A new way of exchanging information: verifiable credentials in a decentralized context

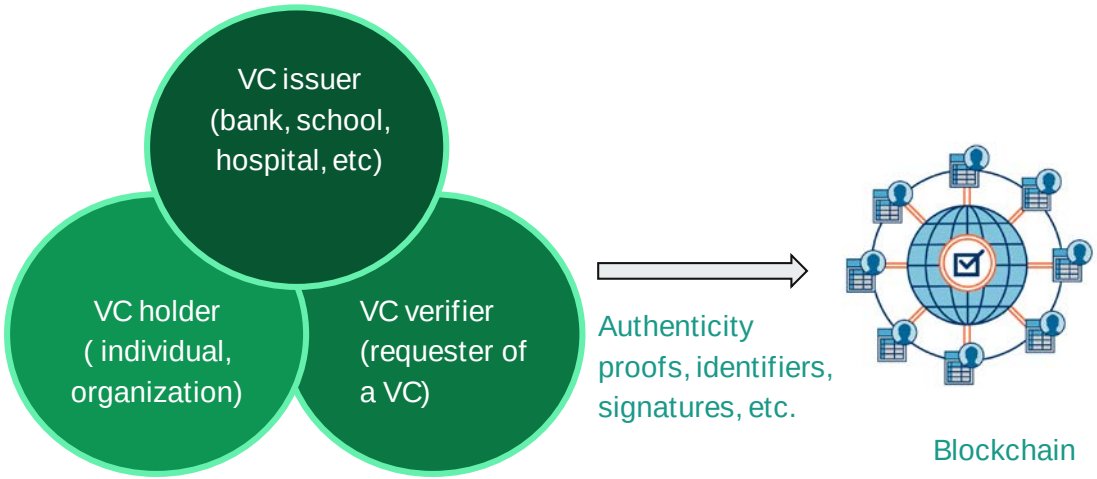
Iraklis Varlamis
GRNET, Director for Digital Governance
Associate Professor, Harokopio University of Athens
varlamis@admin.grnet.gr

Digital signatures

- Digital signatures/stamps are used to verify the authenticity and integrity of electronic documents, including any evidence issued by and exchanged between public authorities.
- A digital signature is created using a cryptographic algorithm that binds the signer's identity to the document, ensuring that it has not been altered or tampered with.
- A single authority can ensure that VCs are issued only to individuals who meet specific criteria, such as completing a degree, paying their taxes, owning a passport, a driving licensing, or a social security card.
- However, relying on a single authority for issuing and verifying evidences can create a single point of failure and reduce transparency.

Verifiable Credentials (VCs)

- Digital alternatives to physical documents
- Digital certificates that provide proof of identity, qualifications, or other attributes.
- They contain metadata, a declaration of the data nature, a proof of the authenticator



Advantages of Verifiable Credentials

- They can be issued, stored, and shared securely on a blockchain network.
- They can be verified instantly, without the need for a central authority or intermediary.
- They enable individuals to maintain control over their personal data and share it selectively with trusted parties.
- VCs have the potential to revolutionize the way credentials are managed, verified, and shared in various industries, such as education, healthcare, and finance.

The role of blockchain

- In a centralized approach, a single central authority issues and signs VCs, which can create a single point of failure and reduce transparency.
- In a centralized approach, individuals may have to rely on the central authority to verify their VCs, which can lead to delays and errors.

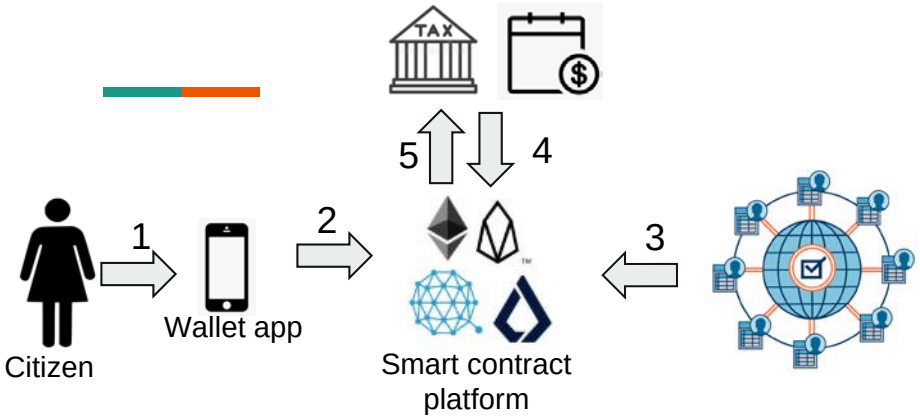
- In a blockchain-based approach, VCs can be issued and signed by multiple parties in a decentralized network, enhancing security and transparency.
- In a blockchain-based approach, VCs can be verified instantly and automatically by anyone on the network, without the need for a central authority or intermediary.
- VCs can be issued directly to individuals, who keep the ownership and decide with whom to share

By using a blockchain-based approach for VCs, organizations can reduce the risk of fraud, increase efficiency, and enhance security and transparency in the credentialing process, while also providing individuals with greater control over their personal data.

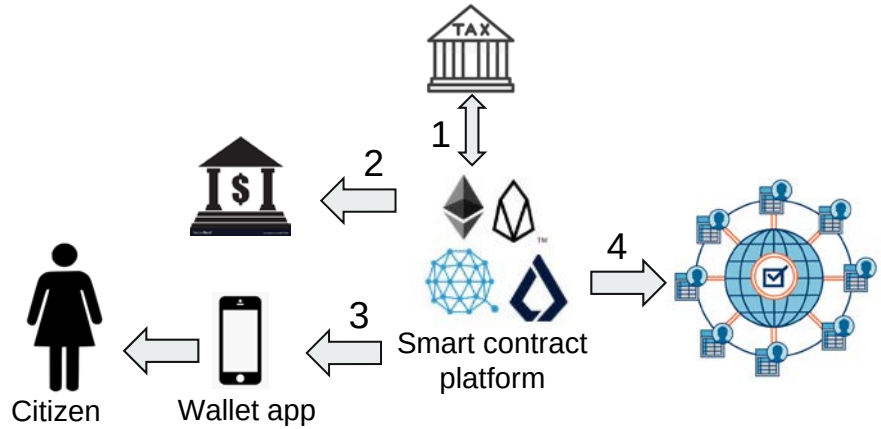
The role of smart contracts

- Smart contracts are self-executing programs that can automate the issuance and verification of VCs.
- They can enforce the rules and conditions of a VC agreement between parties, reducing the risk of fraud or errors.
- Smart contracts can ensure that VCs are only issued to individuals who meet specific criteria, for getting a degree or a tax reduction.
- They can also facilitate the sharing and verification of VCs across different organizations, without the need for a central authority.
- By using smart contracts to deliver VCs, organizations can streamline the credentialing process, reduce costs, and enhance security and transparency.

Example - Tax filing



1. Log in the mobile app
2. Connect to a smart contract platform that automates the tax filing process.
3. Retrieve tax-related VC from the blockchain and initiate a tax filing process using the tax agency's rules and regulations.
4. Verify VC against external data sources (employer's payroll, tax agency's databases).
5. The smart contract platform generates a tax return for the tax agency to review

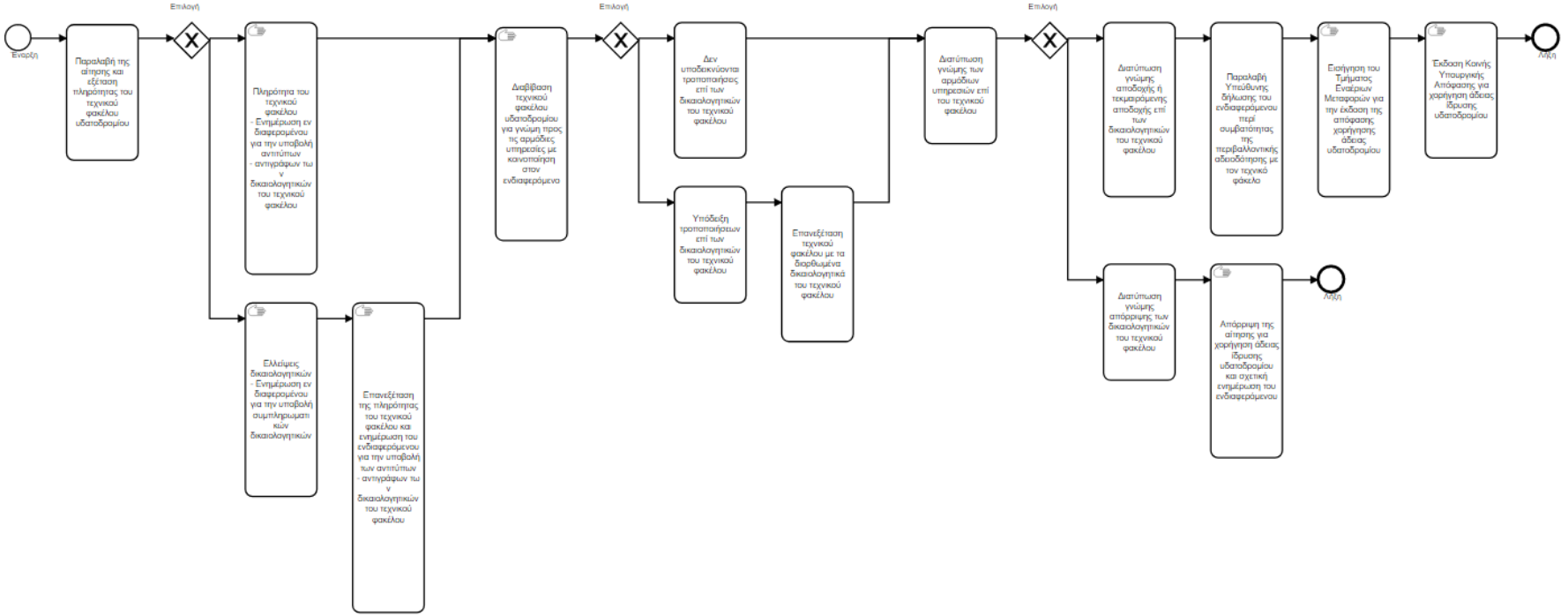


1. The tax agency confirms a tax return based on the verification results from the smart contract platform.
2. The platform calculates the tax liability or refund, based on the tax agency's rules and regulations, and sends the refund to Mary's bank account.
3. It updates the tax-related VC with the tax filing status and payment/refund information, which is accessible from the mobile device.
4. It automatically generates a tax receipt and stores it on the blockchain as a tamper-proof record of the tax filing process.

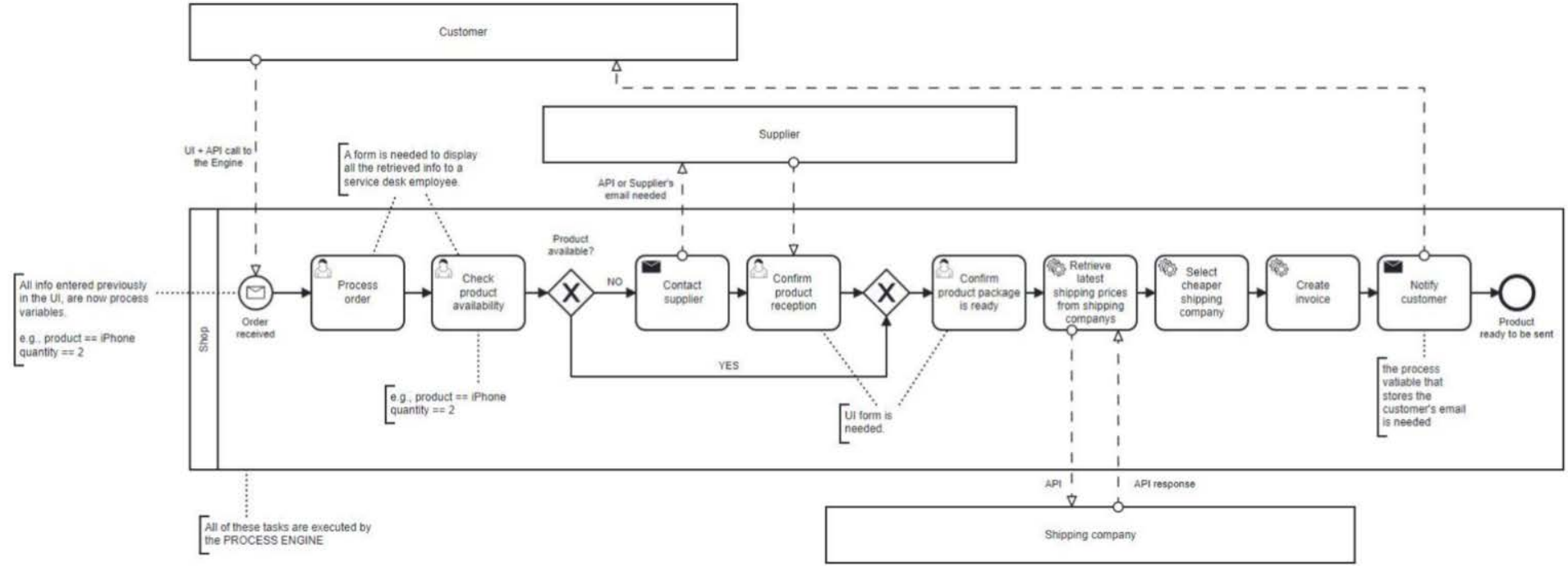
What we need

- Properly recorded processes (mitos.gov.gr)
- Interoperability (Interoperability Center of the Ministry of Digital Governance-ΚΕΔ)
- Blockchain and smart contract technology

What we do - Moving from the strategic…



What we do - ...to the technical modeling

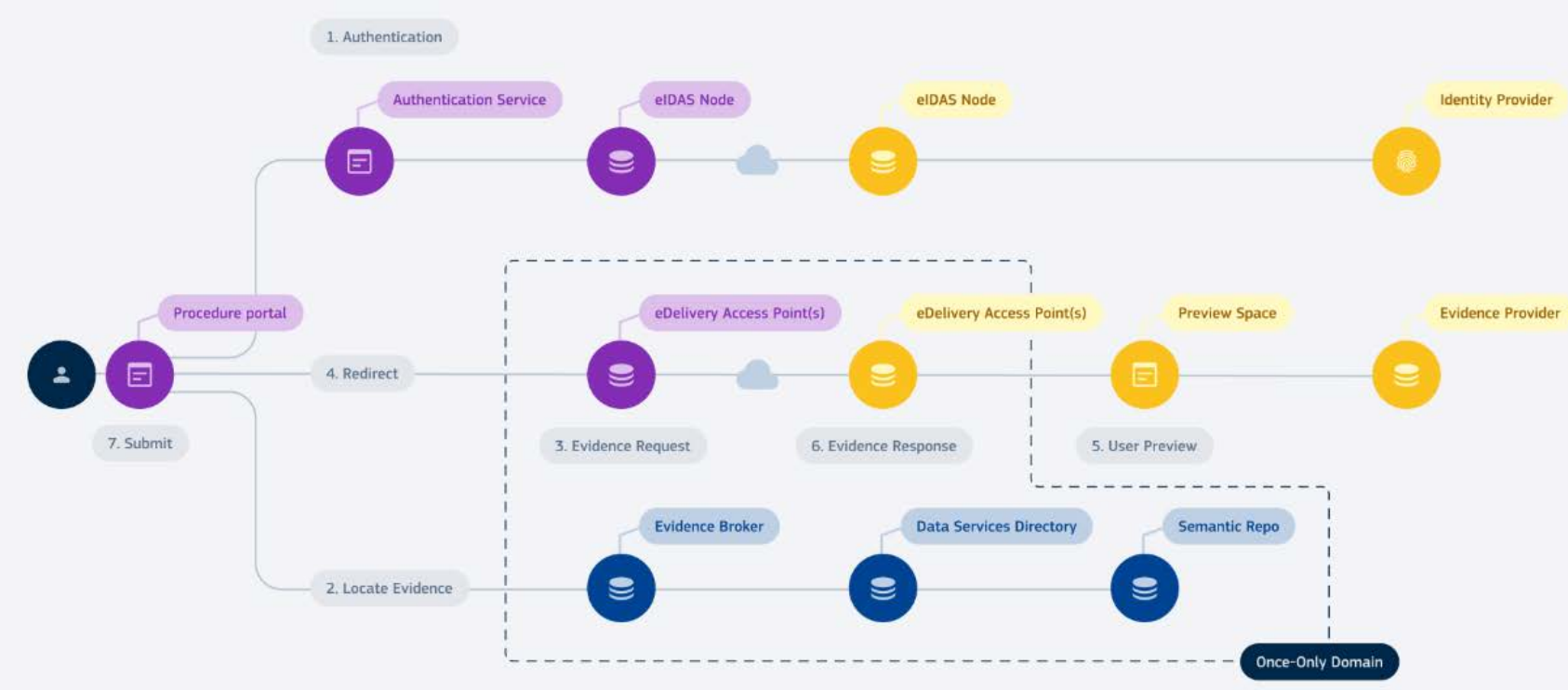


And we need …

A blockchain backend

- To verify the evidences and credentials
- To check their information
- To check their validity and expiration date
- To orchestrate the secure exchange and processing of information based on rules

Once-Only Technical System - They EU vision



Thank you!

varlamis@admin.grnet.gr