# Problem statement, solution and challenges

## **Problem 1:** Ineffectiveness of Loyalty in Small Ecosystems

### What is the problem?

Corporate companies give extra benefits to their employees other than the regular salary. On the other hand, some of the benefits given to employees are not utilized and wasted. It is also very expensive a wide range benefit selection. Companies tend to maximize the effectiveness of the benefits of their employees without wasting unnecessary money. Increasing the effectiveness while decreasing the budget contradicts most of the time.

### Why blockchain/DLT/IDelta is the solution for that problem

Some of the benefits doesn’t meet the requirements of the employees and they expire before they are used and become wasted. Instead of giving benefits directly to employees, a token or coin could be given employees and benefits can be offered on the digital markets of the companies. If DLT is used, every benefit that is offered in the system will be available to a wider network of people. Also, employees of small companies can reach to a wider selection of benefits. Instead of using a central system, DLT increases the trust between companies and employees and makes the process more transparent to everyone. Thus, DLT encourages companies and employees to join the network and create a virtuous cycle with positive feedback.

### If blockchain/DLT/IDelta is the solution for that problem, what are the challenges.

Companies should also create a digital identity for each of their employees. Security and maintenance of those digital identities could be a problem for novice users.

## **Problem 2:** Fraud of Gaining Benefits

### What is the problem?

Sometimes, two companies give benefits to each other’s employees. The problem is they can’t be sure if any employee is really an employee of the companies who made the deal. They can verify the identities by making integrations to each other’s system or building a central system, but this would create many new expenses and technical difficulties.

### Why blockchain/DLT/IDelta is the solution for that problem

A Digital Employee Identity is the solution for the problem. In this scenario, companies don’t need to know the personal information, they just need a verification. A DLT which holds hash codes of the employee id cards, could easily provide the verification of digital identities. DLT also reduces, many bi-directional integrations with any two companies. Every company in the network can easily reach the DLT for verification by only joining the network.

### If blockchain/DLT/IDelta is the solution for that problem, what are the challenges.

Verification of identities without giving any personal information. Revoking the validity of the identity from DLT. Making companies keep the DLT updated.

## **Problem 3:** Non-trustworthy of Current Employee IDs

### What is the problem?

Many companies give services to their users by sending their employees to the offices and homes of the users. As an example, telecom companies or their sub-contractors send their employees when a user buys a network connection. Users cannot be sure if the coming party is truly an employee of the selling telco company. Employees have physical id cards, but those id cards cannot be validated by the users with sure. Therefore, a person can abuse this situation if he/she knows the user requested a service to his/her house.

### Why blockchain/DLT/IDelta is the solution for that problem

Using DLT and Digital Identity, users can easily verify the digital identities. If a network of DLTs is established, it would be the only source for verification and it becomes very popular. Some companies can build their own DLT for verification of its employees, but then it becomes confusing for users and app developers to read data from several DLTs. I-Delta will be de solution for this scenario by providing interoperability between DLT technologies and instances, so Developers and Companies can verify the identities just by knowing a single protocol and system.

### If blockchain/DLT/IDelta is the solution for that problem, what are the challenges.

Interoperability of data-only DLTs is not a big problem, however if the smart contract and consensus mechanisms are very different, then it is becoming very complicated to enable inter-operability between DLTs.

## Project Innovations and Technological Value Chains

Since the paper of Bitcoin, the biggest innovation of DLT is the Smart Contracts, because it increased the value of DLT and created a platform for endless scenarios and use-cases. Currently, most of the DLT research projects try to solve the scability and performance problems of DLTs and they focus on consensus algorithms. Blockchain and DLTs are still new technologies and many other innovations are possible other new consensus algorithms and smart contract mechanisms.

DLTs are promoted as more secure platforms than the central systems and databases, but it’s not secure in all manners. DLTs are considered to be secure, because they are disintermediated, censorship-resistant and tamper-proof digital platforms of distributed trust. On the other hand, they reveal all the information that is written on. By its nature, sensitive information cannot be hidden from specific parties of the network unless data is encrypted with specific cryptographic algorithms. Using simple symmetric and asymmetric encryption to secure some data between two parties is not a good solution for DLTs. The biggest value of DLTs is trust between parties. By simply encrypting data between two parties make other parties useless for the data and creates a P2P channel. Other parties cannot understand the operations and cannot make an effective role in consensus. As a solution to this problem, cryptographic algorithms can be mixed and matched with sophisticated methods and other algorithms to create proofs that can be voted by all parties while not revealing sensitive information. This method mostly known as zero knowledge proof (ZKP). In I-DELTA project, we are going to offer practical zero knowledge algorithms for the common problems. Creating a general zero knowledge algorithm is very hard and resource consuming on consensus phase. Instead, discovering and inventing zero knowledge algorithms for specific use cases are much more practical and resource effective. ZK-Snark is a general ZKP, but there are many applications of homomorphic encryptions for ZKP algorithms which solve real problems. On top of data layer, I-DELTA will provide a ZKP layer that can be used as an API with user-defined smart contracts. These common problems will include at least the following use cases;

* Verification of balances of accounts without knowing their real balance
* Verification the validity of an amount of asset transfer
* Verification of a field of digital identity without revealing personal information (such as verification age restriction without revealing age and other personal information)
* Verification of DNA similarities between two people (such as parent test) without revealing any subset of DNA information

and their general ideas.