4thpillar Technologies publications
Type: Light Paper
Authors: Dr. Tali Režun, Denis Jazbec
Status: Published
Europe 01.08.2021
https://the4thpillar.io/, https://4thtech.io/

4thpillar Technologies (i.e., 4thTech)
Layer 1 blockchain instant messaging (i.e., FOURim) Light Paper

The internet changed the way we live, it opened the ways of unlimited communication and revolutionized access to information, but it failed greatly regarding our digital freedom. Instead of providing trust, granted privacy, security, peer-to-peer communication, simplification, and digital money, it evolved into a system of global intermediaries, that manipulate and exploit our private data. There is a new technology at the gates called blockchain, which in its core excludes any intermediary's, it brings peer-to-peer communication, online trust, security, privacy, authenticity, synchronised ledger and much more. 4thpillar Technologies *(i.e., 4thTech)* main innovation is the multi-blockchain (i.e., Ethereum, HashNet, Polkadot Edgeware…) digital data exchange protocol, accompanied by a unique digital identity solution. With the development of Solana, the close to real-time blockchain applications are beginning to take shape, with that the idea of the true on-chain instant messaging (i.e., chat) came to life. This light paper was written as a hybrid addressing the *4thpillar Technologies* product concept benefits and solutions.

Dr. Tali Režun, head of 4thTech initiative

Keywords: web3, 4thpillar, 4thTech, fourdx, fourid, fourns, fourim, four token, internet, digital transformation, blockchain technology, decentralization, peer-to-peer, online trust, online security, online privacy, DLT, Solana blockchain

1. 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 instant 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 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 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.

2. INTRO TO 4THTECH

In 2017, *4thTech* proposed and later developed a set of fully working solutions, which leverage trust provided by the blockchain to enable secure, immutable, instant cross-border wallet to wallet; (1) *identity protocol* (i.e., FOURid) that connects wallets when data is exchanged and serves as the public key exchange point between users; (2) *data exchange* (i.e., FOURdx) that provides a secure, immutable wallet A to wallet B (i.e., FOURwaL) data file and metadata exchange.; and; (3) digital *data verification* (i.e., FOURns), that provides unique digital data timestamp and file checksum authenticity verification. With the multi-blockchain deployment and support of Ethereum, HashNet, Polkadot Edgeware and now Solana, *4thTech* provide a variety of options for a user to choose when exchanging digital information over the blockchain, whether from the interoperability perspective, transaction cost or speed.[1]

[1] https://www.the4thpillar.io/documents/whitepaper.pdf
[accessed 5 May 2021]

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]

2. FOUNDATION

In April 2021, 4thTech launched the *Web Platform 2.0* and *Wallet 2.0* (i.e., FOURwaL) and with that enabled further ecosystem development. The 4thTech Web 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, two additional blockchains were already added; HashNet and Polkadot substrate Edgeware, both chosen based on their uniqueness. Due to extreme transaction speed, Solana comes as the fourth supported blockchain and will serve as the blockchain of choice enabling the *instant messaging protocol* (i.e., FOURim) and digital data exchange (i.e., FOURdx). Special logic was added into the programming of the *4thTech Web Platform 2.0*, which enables us to add additional blockchain support when needed.

3. INTRO TO SOLANA

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]

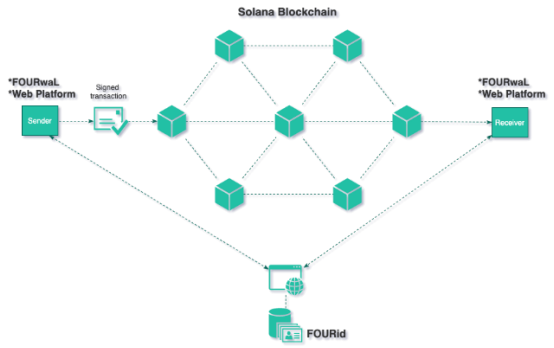
4. AIM AND OBJECTIVE

The aim and project objective are to enable; (1) a secure affordable »Layer 1« instant messaging solution; (2) wider adoption of blockchain technology, and; (3) to pioneer the future of on-chain messaging (i.e., chat).

5. THE SOLUTION

The FOURim protocol leverages the Solana blockchain to serve as an immutable »Layer 1« ledger exchanging encrypted messages from FOURwaL wallet address A to FOURwaL wallet address B theoretically in real-time[5]. The 4thTech *identity protocol* (i.e., FOURid) 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). According to Solana, the average transaction confirmation is 0.89s, with up to 50.000 TPS capacity and transaction (i.e., TX) price of 0.00025$ (21.5.2021), which enables almost real-time on-chain messages to exchange with low TX cost. The capacity of the message length and exact TX message cost will be determined in the test phase. There is a possibility of the unlimited message length which would directly correlate with TX price.

[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]
[4] https://solana.com/ [accessed 11 May 2021]
[5] https://www.the4thpillar.io/documents/FOURim-technical-diagram.png [accessed 11 May 2021]



5.1. SOLUTION COMPONENTS

The 4thTech instant messaging protocol (i.e. FOURim) main components are; (1) *4thTech Chromium*[6] *and Firefox*[7] *add-on wallet* (i.e., FOURwaL) with added Solana blockchain support; (2) *digital identity protocol* (i.e., FOURid) which serves as a public key exchange point between both users; (3) *4thTech User Client Web Platform*[8] which enables users with blockchain digital data file exchange, data verification protocol and will enable future instant messaging service (i.e., FOURim); (4) *FOUR token*[9], a multi-blockchain asset that as a locked (staked) asset acts as an enabler activating the instant messaging feature inside the *4thTech* Web Platform.

5.2. SPECIFICATION

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

(1) Deployment: *Solana public blockchain*,
(2) Blockchain gateway: *FOURwaL*,
(3) Platform: *4thTech Web Platform*,
(4) Activation: *FOUR token* Web Platform Staking
(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.*[10]

5.3. PROCESS

The FOURim messaging exchange process; (1) encryption of instant message; (2) the execution of blockchain transactions, via smart contract.

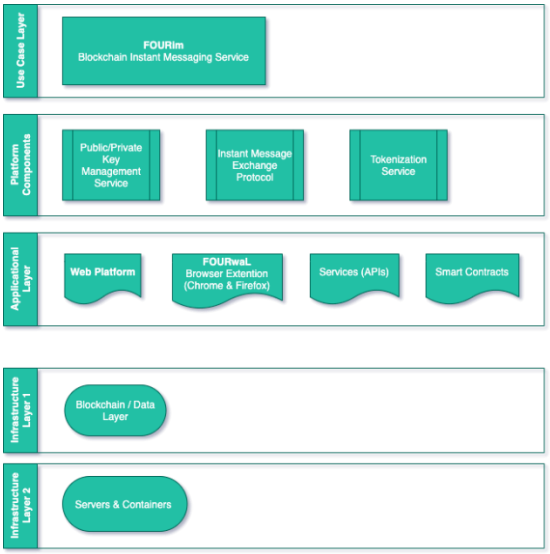
5.4. CONNECTION TO SOLANA BLOCKCHAIN

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

5.5. SECURITY

FOURim utilizes *RSA* encryption to secure immutable blockchain instant message exchange. The messages are encrypted with the asymmetric algorithm (i.e., RSA), which is used to encrypt the instant message with the public key of the receiver. This design does not allow an attacker to infer relationships between segments of the encrypted message.

6. LAYER INFRASTRUCTURE DIAGRAM



[6] https://chrome.google.com/webstore/detail/fourwal-4thtech-wallet/ahcefhodjjnpmeeaghfhocjiicghdcbn?hl=sl&authuser=5 [accessed 20 May 2021]

[7] https://addons.mozilla.org/sl/firefox/addon/fourwal-4thtech-wallet/ [accessed 20 May 2021]

[8] https://www.the4thpillar.com/ [accessed 20 May 2021]

[9] https://wiki.the4thpillar.com/guide/discover.html#four-token [accessed 18 May 2021]

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

(1) *use cases* layer defines the FOURim (i.e. blockchain instant messages protocol); (2) the second layer defines the *platform components* (i.e. public/private key management service, instant message exchange protocol and tokenization service; (3) the third layer defines the *applications* (i.e. web platform, browser extension wallet, API services and smart contracts), and; (4) an *infrastructural layers* are defining capabilities and connectivity's to blockchain networks and hardware and scalability tools.[11]

7. WALLET *(i.e., FOURwaL)*

With a single purpose, *FOURwaL* serves as a blockchain gateway, a tool for *4thTech* services access. It provides the simplest but secure way to connect via Firefox and Chromium-based browsers to the *4thTech* blockchain applications (i.e., FOURid, FOURdx, FOURns and now FOURim) 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 instant messages.[12]

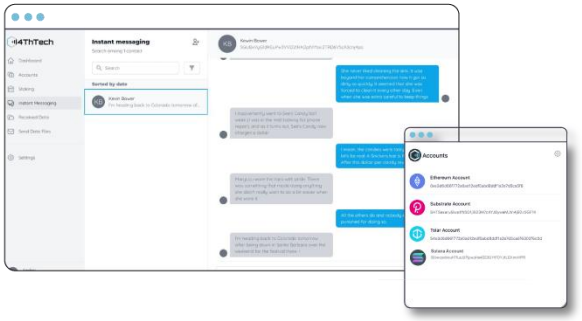
**__Note;__ According to Wiki, a cryptocurrency wallet is a device, program or service which stores the public and/or private keys and can be used to track ownership, receive or spend cryptocurrencies. As all cryptocurrencies run on blockchains, cryptocurrency wallet can be referred also as blockchain wallets. Up to now, blockchain wallet was mostly used for cryptocurrency asset holding and exchange.*[13]

**__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

8. WEB PLATFORM

The *4thTech web 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. The platform combines several services and solutions; (1) *blockchain identity protocol* or short FOURid (status: active); (2) *digital data exchange* or short FOURdx (status: active); (3) *digital data verification* service or short FOURns (status: active); (4) *digital data file encryption service* (status: active); (5) *off-chain database and repository* (status: active); (6) *JSON metadata schema* (status: active); (7) *transaction fee mechanism* (status: partly active, partly in development), and; (8) *Solana blockchain instant messaging service* or short FOURim (status: in development).



9. SMART CONTRACTS

Smart contracts are essentially a code or rules written into a digital program, and were written to facilitate unique requirements such as; (1) saving instant messages from the sender; (2) retrieving instant messages from receivers.

10. DATA REPOSITORY

A database is an organized collection of data, stored and accessed electronically. The *4thTech* system contains three databases; (1) *MySQL database*: storing user encrypted info, platform settings, user wallets, RSA public key for data encryption. MySQL database is protected with a firewall. Data exchanges are protected with an HTTPS connection. In the case of a user request, it is possible to delete any user-related data: (2) *local or cloud file repository*: storing encrypted electronic data files. In the case of a user request, it is possible to delete any user-related data; (3) *blockchain*: encrypted message and timestamp of the send an instant message.

[11] https://www.the4thpillar.io/documents/FOURim-layer-infrastructure.png [accessed 20 May 2021]

[12] https://wiki.the4thpillar.com/guide/discover.html#fourwal [accessed 20 May 2021]

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

11. SYSTEM ARCHITECTURE ADVANTAGES

(1) decentralization; (2) immutability; (3) privacy and security; (4) near to real-time transaction speed, and; (5) extremely low transaction cost

12. FOURim SERVICE FEES

The FOURim *service FEE* is for now solely based on the Solana blockchain network transaction (i.e., TX) cost. One TX is needed to store the encrypted instant message to the smart contract. Tier 3 Staking of FOUR tokens unlocks the FOURim service. The users will be able to unlock the instant wallet to wallet messaging service by locking the FOUR tokens on the *4thTech* Web Platform. No FOUR tokens are spent to activate the service.

13. FOUR STAKING/LOCKING

FOUR_STAKING will be enabled within the platform in the coming update. After choosing the *STAKING/LOCKING* tier 3, the wallet FOUR balance must be sufficient. With a single click, the FOUR funds are staked at a *STAKING_SC* address. As FOUR is an ERC-20 token, an Ethereum *SC_TX* is executed accompanied by Ethereum *TX_FEE*. After the *SC_TX* execution, the funds are staked at the *STAKING_SC* address and the *4thTech* instant messaging service is enabled immediately. After the staking period, the FOUR staked funds can be claimed back.

14. CONCLUSION

Blockchain already establishes its technology and its decentralized advantages. Now it is on us to develop useful use cases such as FOURim, and in our case enable online privacy of data and communication. 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 data file exchange and chat user interface, which manifested itself in the form of a *4thTech* wallet and web platform.

15. 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 Režun; *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.*[14]

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.*

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