Whistleblower Protection

Prepared by

Sarah Afshari and Ali Eghbali

in association with

European Institute of Management & Finance

22 September 2022

Content

- EU Whistleblowing Directive
- National Implementation
- Technical Solution
  - Blockchain-based immutable information chains
  - Smart Integrity Platform by DISS-CO®
- Q&A

The aim of the EU Whistleblowing Directive

Protection for the broadest possible range of categories of persons, who,

- irrespective of whether they are Union citizens or third-country nationals,
- by virtue of their **work-related activities**,
- irrespective of the nature of those activities and
- of whether they are paid or not,
- have privileged access to **information on breaches**
- that it would be **in the public interest** to report and
- who **may suffer retaliation** if they report them.

Breaches falling within the scope of the Union acts

- public procurement
- financial services, products and markets, and prevention of money laundering and terrorist financing
- product safety and compliance
- transport safety
- protection of the environment
- radiation protection and nuclear safety
- food and feed safety, animal health and welfare
- public health
- consumer protection
- protection of privacy and personal data, and security of network and information systems.

Not in Scope (1/2)

The Directive does not affect the application of Union or national law relating to:

- protection of classified information
- protection of legal and medical professional privilege
- secrecy of judicial deliberations
- rules on criminal procedure

Not in Scope (2/2)

The Directive also does not affect:

- national rules on the exercise of the right for workers to consult their representatives or trade unions
- protection against any unjustified detrimental measure prompted by such consultations
- the autonomy of social partners and their right to enter into collective agreements

Who is protected?

- Employees. Persons who, for a certain period of time, perform services for and under the direction of another person, in return for which they receive remuneration
- workers in non-standard employment relationships, including part-time workers and fixed term contract workers, as well as persons with a contract of employment or employment relationship with a temporary agency
- civil servants, public service employees, other persons working in the public sector
- self-employed persons providing services, freelance workers, contractors, subcontractors and suppliers
- shareholders and persons in managerial bodies
- persons whose work-based relationship has ended
- candidates for employment or persons seeking to provide services to the organisation
- volunteers
- paid or unpaid trainees

Who else?

- facilitators who are individuals who assist a reporting person in the reporting process in a work-related context, and whose assistance should be confidential
- third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons
- legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context

What could be reported?

- Events that may constitute a breach or breaches of European and national laws

or

- events which provide a reasonable suspicion of such an infringement

When to report?

- If you observe acts or omissions that you have **reasonable ground** to believe to be a violation.
- If there is a high probability that an infringement will occur.
- When information is available that can detect violations that have already occurred.
- If attempts have been made to conceal violations.

Important: the reported facts must correspond to the truth from your point of view.

How is the whistleblower protected?

Any form of retaliation against whistleblowers is prohibited including threats of retaliation and attempts of retaliation including but not limited to:

- suspension, lay-off, dismissal or equivalent measures
- demotion or withholding of promotion
- transfer of duties
- change of location of place of work
- reduction in wages
- changes in working hours
- withholding of training
- a negative performance assessment or employment reference
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty
- coercion, intimidation, harassment or ostracism

How are concerned persons protected?

- A concerned person is a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated.
- The Internal Reporting Office is responsible to protect the rights of the person concerned in order to avoid reputational damage or other negative consequences.
- The confidentiality of the identity of the person concerned is protected.
- National law ensures the rights of defence including the right of access to the file, the right to be heard and the right to seek effective remedy against a decision concerning the person concerned under the applicable procedures set out in national law in the context of investigations or subsequent judicial proceedings
- The rights of defence and access to remedies of the person concerned should be fully respected at every stage of the procedure following the report

What happens in case of wrong accusations?

- Any person who suffers prejudice, whether directly or indirectly, as a consequence of the reporting or public disclosure of inaccurate or misleading information should retain the protection and the remedies available to him or her under the rules of general national law.
- Where such inaccurate or misleading information was reported or publicly disclosed deliberately and knowingly, the persons concerned should be entitled to compensation in accordance with national law.

National implementation in Cyprus

- The Law on the Protection of Persons Reporting Breaches of **Union and national law** 6(I)/2022 (the "Whistleblowing Law"), which came into force on 4 February 2022, defines the following obliged parties:

- Private sector: legal entities
  - Group 1: ≥250 employees
  - Group 2: ≥50 employees
  - Group 3: < 50 employees, falling within the ambit of the Union acts referred to in the Annex of the Whistleblowing Law, such as rules relating to public procurement, financial services, prevention of money laundering and terrorist financing, product safety, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and animal welfare, public health, and consumer protection.
- Internal Reporting Channel: The obligated parties are required to establish internal reporting channels
  - Group 1: immediately.
  - Group 2: until 17 December 2023, thus ceasing the sharing of any resources as regards the receipt of reports and any investigation to be carried out.
  - Group 3: may share internal channels for reporting and follow-up, provided that the channels are distinct and autonomous.
- Public sector:
  - Group 1: State-owned or governmental legal entities or bodies and
  - Group 2: Municipalities and Communities (Local Authorities) with more than 5.000 inhabitants or more than 25 workers.

National implementation in Cyprus

- A whistleblower (or a ‘reporting person’) is broadly defined as a natural person who reports internally, externally, or publicly discloses information on breaches in their work-related activities within a legal entity.
- **Anonymous Reports:**

  The Whistleblowing Law does not impose a direct duty on private sector legal entities to accept and follow up on an anonymous report. However, when an anonymous whistleblower is subsequently identified and/or suffers retaliation, they are entitled to the full protection of the law.
- **Sanctions:**
  - Entities: Fines up to 30k €
  - Individuals who hinder or attempt to hinder reporting, retaliate against reporting persons, bring vexatious proceedings against reporting persons, infringe the duty to maintain the confidentiality of the reporting person's identity, or knowingly report or disclose false information could incur criminal liability.

  ➔ Fines up to 30k € and imprisonment of up to 3 years

Comparison to Germany

The Whistleblower Protection Act exists as a draft.

Main differences:

- Anonymous reports can be processed if this does not leave the processing of confidential reports behind
- Legal entities as facilitators are not protected
- The reversal of the burden of proof does not apply to supporters
- Municipalities and communities are only obliged to have more than 10,000 inhabitants
- There is no financial support for the whistleblower
- Fines up to 100 k €
- As far as verification of the information by the whistleblower is concerned, there is even talk of it being reasonable for the whistleblower to engage a lawyer

What should the IRO do?

The Internal Reporting Office (IRO):

- acts impartially and independently
- has the necessary knowledge and background to handle internal messages
- receives messages
- advises the user on questions
- conducts internal investigations
- maintains communication with the person reporting the potential violation
- coordinates internal communication

And what else?

- observes deadlines
- is the interface between management, data protection officers, the works council, the trade union and other stakeholders involved
- cooperates with external authorities in investigative proceedings
- protects both the reporting person and the persons concerned
- is responsible for the coordination of the **follow-up measures**
  - **Close the control gaps**
  - **Improve governance**
  - **Raise awareness**

The biggest risk

- The reporting person has the choice to report externally
  - To the competent authority
  - To the press, if the competent authority does not respond appropriately within the statutory time limits

- Risks:
  - Reputational damage
  - Greater financial damage through
    - Internal and external resources to deal with the requests from the competent authority

About Blockchain

- Continuously expandable list of data records in individual blocks.
- New blocks are created according to a consensus procedure and appended to an existing chain using cryptographic procedures.
- Each block typically contains a cryptographically secure hash (scatter value) of the previous block, a timestamp and transaction data.

Transparency throughout the Chain

Distributed Ledger

A distributed database for recording data that shared across the network

Cryptography

Ensuring security, authentication and endorsing transactions

Smart Contract

Embedding rules in the blockchain network and enforcing them when performing transactions

Consensus

Confirmation of transactions made in the network by all members

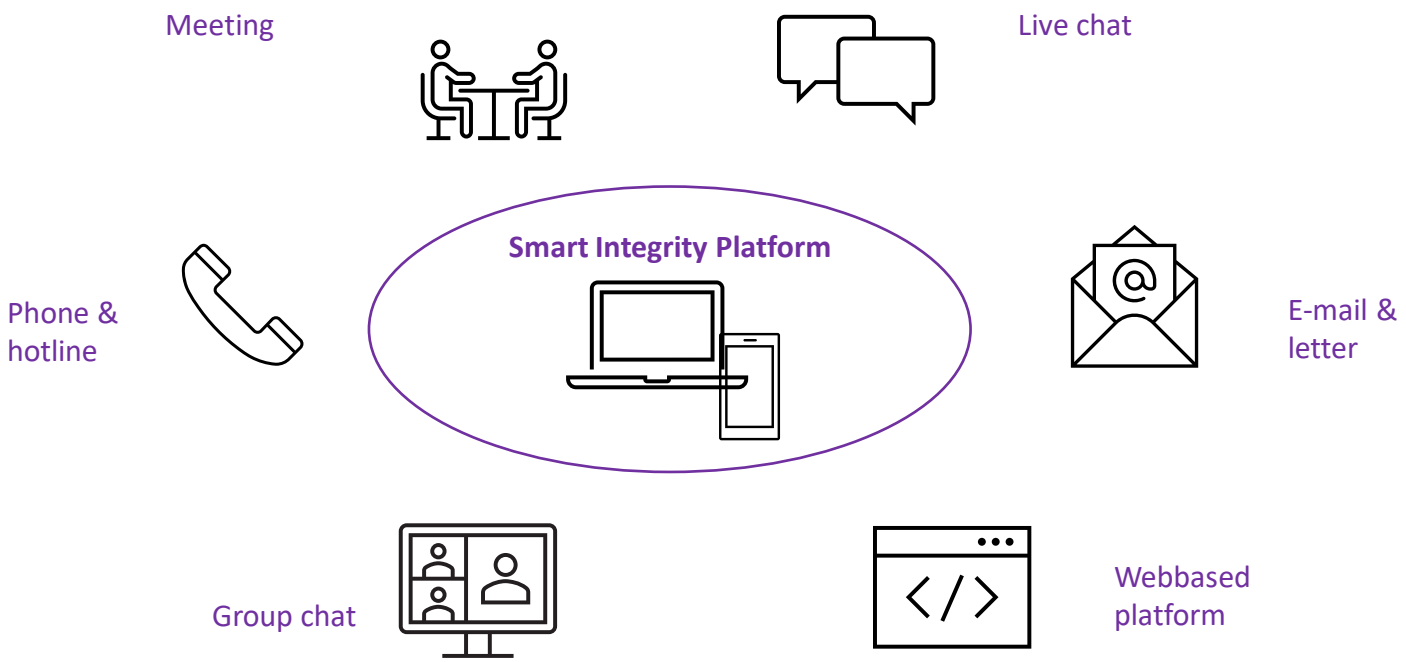
How can blockchain help?

- Blockchain technology ensures higher safety through immutable data chains
- Data chains are saved in data blocks that are connected with HASH.
- Among other things, the data records receive a time stamp and cannot be changed. This increases the prevention of fraud by reducing the risk of manipulation to a minimum.
- Users and owners can trust data hosted by the blockchain.
- Deletion of data outside of blockchain on DISS-CO’s Smart Integrity Platform is possible to ensure GDPR compliance.

DISS-CO

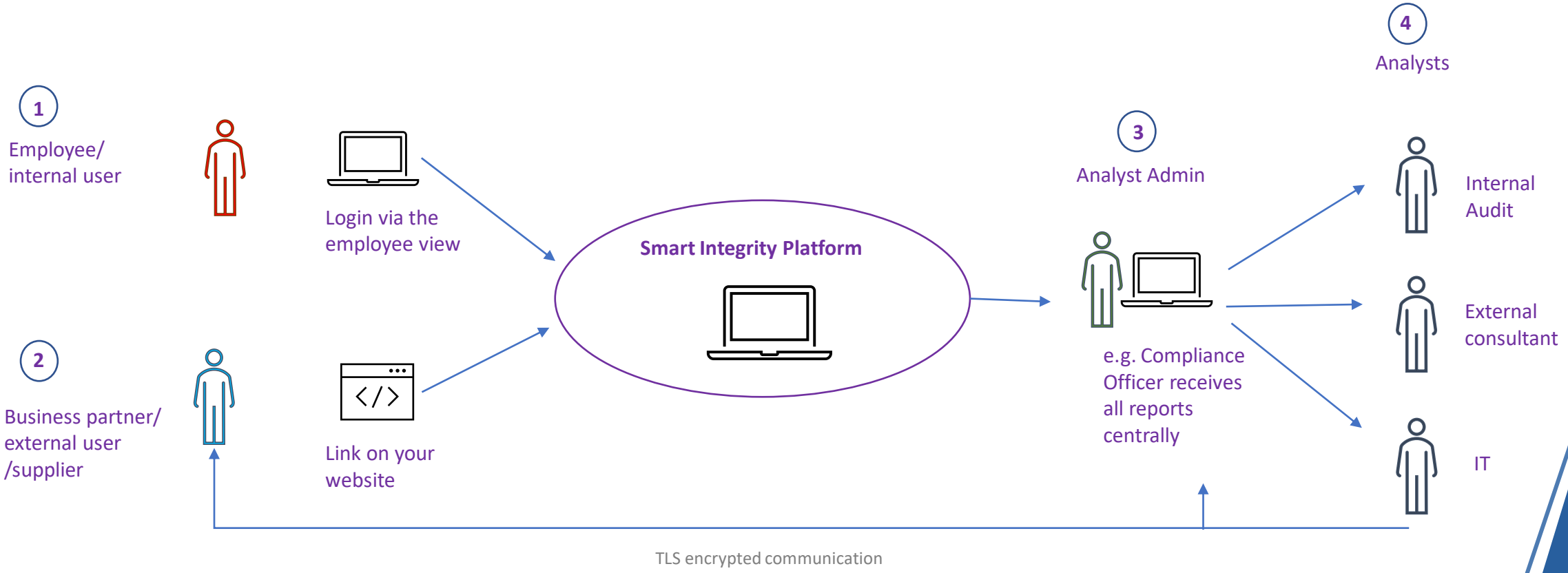
The Smart Integrity Platform - Reporting Channel

Multiple channels, centralised incident recording and case management. The use of the Smart Integrity Platform guarantees absolute anonymity and security of your data.



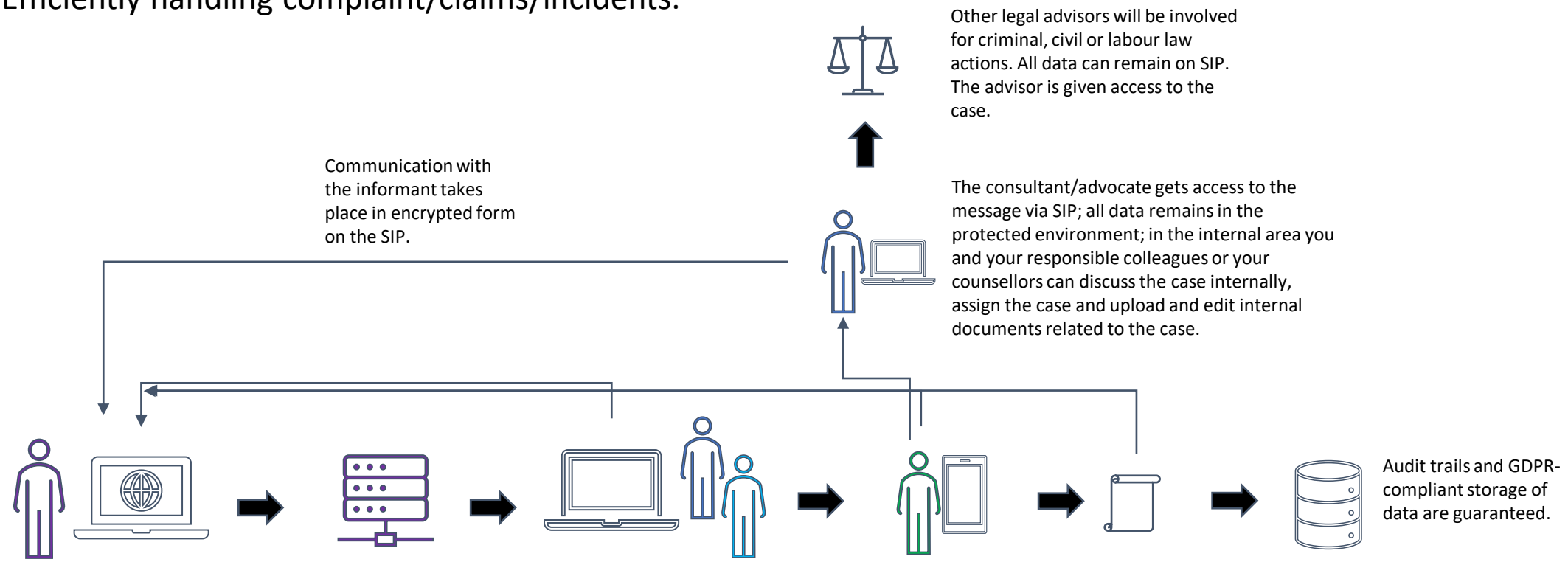
The Smart Integrity Platform - Reporting Channel

Encrypted internal and external communication.



The Smart Integrity Platform - Reporting Channel

Efficiently handling complaint/claims/incidents.



Sarah Afshari

Sarah.afshari@diss-co.tech

DISS-CO GmbH
Winterhuder Weg 29
22085 Hamburg

https://diss-co.tech

Tel.: +49 (0)40-226 392 51-0

Sarah Afshari is the founder & Managing Director of DISS-CO, a tech start-up that focuses on agile digital solutions for risk, governance & compliance. She has more than 18 years of experience in combating white-collar crime. As the Director of a big4 company, she was responsible for international investigations and compliance audits, distributor and supplier audits. As the Compliance Officer of a listed construction company, she improved the compliance management system and was responsible for the internal investigations.

Example projects & activities:

- Management of international investigations, e.g., for listed companies under US DOJ and SFO monitorship
- Management of international compliance audits and internal audits for a listed automotive company
- Anti-bribery/FCPA audits at 22 subsidiaries of a company in the energy sector
- Third-party audit at 16 distributors of a company with governmental customers (navy, military)
- Asset tracing of 1 billion USD in the Middle East
- +300 fraud and bribery investigations
- Mass data analytics for monitoring fraud risks
- Advisor to the EEAS of the European Commission regarding Supplier/Customer Due Diligence Procedures
- Speaker at compliance events

Ali Eghbali

ali.eghbali@diss-co.tech

DISS-CO GmbH
Winterhuder Weg 29
22085 Hamburg

Email: info@diss-co.tech
https://diss-co.tech
Tel.: +49 (0)40-226 392 51-0

Ali Eghbali is the CTO of DISS-CO and a blockchain expert. He gained his extensive experience in the field of blockchain and smart contracts in various projects, for example in the energy sector. Ali is also a cyber security expert, a certified ethical hacker and computer forensic investigator.

His focus lies on the development of DISS-CO's Smart Integrity Platform with the whistleblowing module and an upcoming blockchain module.

Ali is experienced in the development and programming of blockchain systems for fraud prevention and supply chain.

Example projects and activities:

- Designing blockchain system in energy sector
- Designing blockchain system for industrial real-time monitoring
- Designing blockchain system for Wireless Sensor Network (IoT based Blockchain)
- Implementing penetration tests for companies
- Designing network architectures and implementing Microsoft Windows and Linux Servers for companies in different sectors
- Lead of development team
- Developing back-end for USSD service for cellphones

Thank you!