/token.html#smart-contract>

FOUR staking & tokenization--FOUR staking provides FOUR holders with rewards in the form of dMail & dChat service fee margin discounts, while it enables additional features. By staking, the user agrees to lock up their FOUR tokens for a certain period, during which they are unspendable. FOUR staking acts on behalf of user benefit to secure services fee margin discounts when executing dMail & dChat TX and unlocking additional features. Minimalistic and intuitive UI-platform design enables users to stake FOUR with a single click.

Services fees--With the FOUR staking deployment, 4thTech will start to charge services fee margin in cryptographic tokens to execute data exchange from wallet to wallet. The total public-chain service fee is based on chosen public blockchain network TX (i.e. transaction) cost, and added 4thTech service fee margin. In the case of dMail public-blockchain network TX cost is based on two TX. The first TX saves the link to the metadata file and checksum of the metadata file to the SC as the second TX sends the transaction fee in the native token (i.e. ETH, EDG, TOL, SOL) to the solution fee taker address. 4thTech services fee margins are added and are defined in FIAT but converted in ETH, EGD, TOL or SOL based on the market exchange rate. The overall dMail or dChat TX GAS_PRICE FEE depends on the public-blockchain network selected.

Tokenization & Staking use case--Let's assume that:

*public blockchain TX COST = 0.03\$

*dChat services FEE_MARGIN = 5\$

*TOTAL USER COST = 5,03\$

*FOUR_STAKING DISCOUNT = 50% (if FOUR is STAKED at the highest tier)

*TOTAL USER COST USING FOUR_STAKING = 2,53\$ (settled in native the token of the chosen supported public blockchain)

***Note:** 4thTech services fee will be defined parallel to the staking protocol deployment.

XI. STORAGE

A database represents an organized collection of data, stored and accessed electronically. 4 databases are formed in the 4thTech system; (1) **MySQL database** is used to store; (1) user nicknames; (2) platform settings; (3) user wallets, and; (4) RSA public key for data encryption. Data exchange within the MySQL database is protected with an HTTPS connection and a firewall. In the case of a user request, it is possible to delete any user-related data to comply with GDPR; (2) **data file cloud repository** is used for the temporary 7-days storage of encrypted data files that are exchanged between wallets in the FOURdx process. The decryption of the data files is possible only with a private key of the user. 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; (3) **local storage** is used to store; (1) FOURwaL private keys; (2) dChat short messages, and; (3) user-initiated backup of conversations, data files and reports. The security of local storage is in the user's domain, and; (4) **blockchain** (Ethereum, Tolar HashNet, Substrate, Solana) is used to store; (1) a link to the encrypted metadata file and timestamp (dMail); (2) encrypted message, timestamp and sender address (dChat). The overall security of the blockchain network depends on its decentralization, while access security depends on the user's private key safety measures.

XII. 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 blockchains were added, both chosen based on their uniqueness. The support for HashNet protocol was added already in July 2020, while Edgware, a Polkadot Substrate was added in v2.0. HashNet DLT is a ground platform we find essential to building the 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. Edgware 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 programing, which enables us to add additional blockchain support when needed. Solana blockchain support was added in Q2 2021 to enable a secure affordable Layer 1 instant messaging solution. According to Solana (*Scalable Blockchain Infrastructure: Billions of Transactions & Counting* | Solana: Build Crypto Apps That Scale, n.d.), Solana is the next generation censorship-resistant blockchain with over 500 validators, extreme transaction speeds and low cost, therefore perfect for Layer 1 on-chain instant messaging. Solana leverages Proof of

History and several other breakthrough innovations to allow the network to scale at the rate of Moore's Law.

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/Edgware and Solana node, 4thTech uses JSON-RPC protocol.

XIII. SECURITY PROTOCOLS

4thTech utilizes advanced encryption standards (i.e. AES), with a combination of RSA encryption and hash algorithm 256 (i.e. SHA 256) to secure immutable dMail and dChat communication. The data is encrypted with a symmetric algorithm (i.e. AES), as the asymmetric algorithm (i.e. RSA) is used to encrypt the symmetric key and initialization vector (i.e. IV) with the public key of the receiver. 4thTech encryption design does not allow an attacker to infer relationships between segments of the encrypted message. SHA 256 is defined as one of the most secure ways to protect digital information. SHA 256 is a mathematical process that generates a 256 bit (64 characters long) random sequence of letters and numbers (hash) out of any input. Secure hash algorithm 256 is used to calculate the file content hash value when executing an on-chain data file exchange transaction via smart contract.

XIV. 4THTECH AS MULTI-BLOCKCHAIN APPLICATION

Multi-blockchain support enables transaction cost and speed choice, which is especially important when dealing with public blockchains. Next, to already supported Ethereum, three additional blockchains were added to support 4thTech dID, dMail and dNotary, all chosen based on their uniqueness. The support for Tolar HashNet protocol was added in v1.0 already in July 2020, while Edgware, a Polkadot Substrate was added in v2.0. Solana blockchain support was added in Q2 2021 to enable a private, immutable on-chain dChat. Special logic was added into programing, 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. Tolar HashNet can handle a high volume of transactions, while the platform ensures valid, scalable usage which makes it perfect for Enterprise applications (tolar.io, 2019). Substrate Edgware 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. According to Polkadot (*POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK*, n.d.) smart contracts are written in Ink! programming language. Ink! is a Rust-based eDSL for writing Wasm smart contracts specifically for the Contracts module. According to Solana.com, Solana is the next generation censorship-resistant blockchain with over 500 validators, extreme transaction speeds and low cost.

Connectivity--4thTech uses hosted Ethereum-node on Infura over JSON-RPC protocol, to connect to the Ethereum node. In the case of Tolar 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 Edgeware and Solana node, 4thTech uses JSON-RPC protocol.

XV. DATA PROTECTION

4thTech dMail does not store the transmitted data and attachments on-chain. The E2EE data is temporarily (i.e. 7-days) stored off-chain. The protocol records links to encrypted files and hashes of the encrypted content on the blockchain. This safeguards the rights of individuals to confidentiality, privacy and enables data deletion. The data can be accessed only with the user's private key. 4thTech does not hold any private keys, private key is available only to the user.

To achieve the security of decentralization, the dChat messages are not stored on a company server but are temporarily stored on the Solana blockchain itself and deleted after 7 days.

****Note:** Currently GDPR compliant centralized off-chain storage is used, that complies with the mentioned directives, when a decentralized storage option will be available, the compliance solutions will be addressed.*

XVI. REGULATORY AND RISK MIGRATION

The exchange (i.e., swap) of the four-token is available on the designated exchanges and de-fi protocols and it is not a public offering of equity or debt and, consequently, does not fall under securities or any prospectus regulation. According to the legal opinion of YSL Legal LLP, the four-tokens are not "capital markets products" as stipulated or contemplated under the Securities and Futures Act by the Token Functions. The four-tokens are not securities as defined under applicable laws. Therefore, the four-tokens have not been registered with any competent regulator. The exchange (i.e., swap) of the four-tokens is unregulated. Changes to legislation in the most relevant jurisdictions in the world are closely monitored. Appropriate actions will be undertaken to act accordingly if regulatory changes impact the four-token exchange and operations. We are not a financial institution and are currently not under the supervision of any financial supervisory authority. We do not provide any licensed financial services, such as investment or brokerage services, capital raising, fund management or investment advice.

XVII. BLOCKCHAIN, GDPR AND 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 the 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.*

XIX. CONCLUSION

Privacy, data ownership and secure online communication is fundamental right of every person. With the help of advanced Web 3.0 blockchain protocols as an underlying infrastructure, 4thTech enables a suitable E2EE dApp 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.

XX. DISCLAIMER

4thTech is a blockchain technology innovation and development initiative. Its main focus goes to the development of future Web3 communication technology. 4thTech does not guarantee or influence the token price or deal with financial or trading token elements, nor offer any licensed financial services, such as investment or brokerage services, capital raising, fund management, or investment advice. The content of this paper is provided for information purposes only and is not to be used or considered to be an investment recommendation or an offer or solicitation to buy, sell or subscribe to any securities or other financial instruments.

****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.). Retrieved July 5, 2021, from <http://adriatic-council.eu/beyond-4-0-ljubljana-2018/>
- 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-for-digital-identity.* (n.d.). Retrieved December 31, 2020, from <https://www.nec.com/en/global/solutions/blockchain/blockchain-for-digital-identity.html>
- Blockchain Technologies | Shaping Europe's digital future.* (n.d.). Retrieved May 5, 2020, from <https://ec.europa.eu/digital-single-market/en/blockchain-technologies>
- 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).
- 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 W A N D T E I N F O R M A T I O N S T E C H N I K F I T.*
- POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK.* (n.d.). Retrieved December 31, 2020, from <https://github.com/ethereum/wiki/wiki/Chain-Fibers-Redux>
- Regulating emerging technology | Deloitte Insights.* (n.d.). Retrieved May 5, 2020, from https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html?id=gx%253A2sm%253A3tw%253A4FoRPart12018%253A%253A6Public_Sector%253A20180623170500%253AGlobal&linkId=53371991
- Scalable Blockchain Infrastructure: Billions of transactions & counting | Solana: Build crypto apps that scale.* (n.d.). Retrieved July 5, 2021, from <https://solana.com/>
- The Best Blockchain Business Models | Blockchain Council.* (n.d.). Retrieved May 5, 2020, from <https://www.blockchain-council.org/blockchain/the-best-blockchain-business-models/>
- 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>
- tolar.io. (2019). *Tolar - Next-gen cryptocurrency.* Tolar.Io. <https://www.tolar.io/>
- YSL Legal (2020) <https://github.com/4thtech/static-assets/raw/main/pdf/four-ysl-legal-opinion-summary.pdf>
- Time For Trust: How blockchain will transform business and the*