

4THPILLAR TECHNOLOGIES (i.e. 4THTECH) MVP Short Paper 1.0

Executive Summary-- Leading to the 4thtech 3rd anniversary, which is on the 10th of October 2020, 4thtech fully-featured advanced MVP (i.e. FOURdx, FOURid, FOURns) is before release. It will provide the rationale and framework needed for further 4thtech cross-platform client development, legislation adoption, cross-chain deployment and recognition.

Dr. Tali Rezun, 4thtech consortium council chair

Keywords: 4thpillar, 4thtech, fourdx, fourid, fourns, four-token, internet, digital transformation, blockchain technology, decentralization, peer-to-peer, online trust, online security, online privacy, DLT, eDelivery, document exchange, notarisatation, 4thtech MVP

1. INTRODUCTION

4thpillar technologies (i.e. 4thtech) implements blockchain-based solutions and facilitates digital transformation for the public and private sector. For three years now we are developing an upgrade to existing European Union eDelivery, Digital Identity and Notarization solutions by providing a blockchain-based alternative.

Blockchain technology proposes the ideal foundation to simplify digital data and documents exchange. To address this issue in 2017, 4thtech, proposed and later developed a safe, fast cross DLT blockchain-based solution, which leverages trust provided by the blockchain and provides secure, immutable, instant cross-border electronic data and document exchange (i.e. FOURdx). To provide an option for blockchain address ownership verification, the identification mechanism (i.e. FOURid) later was constructed in 2018, which can with the help of X.509 Public Key Infrastructure authenticate verified connection between a blockchain wallet and a person. Notarisatation Service (i.e. FOURns) is also an essential part of the 4thtech ecosystem and provides unique digital data or document timestamp and authenticity verification.

2. 4THTECH MVP CURRENT DEVELOPMENT

4thtech MVP developed solutions (i.e. FOURdx, FOURid, FOURns) provide the rationale and framework needed for further 4thtech cross-platform client development, legislation adoption, cross-chain deployment and recognition. The completed fully-featured 4thtech MVP also concludes projects second biggest development mile-stone and paves the way towards the final goal, that is the development and deployment of 4thtech cross-platform client (i.e. Windows, Mac OS, Linux, Android, iOS). As we are closing in on the project's 3rd anniversary, the fully-featured MVP is near completion. The final development is in progress (please check the progress status); (1) MVP smart-contract update with the build-in support for the notarisatation service (done); (2) digital identity mechanism update with the X.509 standard digital certificate compatibility integration (in progress); (3) MVP platform feature update (in progress), and; (4) Additional open-source chain support (in progress).

3. 4THTECH MVP CROSS-CHAIN DEPLOYMENT

With the 3rd-chain deployment, 4thtech MVP establishes its cross-chain presence. Deployed first at Kovan test-net at the beginning of 2018 and later on the Ethereum main-chain proved to be a good decision which provided a reliable 4thtech

eDelivery protocol testing environment. With recent transaction fees increase, Ethereum main-chain becomes unreachable and in overload peaks transaction speed halted to snail speed. 4thtech MVP solutions are using complicated smart contracts that use multiple transactions to execute eDelivery (e.g. on September 1, 2020, one 4thtech eDelivery document exchange on Ethereum chain cost 65,05\$).

The current MVP eDelivery combines two smart contract transactions; (1) first transaction saves the data of the document to the smart contract, and; (2) second transaction sends the transaction fee in FOUR to 4thtech fee-taker address.

1. Transaction one calculation:

$$\text{TX_COST} = \text{GAS_UNITS} * \text{GAS_PRICE}$$

$$\text{TX_COST} = 260.701 * 421 \text{ gwei}$$

$$\text{TX_COST} = 109.755.121 \text{ gwei}$$

$$\text{TX_COST} = 109.755.121 \text{ gwei} * 0,000000001$$

$$\text{TX_COST} = 0,109755121 \text{ ETH}$$

2. Transaction two calculation:

$$\text{TX_COST} = \text{GAS_UNITS} * \text{GAS_PRICE}$$

$$\text{TX_COST} = 75.465 * 421 \text{ gwei}$$

$$\text{TX_COST} = 31.770.765 \text{ gwei}$$

$$\text{TX_COST} = 31.770.765 \text{ gwei} * 0,000000001$$

$$\text{TX_COST} = 0,031770765 \text{ ETH}$$

3. Total eDelivery transaction cost on Ethereum chain (September 1, 2020):

$$0,109755121 \text{ ETH} + 0,031770765 \text{ ETH} = 0,14152 \text{ ETH} (65,05\$)$$

Transaction speed comparison tests (*4thpillar Technologies | Blockchain eDelivery Transaction Test "Ethereum vs. SI-Chain" - YouTube*, n.d.) was executed on both Ethereum and SI-Chain under the same conditions. 4thtech MVP eDelivery transaction on Ethereum took 00:01:06 (i.e. one minute and 6 seconds), the same transaction on SI-Chain took only 00:00:12 (i.e. 12 seconds).

With the aim to upgrade the existing CEF eDelivery (Connecting Europe Facilities main goal is to ensure Public Administrations data and documents exchange at low cost), Ethereum is just not the solution.

To solve the cost and speed challenge, in 2020 4thtech MVP was deployed on SI-Chain, which was established with the support of the Slovenian Ministry of Economic Development and Technology by the innovative technology company HashNet in cooperation with Telemach, a telecommunication solutions provider (*Slovenia launches national test blockchain infrastructure and Slovenian Blockchain partnership | GOV.SI*, n.d.).

The SI-Chain technology facilitates transactions and the creation of smart contracts with the scope; (1) to develop a framework/mechanism for development and implementation of blockchain services infrastructure, which will be compatible and in line with European blockchain services infrastructure and usable or extendable globally, and; (2) To create a study on strategy for development and implementation of interoperable global blockchain technology infrastructure, taking into consideration existing standards for implementation of cross border blockchain infrastructure in an interoperable manner.

Si-Chain is based on HashNet technology, which according to (*Tolar - Hashnet*, n.d.) employs DLT and consensus algorithm that keeps all positive characteristics of blockchain technology while increasing throughput to more than 50,000 transactions per second, what gives us the significant advantage.

To simplify the 4thtech MVP user transaction payments when executing eDelivery, notarisatation service or digital identity verification, all fee payments are processed in 4thtech native FOUR across all chain deployments. This is possible due to FOUR unique features; (1) embedded TTS interface (i.e. token teleportation-service), that enables cross-DLT accounts with the ability to transfer the ERC-20 tokens without having to pay for the native chain transaction fees. Instead, the account pays for token transfer fees in the 4thtech native FOUR, and; (2) MTO (i.e. multiple-transfer option) is a settlement service that conserves blockchain network transactions and bundles signed multiple transactions together and settles them on the blockchain (i.e. as one transaction). (*4THPILLAR TECHNOLOGIES Project White Paper*, n.d.)

As explained later in the interoperability chapter, the easiest solution would be to adopt the single

DLT/Chain standard, as this would be the quickest solution. As the world and the technology are not there yet, the task of 4thtech multi DLT systems deployment stands.

4. 4THTECH MVP SOLUTIONS

After two years of 4thtech MVP testing, the technical feasibility and its practical potential have been proven and the three main solutions crystalized (i.e. FOURdx, FOURid and FOURns). All additional information regarding 4thtech MVP solution testing is available on www.the4thpillar.io.

4.1. 4THTECH MVP BLOCKCHAIN E-DELIVERY PROTOCOL (i.e. FOURdx)

As main 4thtech MVP solution, blockchain eDelivery protocol (i.e. FOURdx) leverage trust provided by the blockchain and provides secure, immutable, instant cross-border electronic data and document exchange. The fully-featured protocol is capable of; (1) connecting senders and recipients by executing blockchain electronic data and documents exchange (i.e. blockchain eDelivery); (2) performing blockchain eDelivery based on the current CEF (i.e. Connecting Europe Facility); (3) archiving securely encrypted data and documents off-chain, and (4) following the EU GDPR guidelines.

Simplifying the process;

- a) available chain SELECTION (currently Ethereum, SI-Chain are available, the third open-source chain support is being implemented);
- b) electronic data and documents UPLOAD to the FOURdx API (current MVP limitation to 20MB file size);
- c) the electronic data and documents STORAGE to the off-chain 4thtech repository (later external repository options will be available);
- d) SENDING link to encrypted files and hashes of the encrypted content through the chosen blockchain to a recipient-specific wallet address, and;
- e) DOWNLOAD and DECRYPTION of the received electronic data. Decryption is done with his/her private key saved in the

browser's FOURwaL (i.e. 4thtech blockchain gateway wallet).

4.2. 4THTECH MVP DIGITAL IDENTITY MECHANISM (i.e. FOURid)

Blockchain digital identity mechanism (i.e. FOURid), derives as a direct result of the existing blockchain eDelivery protocol (i.e. FOURdx). The identity mechanism is capable of individual (or organization) wallet address verification. A link is created between an individual (or organization) and their blockchain wallet within the 4thtech system. The identity mechanism is also capable of; (1) connecting the X.509 standard digital certificate with blockchain wallet; (2) providing the digital identity for blockchain eDelivery (i.e. FOURdx), and; (3) providing digital identity for blockchain Notarisation (i.e. FOURns).

Simplifying the process;

- a) user ACCOUNT CREATION using 4thtech blockchain gateway (i.e. FOURwaL);
- b) DIGITAL CERTIFICATE (i.e. X.509 standard) user KYC PROCESS (i.e. name, surname, identity number, tax number);
- c) digital certificates user identity VERIFICATION CHECK;
- d) LINK creation between the verified user and his/her wallet

Digital certificate X.509 standard;

According to (*Državni center za storitve zaupanja Izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA POLITIKA SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe Javni del notranjih pravil Državnega centra za storitve zaupanja* *Državni center za storitve zaupanja*, n.d.) 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. According to CEFs (*Trusted List Browser*, n.d.), the X509 standard is widely used in European Union and as such appropriate for FOURid integration. The X509 Public Key Infrastructure is also approved by eIDAS (i.e. electronic IDentification, Authentication and Trust Services).

4.3. 4THTECH MVP BLOCKCHAIN NOTARISATION SERVICE (i.e. FOURns)

4thtech notarisation service is a by-product of eDelivery protocol (i.e. FOURdx) and digital identity mechanism (i.e. FOURid) and is able to leverage the power of cross-DLT blockchains to facilitate source and time confirmation for digital data and documents. The 4thtech blockchain notarisation service is also capable of; (1) storing and timestamping a digital data or document; (2) providing the verification of the digital data or document authenticity, and; (3) providing access and review of the notarisation details.

Simplifying the process;

- a) user ACCOUNT CREATION using 4thtech blockchain gateway (i.e. FOURwaL);
- b) user ACCOUNT VERIFICATION using 4thtech digital identity mechanism (i.e. FOURid) which uses established online verifications protocols (i.e. digital certificate standard X.509 Public Key Infrastructure);
- c) digital data or document UPLOAD to the data repository, using eDelivery protocol (i.e. FOURdx), and;
- d) blockchain NOTARISATION TRANSACTION SIGNATURE, using 4thtech blockchain gateway (i.e. FOURwaL).

5. 4THTECH MVP TECHNICAL SPECIFICATIONS

- Blockchain deployment: Ethereum, SI-Chain (i.e. Private Hashnet Chain)
- Blockchain gateway: FOURwaL (i.e. 4thtech Google Chrome add-on wallet)
- Transaction payment: FOUR (i.e. ERC20 token)
- Programming languages:(1) JS (TypeScript) for frontend; (2) PHP for web services; (3) Solidity and JavaScript for smart contracts, and;(4) other.
- Scaling: Docker container technology
- Digital Certificate compatibility: X.509 STANDARD compatible

6. 4THTECH MVP LEGAL, GOVERNANCE AND TECHNICAL INTEROPERABILITY

This chapter discovers aspects of legal, governance and technical interoperability and it is an abstract of UN/CEFACT project presentation in Geneva virtual event from 9th of July 2020. (- *Trade - UNECE*, n.d.)

6.1. 4THTECH MVP LEGAL INTEROPERABILITY

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. GDPR also invokes the right of data erasure, which can be especially tricky when dealing with blockchain-ledger. (*EUR-Lex - 32016R0679 - EN - EUR-Lex*, n.d.)

To achieve legal interoperability, 4thtech solutions are 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 electronic data or document 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 electronic data or documents 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. (*Blockchain eDelivery protocol UN/CEFACT use-case*, n.d.)

6.2. 4THTECH MVP GOVERNANCE INTEROPERABILITY

4thtech solutions are deployed as an application operating currently on Ethereum and SI-Chain networks, with third open-chain deployment coming. As such, the 4thtech solutions transaction governance falls under the DLTs governance of its

deployment. The challenge lies in single and multiple cross-platform DLT governance interoperability and content user control.

4thtech solutions can be deployed on a different DLT chain, so there is only a matter of choosing the chain that will be most compatible and Governance interoperable according to deployment needs. As the protocol uses DLTs only for recording transaction links to encrypted files and hashes of the encrypted content exchanged between sender and the receiver, and the content can be accessed only with the private key, the protocol transaction Governance is completely in the user's hands. (*Blockchain eDelivery protocol UN/CEFACT use-case*, n.d.)

6.3. 4THTECH MVP TECHNICAL INTEROPERABILITY

In the case of technical 4thtech solutions interoperability, the challenge is how to interact between different DLTs and be compatible with-in the Multi-DLT systems.

The easiest solution would be to adopt the single DLT standard, as this would be the quickest solution. As the world and the technology are not there yet, the challenges of 4thtech interoperability between multi DLT systems stand. The 4thtech uses hosted Ethereum node on Infura over JSON-RPC protocol, to connect to the Ethereum node. In the case of SI-Chain, 4thtech uses gRPC (i.e. universal RPC framework) to connect to Si-Chain node. Regarding the DLT and Multi DLT interoperability, the same connection principles with specific modification will apply. (*Blockchain eDelivery protocol UN/CEFACT use-case*, n.d.)

7. 4THTECH MVP FURTHER DEVELOPMENT

4thtech final goal is to release the suite of products in the form of the cross-platform client (i.e. Windows, Mac OS, Linux, Android, iOS) which will be compatible and in line with European Blockchain services infrastructure and usable or extendable globally.

According to (Rezun & Jazbec, n.d.) 4thtech cross-platform client has eight development modules; (1) smart-contact DEV (estimated development time 30 days); (2) JSON metadata schema DEV (estimated development time 10 days); (3)

document repository with notarisation function DEV (estimated development time 60 days) (4) RSA public key repository DEV (estimated development time 15 days); (5) digital identity mechanism DEV (estimated development time 70 days); (6) eDelivery cross-platform desktop client DEV (estimated development time 180 days); (7) eDelivery cross-platform mobile client DEV (estimated development time 180 days); (8) blockchain CEF access point development (estimated development time 140 days), and; (9) SI-Chain implementation (estimated development time 60 days).

The start for cross-platform 4thtech client development is planned in January 2021. According to plan, the project should be finished in 16 months.

References

- Trade - UNECE. (n.d.). Retrieved September 1, 2020, from <https://www.unece.org/uncefact-chain-workshop>
- 4thpillar Technologies | Blockchain eDelivery Transaction Test "Ethereum vs. SI-Chain" - YouTube. (n.d.). Retrieved September 1, 2020, from <https://www.youtube.com/watch?v=rjzO5kV Rpbk&t=1s>
- 4THPILLAR TECHNOLOGIES Project White Paper. (n.d.). Retrieved March 26, 2020, from <https://the4thpillar.io/>
- Blockchain eDelivery protocol UN/CEFACT use-case. (n.d.). Retrieved September 1, 2020, from https://www.unece.org/fileadmin/DAM/cefact/OtherMeetings/2020/Online_Workshop_“Towards_Global_Interoperable_Blockchain_Infrastructure_/S2_P2_Tali_Rezun_PPT.pdf
- Državni center za storitve zaupanja Izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA POLITIKA SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe Javni del notranjih pravil Državnega centra za storitve zaupanja ☒ Državni center za storitve zaupanja. (n.d.).
- EUR-Lex - 32016R0679 - EN - EUR-Lex. (n.d.). Retrieved April 6, 2020, from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Rezun, T., & Jazbec, D. (n.d.). BLOCKCHAIN E-DELIVERY CROSS-PLATFORM CLIENT PROPOSAL. Retrieved April 4, 2020, from <https://the4thpillar.io/>

Slovenia launches national test blockchain infrastructure and Slovenian Blockchain partnership | GOV.SI. (n.d.). Retrieved April 4, 2020, from <https://www.gov.si/en/news/slovenia-launches-national-test-blockchain-infrastructure-and-slovenian-blockchain-partnership/>

Tolar - Hashnet. (n.d.). Retrieved April 29, 2020, from <https://www.tolar.io/hashnet>

Trusted List Browser. (n.d.). Retrieved August 31, 2020, from <https://webgate.ec.europa.eu/tl-browser/#/tl/SI>