4thpillar technologies publications
Research Articles and Guidebooks
Type: Technical paper 1.0
Status - Published
Slovenia, Europe, 2020
https://the4thpillar.io/

BLOCKCHAIN E-DELIVERY CROSS-PLATFORM CLIENT AND CEF ACCESS POINT DEPLOYMENT

TECHNICAL PAPER BY DR. TALI REZUN AND DENIS JAZBEC

***Abstract*--We propose a *blockchain eDelivery cross-platform client*, a DSI (i.e. digital service infrastructure) that will provide electronic data and document exchange with notarisation and digital identity service between users in a reliable, safe and trusted way. Additionally, we aim to develop blockchain CEF (i.e. Connecting Europe Facility) compatible Access Point to leverage trust and direct blockchain connectivity. The proposed DSI is an *eDelivery cross-platform client*, an upgrade to the existing *blockchain eDelivery protocol* (i.e. FOURdx). Blockchain eDelivery has significant security advantages, comparing to traditional eDelivery. It is based on a distributed model where electronic data and documents exchange process runs between blockchain wallets, where private and public cryptographic keys are used for transaction authentication. Existing blockchain eDelivery MVP (i.e. minimum viable product) is capable of; (1) connecting senders and receivers by executing electronic data and document exchange; (2) performing eDelivery based on the current EU guidelines, and; (3) archiving securely encrypted data. After two years of MVP testing, the technical feasibility and its practical potential have been proven, with that, the blockchain cross-platform eDelivery client development is the next logical step.**

Keywords— blockchain, eDelivery, protocol, client, 4thpillar technologies, hashnet, sichain, digital transformation, connecting Europe facility

1. BACKGROUD AND RATIONALE

Exchanging sensitive electronic data, documents or merely digital assets should be as easy as exchanging information. Due to its immutability blockchain technology proposes the ideal foundation to simplify digital value-holding file and documents exchange. To address this issue in 2017, 4thpillar technologies (i.e. 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. To provide an option for blockchain address ownership verification, the identification mechanism later was constructed in 2018, which can authenticate verified connection between a blockchain wallet and a person. Notarisation is also an essential part of the 4thtech eDelivery ecosystem and provides unique digital data or document timestamp and authenticity verification.

The eDelivery protocol has been validated with a working prototype, tested on early adopters and recognised as blockchain development suited for European Union needs.

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.)

After two years of the protocol MVP testing, the technical feasibility and its practical potential have been proven, with that PoC (i.e. proof of concept) was confirmed. As the European Union is embracing the benefits of blockchain technology, now is the time for furthered development of the blockchain eDelivery. We propose the development of the blockchain eDelivery cross-platform (i.e. Windows, Mac OS, Linux, Android, iOS) desktop and mobile client.

1.1 OBJECTIVE

The objective of the project is to develop and deploy *cross-platform (*Windows, macOS, Linux, Android and iOS) *eDelivery client*, a DSI with a unique Access Point, that will leverage blockchain for electronic data and documents exchange in a reliable, safe, trusted way. Also, the blockchain eDelivery client will be deployed and integrated on *Slovenian National Blockchain Test Infrastructure* (i.e. SI-Chain), providing a testing framework for future blockchain eDelivery. This action will support the development of blockchain eDelivery, more specifically it will help build the foundations for safe, reliable cross-border digital eDelivery services between both public and private sectors, as well as between such entities and citizens and organisations.

1.2. SCOPE

The project scope is divided into 9 activities converging to achieve the project objective of development and deployment of; (1) smart contract; (2) JSON metadata schema; (3) electronic data and documents repository with notarisation function; (4) RSA public key repository upgrade; (5) blockchain wallet identity mechanism; (6) desktop cross-platform eDelivery client; (7) mobile cross-platform eDelivery client; (8) blockchain Access Point, and; (9) SI-Chain integration.

1.3. NATIONAL BLOCKCHAIN INFRASTRUCTURE DEPLOYMENT

The proposed action results in development and deployment of *blockchain cross-platform eDelivery* client on Slovenian National Blockchain Test Infrastructure (i.e. SI-Chain, first EU cross-border blockchain infrastructure), providing a testing framework for future safe, reliable cross-border digital eDelivery services between both public and private sectors, as well as between such entities and citizens and organisations. Main private partner, a telecommunication company Telemach will ensure cross-border infrastructure and the needed publicity (*Slovenia launches national test blockchain infrastructure and Slovenian Blockchain partnership | GOV.SI*, n.d.). The project with its use cases will be promoted on a national, EU events and conferences in collaboration with European blockchain partnership and also within the UNECE Chain project (*UNECE Chain project*, n.d.)

1.4. PROJECT VALUE

Main project value derived from; (1) establishment of blockchain eDelivery testing framework, what can lead to digital transformation and further enable digital trust; (2) the development contribution to the current and future DLT research, as there is a lack of distributed application use cases on the market, and (3); blockchain eDelivery has significant security advantages, comparing to traditional eDelivery, as it is a network of nodes for digital communications and electronic data and documents exchange and it is based on a decentralised model where files exchange process runs between blockchain wallets and private and public cryptographic keys are used for transaction authentication.

1.5. CEF INTEGRATION

To fully implement the blockchain eDelivery concept and, to make it compliant with the DSI and policy objectives, the development of unique Access Point is needed. The current CEF eDelivery solution is based on a model, where the Access Points of eDelivery implement an electronic data and documents exchange protocol, which ensures secure and reliable data exchange. Trust is established between two public administrations' Access Points and the electronic data and documents exchange is activated. We propose the development of a new Access Point, where trust will be provided by the blockchain. The new Access Point will behave in a similar way that current CEF Access Point but with the main difference of interacting directly with the blockchain. In this case, there is no need for interacting with receiver Access Point. Also, there will be some differences in regarding the Access Point, SML, and SMP interacting because electronic data and documents are transmitted to the receivers Access Point over the blockchain and not over the internet, where different data is used to determine the receiver identity.

1.6. BUILDING ON PRE-EXISTING WORK

Blockchain eDelivery has significant advantages, comparing to traditional eDelivery. It is based on a distributed model where the electronic data and documents exchange process runs between blockchain wallets, where private and public cryptographic keys are used for transaction authentication. Our existing *blockchain eDelivery protocol* is capable of; (1) connecting senders and receivers by executing electronic data and documents exchange; (2) performing eDelivery and notarisation based on the current EU guidelines; (3) archiving securely encrypted data, and (4) following the GDPR guidelines. The innovation and ingenuity reveal from the fact, that the protocol does not store the transmitted electronic data and documents on the blockchain. The electronic data and documents are 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 and privacy. Designed and built completely by the *4thpillar technologies*, the protocol is fully operational, ready for testing and provides the core technology solutions for further development of the proposed *blockchain eDelivery cross-platform client.*

2. THE STORY BEHIND THE 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.

2.1. CONSORTIUM

Supported and approved by Slovenian Ministry of Public Administration, the consortium was formed between *4thpillar technologies* and HashNET, to enter the INEA (i.e. European Commission Innovation and Networks Executive Agency) 2020 CEF Telecom Call - eDelivery (CEF-TC-2020-1). The consortium will present the *blockchain eDelivery cross-platform (i.e. Windows, Mac OS, Linux, Android, iOS) client* development blueprint. If funded, the new cross-platform eDelivery client can reach BETA by the end of 2021 and be integrated into Si-Chain national test blockchain infrastructure. As the core technology (i.e. *Hashnet* and *blockchain eDelivery protocol*) is developed and owned by companies forming the consortium, the contribution to this action applies. Both consortium members perfectly align, as *blockchain eDelivery protocol* needs a blockchain network to run on, and a blockchain network needs applications, so a valuable product is formed.

3. TECHNOLOGY EXPLAINERS

Due to complexity of industry terminology, we have prepared technology and terms explainers for terms; (1) blockchain; (2) eDelivery; (3) blockchain eDelivery; (4) blockchain wallet; (5) hardware wallet (6) RSA and AES encryption, and (7) SHA 256.

3.1. BLOCKCHAIN

Blockchain provides a decentralized and immutable 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. (*4THPILLAR TECHNOLOGIES Project White Paper*, n.d.)

3.2. E-DELIVERY

According to *Connecting Europe: CEF eDelivery supports trans-European multilingualism*, n.d., eDelivery is a network of nodes for digital communications. It is based on a distributed model where every participant becomes a node using standard transport protocols and security policies. eDelivery helps public administrations to exchange electronic data and documents with other public administrations, businesses, and citizens, in an interoperable, secure, reliable and trusted way. It is one of the building blocks of the Connecting Europe Facility. These building blocks are reusable specifications, software, and services that will form part of a wide variety of IT systems in different policy domains of the European Union.

3.3. BLOCKCHAIN E-DELIVERY

According to *4THPILLAR TECHNOLOGIES Project White Paper*, n.d., blockchain eDelivery is a network of nodes for digital communications and document or files exchange. It is based on a decentralised model where files exchange process runs between blockchain wallets. Private and public cryptographic keys are used for transaction authentication. Blockchain eDelivery has significant security advantages, comparing to traditional eDelivery. Blockchain eDelivery (i.e. FOURdx) is a developed and tested protocol capable of; (1) connecting senders and receivers by executing electronic data and documents exchange; (2) performing eDelivery based on the current EU guidelines, and; (3) archiving securely encrypted data.

3.4. BLOCKCHAIN NOTARISATION

4thtech notarisation service is able to leverage the power of cross DLT blockchains and facilitate source and time confirmation for digital data and documents. The notarisation function will be soon available for testing as a part of the blockchain eDelivery protocol and will later be an integrated function of 4thtech eDelivery cross-platform client with main functions; (1) store and timestamp a digital data or document; (2) verify the digital data or document authenticity, and; (3) access and review the notarisation details.

3.5. BLOCKCHAIN WALLET

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 wallet can be referred also as blockchain wallets. Up to now, blockchain wallet was mostly used for cryptocurrency asset holding and exchange. The *4thtech add-on* is a Google Chrome extension wallet, that allows you to visit the distributed web of tomorrow in your browser today. It is one of the *4thpillar technologies* main innovations, a first system on the market capable of handling not only digital assets but also other assets such as links to encrypted electronic data and documents. Designed and build from the ground-up, the *4thtech add-on* is fully operational and, also offers a secure identity vault, providing a user interface to manage digital identities and sign blockchain eDelivery transactions. *4thtech add-on* can be comparable to a bank account, as it contains a pair of public and private cryptographic keys. A public key allows for other wallets to execute eDelivery to the desired wallet's address, whereas a private key enables the decryption of electronic data and documents from that address.

3.6. HARDWARE WALLET

Hardware wallet provides additional security and private key backup. According to *Hardware Wallets Explained - Mycryptopedia*, n.d., a hardware wallet is a physical electronic device that is designed to protect an individual's crypto assets by securing their private keys. The idea behind hardware wallets is to isolate the private keys from online methods of storage, such as a computer or smartphone, which are more susceptible to being compromised by a hacker. Storing your private keys offline prevents against this, as hackers would have to physically steal your hardware wallet to gain access to a user's private keys. *4thpillar technologies* have partnered with HI-WISE project, an advanced plug&play hardware wallet with futuristic uni-body design. Unique to the market, the HI-WISE has no openings and buttons, just a HI definition LCD and it is powered by Qi charging technology. Accompanied by unique mobile multi-wallet with unparalleled safety features and integrated anti-spying algorithms. Hardware Wallet option will be supported in future cross-platform desktop client updates.

3.7. RSA AND AES ENCRYPTION

According to *RSA (cryptosystem) - Wikipedia*, n.d., RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". *Blockchain eDelivery protocol* (i.e. FOURdx) uses the advanced encryption standard (i.e. AES), with a combination of RSA encryption algorithms. The electronic data and documents are encrypted with a symmetric algorithm (i.e. AES), as the asymmetric algorithm (i.e. RSA) is used to encrypt symmetric key and initialization vector (i.e. IV) with the public key of the receiver. This design does not allow an attacker to infer relationships between segments of the encrypted message.

3.8. SECURE HASH ALGORITHM 256 [SHA 256]

According to *What is Secure Hash Algorithm 256? Get the definition here.*, n.d., Secure Hash Algorithm 256 or 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. The same author points out, that a hash is as a mathematical computer process that takes information and turns it into letters and numbers of a certain length. Hashing is used to make storing and finding information quicker because hashes are usually shorter and easier to find. Hashes also make information unreadable and so the original data can become confidential.

3.9. HASH ALGORITHM DOCUMENT OR FILE AUTHENTICITY FEATURE

As explained by *What Is a Checksum (and Why Should You Care)?*, n.d., if you know the checksum (i.e. hash) of the original file, you can run a checksum or hashing utility on it. If the resulting checksum matches, you know the file you have is identical. Identical content of electronic data and documents produces identical hash. If only one symbol in the electronic data or documents is changed, the hash of the changed file is completely different. In the case of *blockchain eDelivery protocol* (i.e. FOURdx), this unique hash functionality enables the authenticity verification of the send electronic data and documents. It provides a way to scan for corrupted or virus-infected electronic data or documents, during digital data exchange. Most importantly, the sender cannot later claim to have sent a different electronic data or documents, as this can be proven using a smart contract by recalculating the hash and comparing it with the data on the blockchain.

4. BLOCKCHAIN EDELIVERY CROSS-PLATFORM CLIENT

Based on our MVP, we plan the furthered development of *blockchain eDelivery cross-platform* (i.e. Windows, Mac OS, Linux, Android, iOS), *desktop and mobile client*, with the following modules; (1) smart contract; (2) JSON metadata schema; (3) electronic data and documents repository with notarisation function; (4) RSA public key repository; (5) blockchain wallet identity mechanism; (6) cross-platform eDelivery desktop client, and; (7) mobile cross-platform eDelivery client.

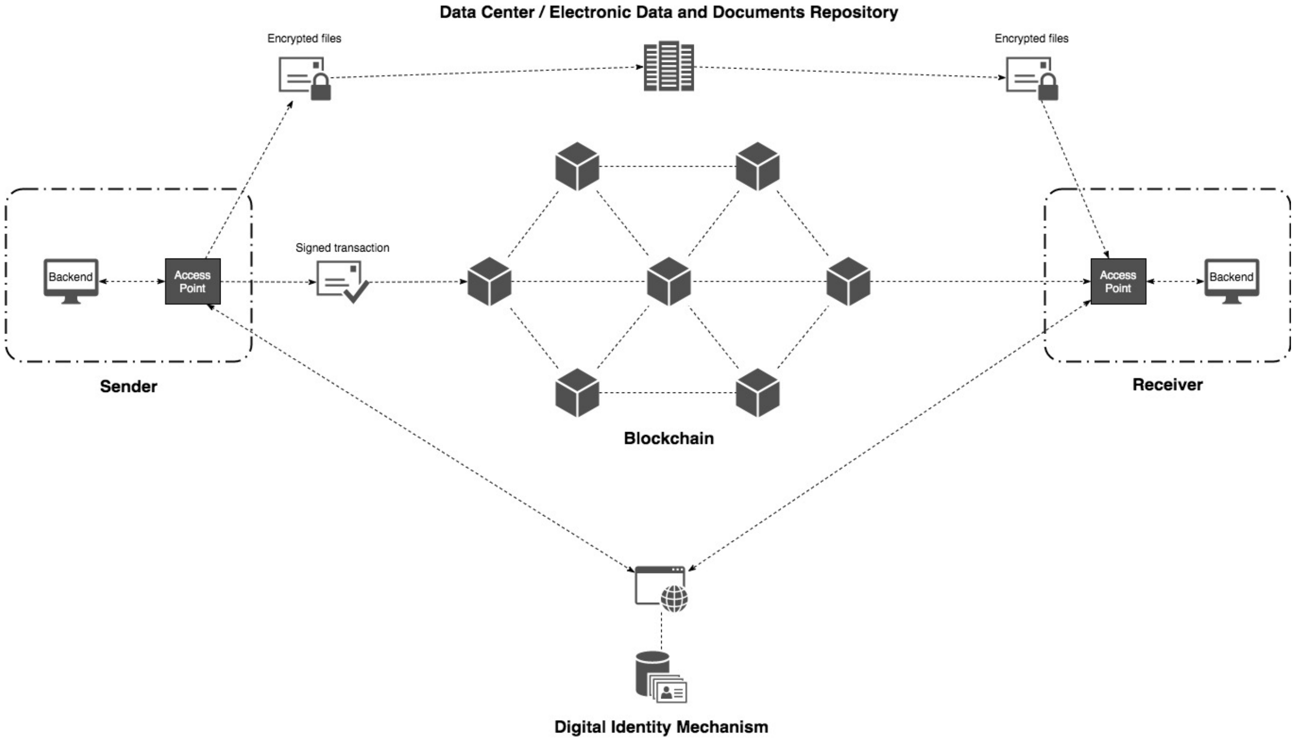

Diagram 1. Blockchain eDelivery cross-platform client ecosystem

4.1. SMART CONTRACTS

Introduction-- A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible. (*Smart contract - Wikipedia*, n.d.)

Current Solution-- Smart contacts are currently used to exchange and manage specific transactions; (1) sender wallet address; (2) sender name and description; (3) document or file type; (4) document or file link, and; (5) document delivery data.

Proposed Solution-- The new upgradeable smart contract will have to be developed, that could record and manage the following; (1) sender wallet address; (2) metadata link; (3) metadata hash (i.e. SHA-256); (4) document delivery data, and; (5) smart contract upgrade. As blockchains are in nature immutable, proper innovation and techniques will have to be used to achieve this action.

Development Plan-- We propose the following smart contract development plan; (1) development specification; (2) smart contract programming; (3) testing, and (4) smart contract chain deployment.

Solution Design-- The smart contract is written in Solidity using Ganache. Ganache is a personal blockchain for Ethereum development you can use to deploy contracts, develop your applications, and run tests.

4.2. JSON METADATA SCHEMA

Introduction-- JSON stands for "JavaScript Object Notation", a simple data interchange format. It began as a notation for the worldwide web. Since JavaScript exists in most web browsers, and JSON is based on JavaScript, it's very easy to support there. However, it has proven useful enough and simple enough that it is now used in many other contexts that don't involve web surfing. JSON Schema itself is written in JSON. It is data itself, not a computer program. It's just a declarative format for "describing the structure of other data". This is both its strength and its weakness (which it shares with other similar schema languages). It is easy to concisely describe the surface structure of data and automate validating data against it. However, since a JSON Schema can't contain arbitrary code, there are certain constraints on the relationships between data elements that can't be expressed. Any "validation tool" for a sufficiently complex data format, therefore, will likely have two phases of validation: one at the schema (or structural) level, and one at the semantic level. (*What is a schema? — Understanding JSON Schema 7.0 documentation*, n.d.)

Proposed Solution-- We propose the following JSON file data structure development, that includes; (1) sender title; (2) subject; (3) content; (4) link to the document or file (i.e. a link to an encrypted ZIP file), and; (5) calculated hash file value.

Development Plan-- We propose the following JSON file data structure development plan; (1) development specification; (2) JSON file data structure programming; (3) deployment, and; (4) testing.

Solution Design-- JSON schema is written in JSON format. In addition to the JSON scheme, we will prepare a simple documentation page with a validator. The page will be written in HTML, JS and CSS (SCSS).

The exact JSON metadata structure will be defined later and will update according to product updates.

4.3. DATA AND DOCUMENTS REPOSITORY WITH NOTARISTION FUNCTION

Introduction-- A database repository is an organized collection of data, stored and accessed electronically (*4THPILLAR TECHNOLOGIES Project White Paper*, n.d.). According to *Data Management for Data Protection (GDPR) | CC CDQ*, n.d. , as the data is processed, the service should be able to delete personal data or sensitive documentation on demand and cope with various retention requirements.

Proposed Solution-- We aim to develop a system that will offer the sender to host their encrypted sent electronic data and documents also on the data repository of *4thpillar technologies*, additionally notarisation service will be able to leverage the power of cross DLT blockchains and facilitate source and time confirmation for digital data and documents.

Development Plan-- We propose the following electronic data repository development plan; (1) development specification; (2) repository programming; (3) deployment, and; (4) testing.

Solution Design-- The backend will be written in PHP with MySQL database. For a better experience on the frontend, we will use Vue JS.

4.4. RSA PUBLIC KEY REPOSITORY UPGRADE

Introduction-- According to *RSA (cryptosystem) - Wikipedia*, n.d., RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem".

Current Solution-- The current *blockchain eDelivery protocol* uses the advanced encryption standard (i.e. AES), with a combination of RSA encryption algorithms. The electronic data and documents are first encrypted with a symmetric algorithm (i.e. AES). The asymmetric algorithm (i.e. RSA) is used to encrypt random symmetric key and initialization vector (i.e. IV) with the public key of the receiver. This design does not allow an attacker to infer relationships between segments of the encrypted message. To encrypt electronic data and documents, the public RSA key of the receiver is needed. In the current *blockchain eDelivery protocol*, the platform solves this issue by recording the public key of every wallet in the *4thtech add-on* domain.

Proposed Solution-- At this stage, we propose an upgrade to the existing solution, by separating the of RSA public key repository and platform.

Development Plan-- We propose the following RSA public key repository development plan; (1) development specification; (2) upgrade programing; (3) deployment, and; (4) testing.

Solution Design-- The backend of our repository API will be written in PHP with MySQL database.

4.5. DIGITAL IDENTITY MECHANISM

Introduction-- There 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. These identities could be based on one or more indicators, which could include, for example, employer identity confirmation, past transaction histories, biometric data and more.

Current Solution-- The current *blockchain eDelivery identity mechanism* (i.e. FOURid), derives as a direct result of the existing *blockchain eDelivery protocol* (i.e. FOURdx). It offers the establishment of blockchain-based individual digital identity and allows user wallets (i.e. including wallet address) to become verified, authenticated and seen in the vastness that is blockchain. A link is created between an individual (or organization) and their wallet, which holds the content and digital assets. Designed and build from the ground-up as a web application with web API, the current solution is fully operational and offers; (1) user on-boarding authorization through a KYC identification process; (2) receiver public RSA key storage; (3) verified connection between the user and his or hers blockchain wallet. (*4THPILLAR TECHNOLOGIES Project White Paper*, n.d.)

Proposed Solution-- We propose the upgrade the existing identity mechanism, focusing at identity verification between organization and individual (e.g. the state and the citizens, schools and students, etc.), to enable the following identity verification mechanism; (1) fulfilment of the digital identity request form by the individual results in wallet creation by the eDelivery client; (2) the individual identification (i.e. KYC) is conducted using either personal identification, video call or some other already established method; (3) unique KYC verification code is issued by the organization; (4) digital identity encrypted verification data package is sent by the organization, through the smart contract to the receiver; (5) the verification data package is received and decrypted by the individual/receiver inside the eDelivery client; (6) the identity data package is confirmed by the individual by imputing the unique KYC verification code in the system; (7) upon the system data verification, the individual identity is confirmed.

Development Plan-- We propose the following identity mechanism development plan; (1) development specification; (2) identity mechanism programming; (3) deployment and; (4) testing.

Solution Design-- The backend will be written in PHP with MySQL database. For a better experience on fthe rontend, we will use Vue JS.

4.6. ELECTRONIC DATA AND DOCUMENTS SENDING PROTOCOL

We plan to develop following electronic data and documents sending protocol; (1) metadata preparation according to valid JSON scheme; (2) encryption of metadata; (3) file upload to the data repository (i.e. a file containing metadata + ZIP file containing documents or files); (4) the calculation of the file content hash (i.e. SHA-256 algorithm is used to calculate the hash value), and; (5) the execution of blockchain transaction, via smart contract.

4.7. BLOCKCHAIN EDELIVERY DESKTOP CLIENT

Introduction-- The proposed DSI is a *blockchain eDelivery cross-platform client*, an upgrade to the existing *blockchain eDelivery protocol.* The existing protocol is fully operational, ready for testing and provides the core technology solutions for further development of the proposed blockchain *eDelivery cross-platform client*.

Current Solution-- Existing *blockchain eDelivery protocol* is capable of; (1) connecting senders and receivers by executing electronic data and documents exchange; (2) performing eDelivery based on the current EU guidelines; (3) archiving securely encrypted data, and (4) following the GDPR guidelines. The innovation and ingenuity reveal from the fact, that the protocol does not store the transmitted electronic data and documents on the blockchain. The electronic data and documents are 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 and privacy. Designed and built completely by the *4thpillar technologies*, the protocol is fully operational, ready for testing and provides the core technology solutions for further development of the proposed *blockchain eDelivery cross-platform client*.

Test Current Solution-- To test current *blockchain eDelivery protocol* (i.e. FOURdx), please follow the video tutorial link (https://youtu.be/uB_uZtZMBUA) or download our Google Chrome add-on and follow the instructions from the product page (i.e. https://the4thpillar.io/products/)

Proposed Solution-- We plan the furthered development of *blockchain eDelivery cross-platform* (i.e. Windows, Mac OS, Linux), *desktop client*, with the following modules; (1) electronic data and documents encryption; (2) desktop wallet interface; (3) desktop wallet interface backup mechanism; (4) electronic data and documents exchange; (5) electronic data and documents repository location option; (6) transaction fee module, and; (7) account settings module.

4.7.1. ELECTRONIC DATA AND DOCUMENTS ENCRYPTION/DESKTOP CLIENT

Introduction-- Electronic data and documents encryption is the process by which electronic data and documents are protected with a cryptographic key (i.e. public key) so that only individuals with the corresponding decryption key (i.e. private key) can read them. (*4THPILLAR TECHNOLOGIES Project White Paper*, n.d.)

Proposed Solution-- We propose to develop the following electronic data and documents encryption solution; (1) the electronic data and documents compression (i.e. zip, gzip); (2) symmetric algorithm encryption of the compressed file (i.e. AES); (3) asymmetric algorithm (i.e. RSA) encryption of the symmetric key and initialization vector (i.e. IV) with the public key of the receiver, and; (4) the merger of asymmetrically encrypted content with symmetrically encrypted content. This design does not allow an attacker to infer relationships between segments of the encrypted message.

**Applies also for mobile client*

4.7.2. DESKTOP WALLET INTERFACE/DESKTOP CLIENT

Proposed Solution-- We aim to develop the cross-platform client wallet as the main front-end user environment with features such as; (1) guided user onboarding (i.e. a collection of basic user data and password definition); (2) wallet access backup options; (a) wallet access file backup; (b) backup using biometric data (i.e. fingerprint scan and facial recognition), and; (3) private keys storage repository (i.e. private keys are stored encrypted on the user device)

**Applies also for mobile client*

4.7.3. DESKTOP WALLET INTERFACE BECKUP MECHANISM/DESKTOP CLIENT

Introduction-- The aspect of blockchain private key security is of most importance. The private key of the must be managed and kept secure since there is no centralized management system behind it. If a user loses their private key, all assets related to that key are lost as well, unless a way to recover that key has been put in place. (*Economic Commission for Europe Executive Committee Centre for Trade Facilitation and Electronic Business Blockchain in Trade Facilitation: Sectoral challenges and examples*, 2019)

Proposed Solution-- We plan to develop the private-key backup system, using biometric data (i.e. fingerprint scan and facial recognition). As biometric sensors are more evolved on mobile devices, this backup option will be included in eDelivery mobile client. The desktop and mobile client wallets will synchronize data, such as biometric keys and similar.

**Applies also for mobile client*

4.7.4. ELECTRONIC DATA AND DOCUMENTS EXCHANGE INTERFACE/DESKTOP CLIENT

Introduction-- The secure blockchain electronic data and documents exchange is the main feature of the proposed *cross-platform eDelivery client.*

Proposed Solution-- We propose the development of similar to email inbox design, but with specific features and solutions, such as; (1) electronic data and documents sending and receiving option; (2) electronic data and documents attachment option; (3) electronic data and documents metadata sending, receiving and reading capability, and; (4) electronic data and documents folder analytics. The proposed *eDelivery client electronic data and documents exchange client* will not store the transmitted data on the blockchain. The electronic data and documents are 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 and privacy.

**Applies also for mobile client*

4.7.5. ELECTRONIC DATA AND DOCUMENTS REPOSITORY LOCATION OPTION/DESKTOP CLIENT

Proposed Solution-- We propose the system, that will provide a choice of the electronic data and documents repository location with full control on the side of the sender and the side of the receiver. We the following repository location options; (1) using the servers owned by user organisation; (2) using repository online services (i.e. Google Drive, Dropbox); (3) using *4thpillar technologies* database repository, and; (4) other.

**Applies also for mobile client*

4.6.6. TRANSACTION FEE/DESKTOP CLIENT

Proposed Solution-- We propose the development of multiple transaction fees options; (1) transaction fee calculated based on a payment plan; (2) transaction fee calculated based on token payment, and; (3) other custom transaction payment option.

**Applies also for mobile client*

4.7.7. ACCOUNT SETTINGS/DESKTOP CLIENT

Proposed Solution-- We propose the development of the following user account settings; (1) dashboard with account overview; (2) backup option; (3) account analytics; (4) transaction payment options, and; (5) blockchain choice setting options.

**Applies also for mobile client*

4.7.8. CLIENT SETTINGS/DESKTOP CLIENT

Proposed Solution-- We propose the development of the following client settings; (1) setting for desktop client document and files archive backup will be possible also using Google drive or similar; (2) desktop client language setting will be available, and; (3) notifications setting options will be provided.

**Applies also for mobile client*

4.7.9. GENERAL SETTINGS/DESKTOP CLIENT

Proposed Solution**--** We propose the development of the following client general settings; (1) received files will be saved on the computer where the desktop client is installed, and; (2) in the case of desktop client removal, the access to the wallet needs to be restored from backup (i.e. the documents or files must be restored as well).

**Applies also for mobile client*

Blockchain eDelivery desktop client Solution Design**--** Blockchain eDelivery desktop client will be built with Electron. Electron is a framework for creating native applications with web technologies like JavaScript, HTML, and CSS.

5. BLOCKCHAIN EDELIVERY MOBILE CLIENT

Proposed Solution**--** Based on the presented desktop client, we propose the development the *blockchain eDelivery mobile client*, for Android and iOS. The mobile client will include most features of a desktop client, with the addition of biometric backup and verification options, as mobile devices support superior biometric sensors compared to desktop computers (i.e. fingerprint scanner and face recognition). Mobile client main functions will be; (1) electronic data and documents encryption; (2) electronic data and documents exchange; (3) external electronic data and documents repository (i.e. *Google drive, Dropbox*, *4thpillar technologies* data repository), and; (4) settings options.

Development Plan**--** We propose the following blockchain eDelivery mobile client development plan; (1) development specification; (2) programing; (3) testing, and (4) deployment on *Google Play* and *Apple Store*.

Solution Design**--** Blockchain eDelivery mobile client will be built with NativeScript. NativeScript is an open-source framework to develop apps on the Apple iOS and Android platforms.

6. VARIOUS BLOCKCHAIN CONNECTION OPTION

As different blockchains are built to serve specific purpose and industry, an option of choice is a must. The eDelivery client will natively work on *Ethereum* blockchain and its fork versions. According to *What is Ethereum? | Ethereum.org*, n.d. , the Ethereum community is the largest and most active blockchain community in the world. It includes core protocol developers, crypto-economic researchers, mining organizations, ETH holders, app developers, ordinary users, fortune 500 companies, and, as of 2018 also *4thpillar technologies* products.

The second blockchain eDelivery protocol (i.e. FOURdx) implementation is currently underway on the Slovenian National Blockchain Testing Infrastructure called SI-Chain, which will enable testing of existing and new blockchain applications for the public and private sector. SI-Chain was established by the innovative technology provider company Hashnet in cooperation with Telemach, the telecommunication solutions provider, in November 2019 (*Slovenia launches national test blockchain infrastructure and Slovenian Blockchain partnership | GOV.SI*, n.d.). HashNet is an innovative consensus platform which provides a novel solution to computational and communicational difficulties of maintaining large-size public distributed ledgers. (*Tolar - Next-gen cryptocurrency*, n.d.)

Other *blockchain eDelivery protocol* implementations will follow, as the demand increases.

7. BLOCKCHAIN CEF ACCESS POINT

Introduction**--** To fully implement the blockchain eDelivery concept and, to make it compliant with the DSI of CEF and its policy objectives, it is subjected to its Access Point development.

Current Solution**--** The current CEF eDelivery solution is based on a model, where the Access Points of eDelivery implement an electronic data and documents exchange protocol which ensures secure and reliable data exchange. Trust is established between two public administrations' Access Points and the electronic data and documents exchange is activated.

Proposed Solution-- We plan the development and deployment of a new Access Point, where trust will be provided by the blockchain. The new Access Point will behave in a similar way that current CEF Access Point but with the main difference of interacting directly with the blockchain. In this case, there is no need for interacting with receiver Access Point. Also, there will be some differences in the case of the Access Point, SML, and SMP interacting because electronic data and documents are transmitted to receiver Access Point over blockchain, not over the internet and different data is used to determine the receiver.

Development Plan-- We propose the following Access Point development and deployment plan; (1) development specification; (2) wallet and blockchain connection programing; (3) webservice programing; (4) deployment and; (5) testing

Solution Design-- Access point will be written in Java.

8. DEVELOPMENT TIMELINE

Blockchain eDelivery cross-platform client has 8 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 development is planned in January 2021. According to plan, the project should be finished in 16 months.

7. CONCLUSION

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, peer-to-peer communication and simplification, it evolved into a system of global intermediaries, that manipulate our private data. Blockchain technology was by now recognised as the technology with high potential to restore online trust and enable final steps toward digital transformation. The system of digital secure sensitive electronic data exchange is needed. We propose blockchain, eDelivery as a valuable electronic data and documents exchange option.

REFERENCES

4THPILLAR TECHNOLOGIES Project White Paper. (n.d.). Retrieved March 26, 2020, from https://the4thpillar.io/

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/

Connecting Europe: CEF eDelivery supports trans-European multilingualism. (n.d.). Retrieved March 8, 2020, from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/04/04/Connecting+Europe%3A+CEF+eDelivery+supports+trans-European+multilingualism

Cryptocurrency wallet - Wikipedia. (n.d.). Retrieved March 7, 2020, from https://en.wikipedia.org/wiki/Cryptocurrency_wallet

Data Management for Data Protection (GDPR) | CC CDQ. (n.d.). Retrieved March 8, 2020, from https://www.cc-cdq.ch/data-management-for-data-protection-gdpr

Economic Commission for Europe Executive Committee Centre for Trade Facilitation and Electronic Business Blockchain in Trade Facilitation: Sectoral challenges and examples. (2019).

Hardware Wallets Explained - Mycryptopedia. (n.d.). Retrieved March 29, 2020, from https://www.mycryptopedia.com/a-look-at-hardware-wallets/

RSA (cryptosystem) - Wikipedia. (n.d.). Retrieved March 27, 2020, from https://en.wikipedia.org/wiki/RSA_(cryptosystem)

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/

Smart contract - Wikipedia. (n.d.). Retrieved March 25, 2020, from https://en.wikipedia.org/wiki/Smart_contract

Tolar - Next-gen cryptocurrency. (n.d.). Retrieved March 28, 2020, from https://www.tolar.io/

UNECE Chain project. (n.d.). Retrieved April 29, 2020, from https://uncefact.unece.org/pages/viewpage.action?pageId=57016392

What Is a Checksum (and Why Should You Care)? (n.d.). Retrieved March 31, 2020, from https://www.howtogeek.com/363735/what-is-a-checksum-and-why-should-you-care/

What is a schema? — Understanding JSON Schema 7.0 documentation. (n.d.). Retrieved March 26, 2020, from https://json-schema.org/understanding-json-schema/about.html

What is Ethereum? | Ethereum.org. (n.d.). Retrieved March 28, 2020, from https://ethereum.org/what-is-ethereum/

What is Secure Hash Algorithm 256? Get the definition here. (n.d.). Retrieved March 28, 2020, from https://decryptionary.com/dictionary/secure-hash-algorithm-256/

BIOS

Dr. **Tali Rezun** is 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. Rezun specializes in online brand awareness, web application development and blockchain technology. He enjoys the title of lecturer, advisor and UN/CEFACT expert. More information about Dr. Tali Rezun: https://talirezun.com/

Denis Jazbec is a software engineer with more a decade of experience and a computer science degree. For the past 3 years, he has been researching blockchain eDelivery protocols and their integration into existing IT systems. He is highly proficient in PHP, JS and MySQL. His focus remains set on quality and secure, fast final products. In the 4thpillar technologies, he holds the title of chief technology officer. Currently, Denis works on a FOURdx cross-platform development.