ZK Payroll Protocol

Ensuring Secure and Private Salary Transactions on the Mina Protocol

Table of contents

Creative
Agency

01 Problem

02 Solution

03 Objective

04 How It Works

Problem

- Visibility of Transactions: In current blockchain-based payroll systems, all transactions are publicly visible, which can **expose sensitive salary information** of employees.
- Potential Risks: This lack of privacy could lead to issues like:
  - Unequal treatment or workplace tension.
  - External parties analyzing internal financial data.
  - Risk to employees' financial privacy.

Solution

Zero-Knowledge Payroll Protocol

- An innovative protocol that allows companies to **pay employees anonymously**, ensuring that only the company and the employee know the salary amount.
- Transactions are still processed transparently on the blockchain, but **sensitive information remains confidential**.

Objective

Protect salary privacy

Prevent public disclosure of employees' salaries.

Online experience

Ensure all actions are conducted online.

Seamless experience

Minimize the number of actions required.

Exclusive Confidentiality

Only the company knows the salary of each employee.

How It Works

Actors

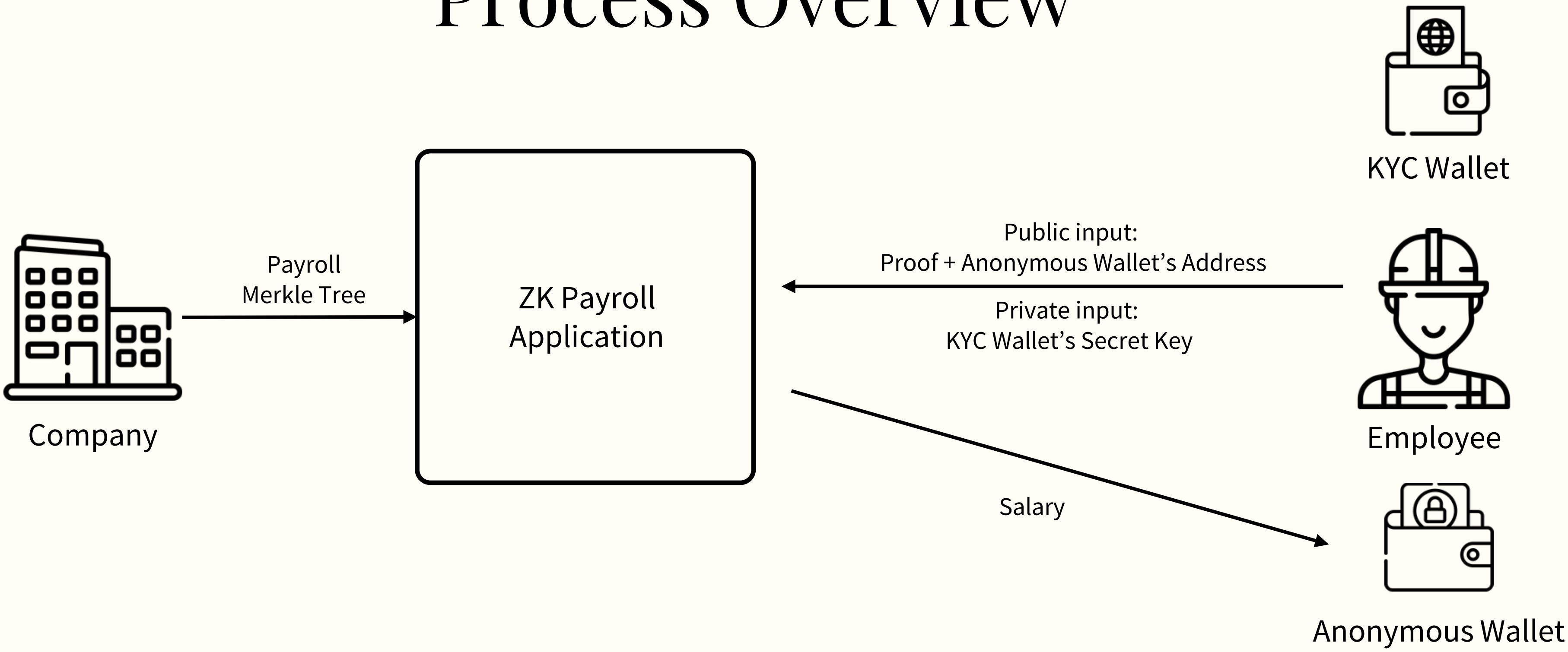
Company

- Initiates salary transfers.

Employee

- Receives salary payments securely and anonymously.
- Represented by a public key (KYC), with the corresponding secret key kept private.

Process Overview



Company

Payroll
Merkle Tree

ZK Payroll
Application

Public input:
Proof + Anonymous Wallet's Address

Private input:
KYC Wallet's Secret Key

Salary

KYC Wallet

Employee

Anonymous Wallet

Payroll Merkle Tree

Whenever the company transfers money to its employees, they will upload a **Merkle** map to a smart contract.

- Each leaf in the Merkle tree will have a key defined as H(pk, n), where H is a hash function, pk is the employee's public key, and n is the nth payment cycle.
- The value associated with each leaf will be the amount of money that can be withdrawn.

Withdraw Process

- To withdraw their salary, the employee will execute a transaction using the **secret key** corresponding to their KYC public key as a private input and specify a wallet address to receive the funds.

⚠ Each time they withdraw, the employee will use a **different address** to prevent identifying multiple transactions as belonging to the same person.

Thanks!

Email: ngdatuananh@gmail.com
Telegram: @zennomi