Block Labs publications
Type: Light Paper
Authors: Dr. Tali Režun, Denis Jazbec
Status: Published
Updated: 26.09.2022
https://4thtech.io/

Solana-L1 Secured W2W dChat Communication Framework
--FOURim Protocol Light Paper--

Abstract--Whenever we speak about online security, we consider it a topic important to us. Securing your digital communications should be your highest priority when going online. Blockchain has 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 early-generation blockchains' scalability and cost constraints. With the arrival of the Solana blockchain, on-chain instant messaging can become a reality. To address this issue the 4thTech developed a Solana-based dChat, which leverages L1s trust to provide end-to-end encrypted immutable on-chain messaging.

Dr. Tali Režun, head of 4thTech R&D

Keywords: Web3, 4thTech, dChat, internet, digital transformation, blockchain technology, decentralization, peer-to-peer, online trust, online security, online privacy, Solana blockchain

I. BACKGROUND

Background key points; (1) the right to online safety should be above all and provided for all online communications; (2) blockchain protocols offered great promise but scalability, throughput and cost were always an issue; (3) Web3 projects & DAOs all use Web2 communication tools, which goes against the decentralization ethos, and; (4) immutable on-chain W2W messaging is prime to become the future of secure communication - Not Your Keys, Not Your Message!

II. SOLUTION KEY POINTS

Solution key points; (1) establishing an on-chain communication framework that is web, desktop & mobile interoperable (one message = one L1 Transaction); (2) bringing social communication to the Web3 Ecosystem; (3) E2EE secure, immutable, censorship-resistant, scalable & accessible »on-chain« messaging; (4) Web3 wallet login, no signup or personal information; (5) resistant to data mining, data tracking & identity theft; (6) W2W private, group & community on-chain messaging with an option of NFT curated chat groups; (7) data file & media sharing via decentralized storage; (8) stand-alone app or White labelled (SDK); (9) interoperable with all significant wallets, and; (1) due to heavy on-chain activity (i.e. 1 message = 1 TX), 4thTech dApps can bring significant growth in daily L1 transactions volume.

III. INTRO TO 4THTECH

We spent the last 4 years developing the 4thTech foundations, which are built around security and ecosystem integrations. Security by design was our guiding approach when building 4thTech. That simply means that we put the consideration of how we could preserve privacy, guarantee protection, and obfuscate metadata to the largest possible degree at the forefront of all our Architectural decisions. At the same time, no personal data whatsoever is collected by 4thTech.

We were able to build the multi-chain framework that is Ethereum, Substrate and Solana interoperable and enables on-chain email and messaging that is private, secure, censorship-resistant, and immutable. Our tech enables both W2W communication as well as E2EE group chat with an additional component of curated community chat groups. Users are also able to share files, and media, through the wallet, in the form of dMail or dChat attachments.

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.

**Validation;* *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.* [1] *Other acknowledgement followed such as Solana FOURim Protocol endorsement*[2] *and Tron Hackathon win*[3]*.*

Value Proposition--When you think about 4thTech and what value it delivers, it really is quite straightforward. There are four major value propositions; (1) 4thTech utilises blockchain to

[1] http://adriatic-council.eu/beyond-4-0-ljubljana-2018/ [accessed 10 May 2021]

[2] https://twitter.com/solana/status/1482045683364511759?s=20&t=LktZ7w2s0D1OEAN9rNuBmA [accessed 10 September 2022]

[3] https://devpost.com/software/4thtech-privacy-enabled-w2w-communication-infrastructure [accessed 10 September 2022]

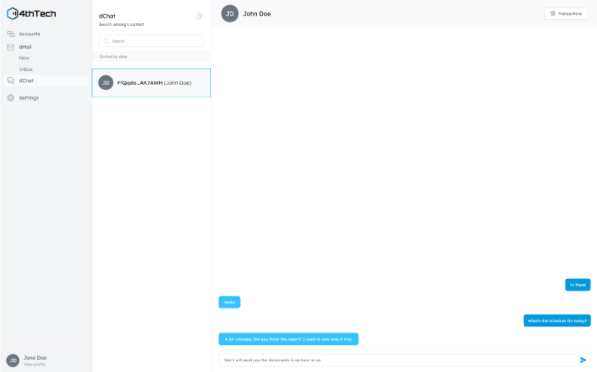
enable security in online communication, which is now virtually non-existing in traditional Web2 applications; (2) behind the scenes, 4thTech enables any project to integrate the dMail & dChat layers into their platform UIs or wallets using the SDK framework, and; (3) to ensure true on-chain security 4thTech protocols have to be transaction heavy as every message represents its own transaction. Due to this heavy on-chain activity (i.e. one message = one transaction), 4thTech dApps bring significant growth in daily L1 transactions.

IV. FOURIM PROTOCOL, W2W E2EE dChat

Privacy and security 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 next-gen blockchain, on-chain »instant« messaging is becoming a reality. To address this issue the 4thTech developed a Solana-based dChat, which leverages the L1 to provide end-to-end encrypted immutable on-chain messaging.

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 and communication.

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 SOL address A to 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).



Hi there!

Hello!

What's the schedule for today?

A bit crowded. Did you finish the report? I need to look over it first.

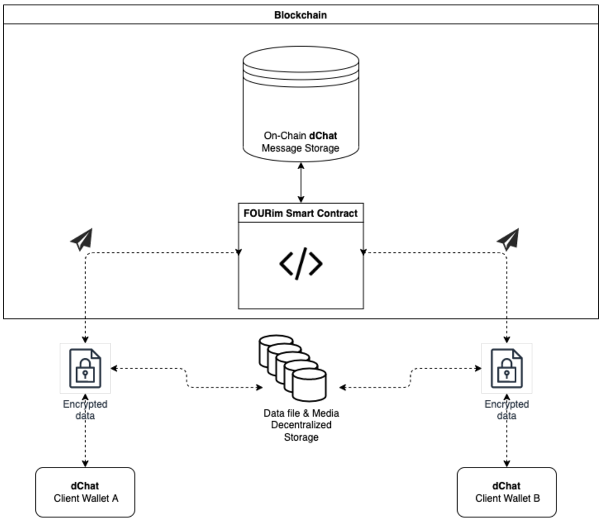
Yes! I will send you the documents in an hour or so.

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



dChat structure diagram

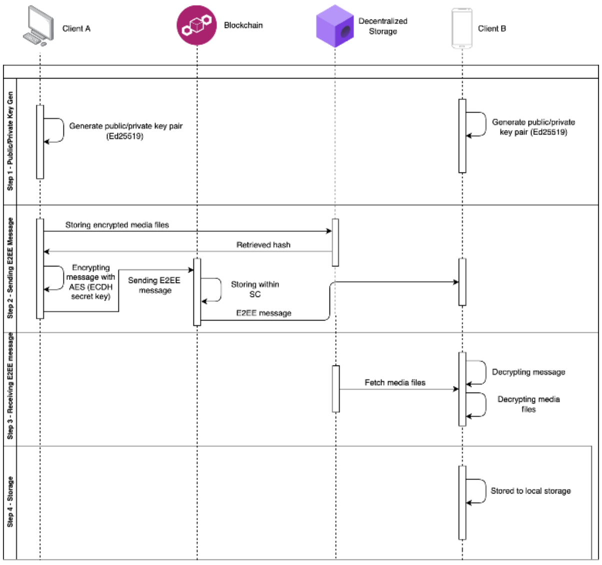
Messaging Process—the messaging process itself is pretty straightforward. Let's take an example of Alice (i.e. Client A) and Bob (i.e. Client B);

(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.


Client A
Blockchain
Decentralized Storage
Client B
Step 1 - Public/Private Key Gen
Generate public/private key pair (Ed25519)
Generate public/private key pair (Ed25519)
Step 2 - Sending E2EE Message
Storing encrypted media files
Retrieved hash
Encrypting message with AES (ECDH secret key)
Sending E2EE message
Storing within SC
E2EE message
Step 3 - Receiving E2EE message
Fetch media files
Decrypting message
Decrypting media files
Step 4 - Storage
Stored to local storage

dChat process diagram

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

Solution components; (1) FOURim Protocol smart contact/program; (2) L1 blockchain; (3) Web3 wallet; (4) FOURid Protocol (i.e. serves as a public key exchange point between both users); (5) UI-platform (i.e. dChat front-end); (6) encryption cocktail, and; (5) decentralized storage.

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

(1) Deployment: *Solana TestNet & MainNet*
(2) Blockchain gateway: *FOURwaL (i.e. TestNet wallet)*,
(3) Platform: *4thTech UI-staging*
(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.*[4]

Storage—There are 4 databases are forming in the 4thTech 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 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; (a) wallet private keys; (b) 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.

Features—Although the primary focus of 4thTech is on security, and censorship resistance of emails and messaging, we do not want to neglect the UI/UX aspect of giving our users a great experience using the chat or email which would have a similar look and feel like their favourite email or messaging app but with specific crypto features; (1) E2EE private & group messaging; (2) E2EE NFT curated chat groups; (3) sending media & data files via decentralized storage; (4) multiple conversations channels; (5) notifications; (6) NFT profiles & emojis; (7) chat conversation archive option; (8) Web3 login, and; (9) SDK & white-label.

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

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

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.4thtech.io/docs/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. Except for the backup and restore function, all the wallet account management is available within the UI-staging platform.[5]

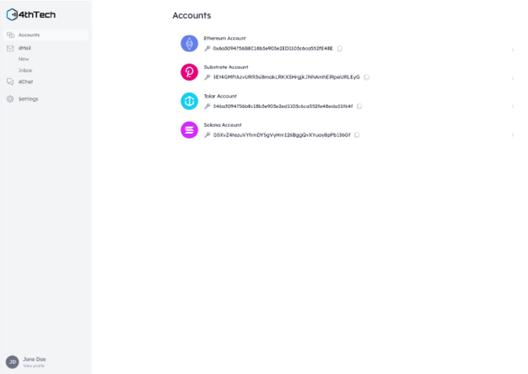
**Note;* *4thTech TestNet wallet is currently needed to connect to the UI. To enable the use of other popular wallets such as Phantom, we have to upgrade the encryption standard to Elliptic-Curve Diffie-Hellman.*

**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.



Accounts

Ethereum Account
0x6a3094756B8C18b3e903e2ED1103c6ca552fE48E

Substrate Account
5Et4GMftAzvURR3si8makLRKXSHrgjkJNhAmhERpaURLEyG

Tolar Account
546a3094756b8c18b3e903e2ed1103c6ca552fe48eda51f64f

Solana Account
G5XvZ4tezuVYhmDY5gVyHm126BggQvXYuay8pPb136Gf

In April 2021, 4thTech launched *UI-platform 2.0* and *Wallet 2.0* (i.e., FOURwaL) and 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 adaptable. The core library is focused on the view layer only and is easy to pick up and integrate with other libraries or existing projects.*[6]

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 security of data and communication. With the arrival of fast 3.0 blockchains, 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 L1 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

All content provided herein, including but not limited to text, graphics, logos, and images (the "Content"), is the property of Block Labs Luxembourg S.a r.l., a legal entity established under the laws of the Grand Duchy of Luxembourg, registered with R.C.S. Luxembourg under N B263508 at the following address: 41, rue du Puits Romain, z.a. Bourmicht (Atrium Business Park), L-8070 Bertrange, Luxembourg (the "Company" or "we"). It is protected by copyright and other laws that protect intellectual property and proprietary rights. You are granted a non-exclusive, non-transferable, revocable license to access and use the Content for the sole purpose of obtaining information

[5] https://wiki.4thtech.io/docs/wallets [accessed 20 May 2021]

[6] https://v3.vuejs.org/guide/introduction.html [accessed 20 May 2021]

about the 4thTech technology and other educational purposes. We have done our best to ensure that the Content is accurate, updated, complete, and provides valuable information, but neither do we guarantee nor take any responsibility for its accuracy and/or completeness. The Content is not intended as, and shall not be understood or construed as legal, financial, tax, or any other professional advice, sale or offer for sale of any securities, and/or crypto-assets. The Company is not engaged in rending of and/or is not licensed to render any of the crypto-asset services and/or financial services, such as investment or brokerage services, capital raising, fund management, or investment advice.

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.*[7]

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 4thTech 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://talirezun.com/ [accessed 20 May 2021]