Block Labs publications
Type: Light Paper
Authors: Dr. Tali Režun, Denis Jazbec
Status: Published
Updated: 27.02.2022
https://4thtech.io/

# Open Source E2EE on-chain Instant Messaging --FOURim dChat Protocol Light Paper--

**Abstract--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.**

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

*Keywords: web3, 4thpillar, 4thTech, dChat, internet, digital transformation, blockchain technology, decentralization, peer-to-peer, online trust, online security, online privacy, DLT, Solana blockchain*

## I. INTRODUCTION

In this day of age, privacy is becoming more and more important. We depend on online communication as it's becoming a normal part of our lives. Privacy in online communication is a fundamental right of every person. Exchanging private short messages securely over the internet should be easy and accessible to all. Blockchain technology proposes the ideal foundation to enable this solution. Up to now, on-chain 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 within our reach. To address this issue the *4thTech is* proposing a safe, fast Solana-based solution, which leverages blockchain trust and provides a secure, immutable, instant wallet-to-wallet messaging application.

## II. INTRO TO 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.[1]

After two years of *4thTech MVP* (i.e., minimum viable product) 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.

**Note;* *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.* [2]

***Foundation***--In April 2021, 4thTech launched the *UI-platform 2.0* and *Wallet 2.0* (i.e., FOURwaL) and with that enabled further ecosystem development. The UI-platform 2.0 codebase has been rewritten with *TypeScript*, a superset of JavaScript that supports a type system and compiles to plain JavaScript. The platform has also overgone the crucial upgrade from Vue 2 to *Vue 3*, which is much more performant. Under the hood, *Vue 3* is completely rewritten with TypeScript.

**Note;* *Vue is a progressive framework for building user interfaces. Unlike other monolithic frameworks, Vue is designed from the ground up to be incrementally adoptable. The core library is focused on the view layer only and is easy to pick up and integrate with other libraries or existing projects.*[3]

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 Edgeware, 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.

## II. dCHAT, FOURIM INSTANT MESSAGING PROTOCOL

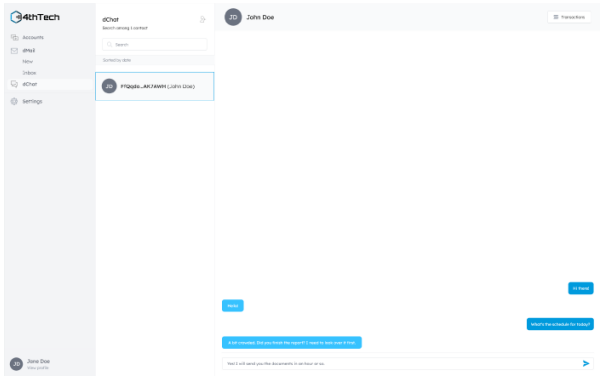
Privacy in online communication is a fundamental right of every person. Exchanging private E2EE instant messages

[1] https://github.com/4thtech/static-assets/raw/main/pdf/whitepaper.pdf [accessed 5 May 2021]
[2] http://adriatic-council.eu/beyond-4-0-ljubljana-2018/ [accessed 10 May 2021]
[3] https://v3.vuejs.org/guide/introduction.html [accessed 20 May 2021]

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. According to Solana.com, 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.[4]

The aim and project objective is to enable; (1) a secure affordable »on-chain« messaging solution with no ads, no data mining, no tracking and no phone number onboarding requirement; (2) wider adoption of blockchain technology, and; (3) to pioneer the future of on-chain messaging.

***dChat solution—***Powered by the FOURim open-source protocol that 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. The FOURim protocol connects to the Solana blockchain node using JSON-RPC protocol, while 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.

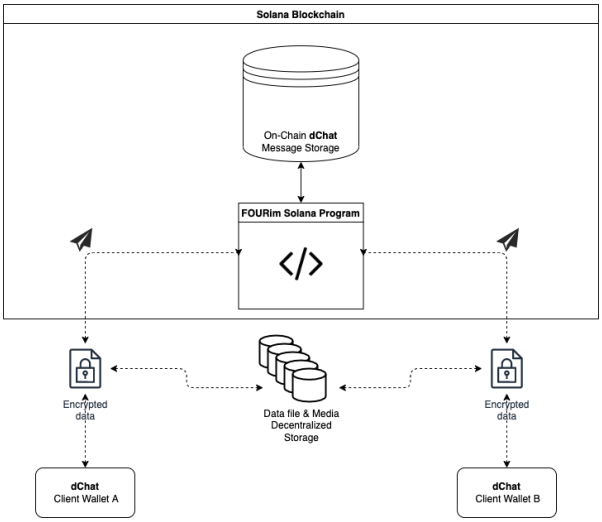



***dChat user control—***The FOURim Protocol enables dChat users to gain control over their messages. The messages are E2EE (i.e. end-to-end encrypted) and stored on the Solana Blockchain. Messages are not stored on a company server! Every message is signed with the receiver's public key. Your Solana 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 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 (i.e. smart contract).

***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

[4] https://solana.com/ [accessed 11 May 2021]

is increased. *JSON-RPC* protocol is used to connect to the Solana blockchain node.

***Solution components;*** (1) 4thTech Chromium and Firefox add-on wallet (i.e. FOURwaL) with added Solana blockchain support; (2) 4thTech dID (i.e. FOURid) which serves as a public key exchange point between both users; (3) 4thTech UI-platform; (4) FOUR token, a multi-blockchain asset that enables the user with the right to stake and access, while providing services fee discounts and activating additional feature inside the 4thTech UI-platform.

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

***dChat spec***--The solution technical and function specification breakdown can be specified as follows;

(1) Deployment: *Solana public blockchain*,
(2) Blockchain gateway: *FOURwaL*,
(3) Platform: *4thTech UI-platform, 4thTech UI-staging*
(4) Discount Activation: *FOUR token (i.e. in development)*
(5) Transaction payment; *SOL token*
(6) Programming languages: *JS, PHP, Rust*
(7) On-chain deployment: *Smart Contract*
(8) Encryption: *RSA* (i.e., Rivest–Shamir–Adleman algorithm)

**Note;** *RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public-key cryptography because one of the keys can be given to anyone.*[5]

***Storage***--A database represents an organized collection of data, stored and accessed electronically. 4 databases are formed in the 4thTech ecosystem; (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** (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.

***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."

***Note:** Results were measured on 21.12.2021 with SOL price at 190$.*

***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*

## III. WALLET *(i.e., FOURwaL)*

With a single purpose, the 4thTech wallet (i.e. FOURwaL) serves as a blockchain gateway, a unique tool for 4thTech UI-platform access and protocol operations. It provides a secure way to connect to 4thTech products (i.e. dID, dMail, **dChat**, dNotary) as it contains a pair of public and private cryptographic keys.
A public key allows; (**1**) RSA encryption of data; (**2**) screening of recipient wallet addresses (i.e. Ethereum, Tolar HashNet, Substrate, Solana); (**3**) for other wallets to execute 4thTech services to the desired wallet's address, whereas a private key enables the decryption of received communication such as data files and short messages from the sender address. With the exception of the backup and restore function, all the wallet account management is available within the UI-platform.[6]

**Note;** *According to Wiki, 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 wallet can be referred also as blockchain wallets. Up to now, blockchain*

[5] https://en.wikipedia.org/wiki/RSA_(cryptosystem) [accessed 20 May 2021]

[6] https://wiki.4thtech.io/intro/discover.html#fourwal-4thtech-multi-chain-client-app-wallet [accessed 20 May 2021]

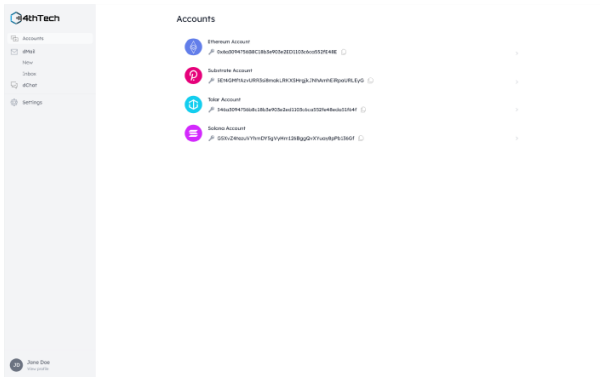
*wallet was mostly used for cryptocurrency asset holding and exchange.*[7]

*****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*

## IV. UI-PLATFORM

The 4thTech UI-platform serves as an onboarding hub accessed by the user via a Google Chrome or Mozilla Firefox web browser with an installed FOURwaL blockchain wallet add-on. It connects and hosts all the deployed 4thTech protocols and services in one ecosystem, giving the user all in one access. 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 UI; (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.




## V. CONCLUSION

Blockchain already establishes its technology and its decentralized advantages. Now it is on us to develop useful use cases such as E2EE dChat, and in our case enable online privacy of data and communication. With the arrival of fast 3.0 blockchains such as Solana, the fast execution protocols such as FOURim can become a reality. Some compromises have to be accepted to gain secure, decentralized, on-chain short message communication with no data mining, ads or tracking. As every message represents its on-chain confirmed transaction and needs to be encrypted and decrypted the execution takes between 1 to 5 seconds. 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. Let's not forget how much time an Ethereum transaction can take, so waiting a few seconds for the message execution is still a small price to pay if private communication is within reach. As the use of decentralized applications tends to cause confusion and difficulties, we have worked hard to develop an efficient and jet simple wallet-to-wallet dMail and dChat user interface, which manifested itself in the form of a 4thTech UI-platform client.

## VI. DISCLAIMER

4thpillar Technologies *(i.e., 4thTech)* is a blockchain technology innovation and development initiative. Its main focus goes to the development of future experimental blockchain 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 light 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.

## BIOS

***Dr. Tali Rezun;*** *Slovenian, of Slovenian and Jordanian origin. Born in Ljubljana in 1978, he started his entrepreneurial career at the age of 18 and grew his business organically until this day. Under the domain of Cotrugli Business School, Tali finished his EMBA and later in 2018 his Business Doctorate (i.e., DBA), specializing in online technology. Dr. Režun specializes in online brand awareness, web application development and blockchain technology. He enjoys the title of lecturer, advisor and UN/CEFACT expert.*[8]

***Denis Jazbec;*** *Software engineer with more than a decade of experience. He is researching and developing blockchain and DLT solutions and acts as a main solution architect of the 4thpillar technologies project. Denis singlehandedly innovated the 4thTech solution of blockchain electronic data exchange. Highly proficient in PHP, JS, Vue.js, Typescript, MySQL and specializes in IT infrastructure, DLT networks and blockchain implementation, while developing in-depth knowledge on multi-blockchain processes and transactions, which makes him an expert in its field.*

[7] https://en.wikipedia.org/wiki/Cryptocurrency_wallet [accessed 20 May 2021]

[8] https://talirezun.com/ [accessed 20 May 2021]