



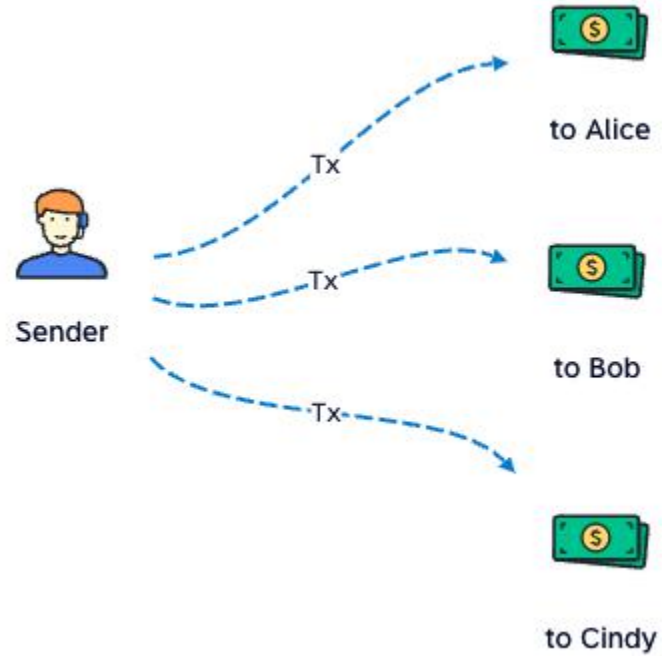
2022

ZkPayroll

Double security



# Batch Pay



## Usually Pay

one tx one payment  
gas: high  
time: long



## Batch Pay

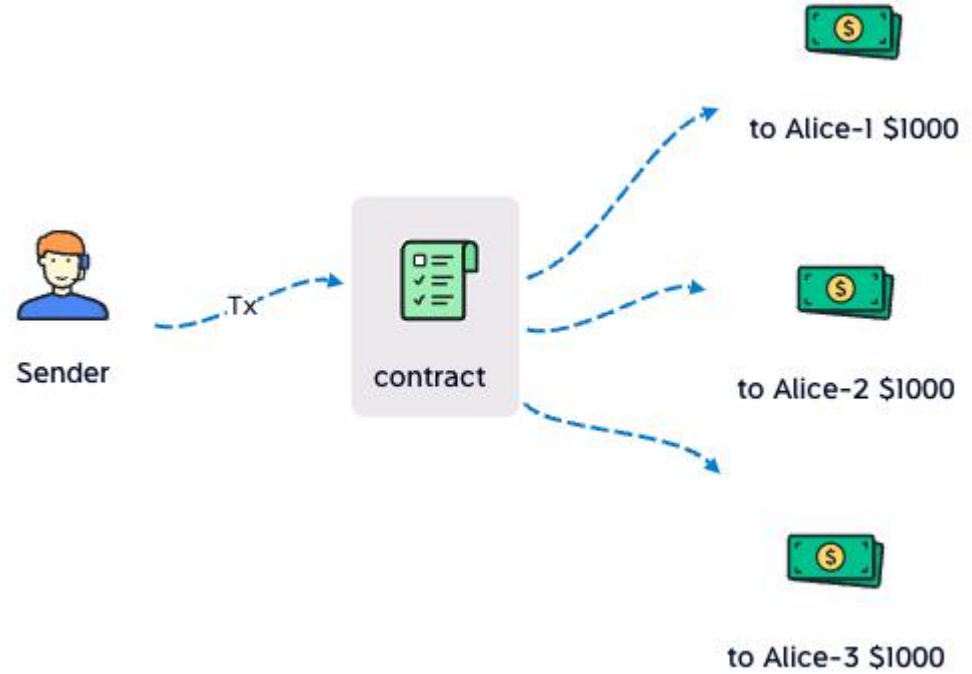
one tx multi payments  
gas: low  
time: short



# Batch Pay

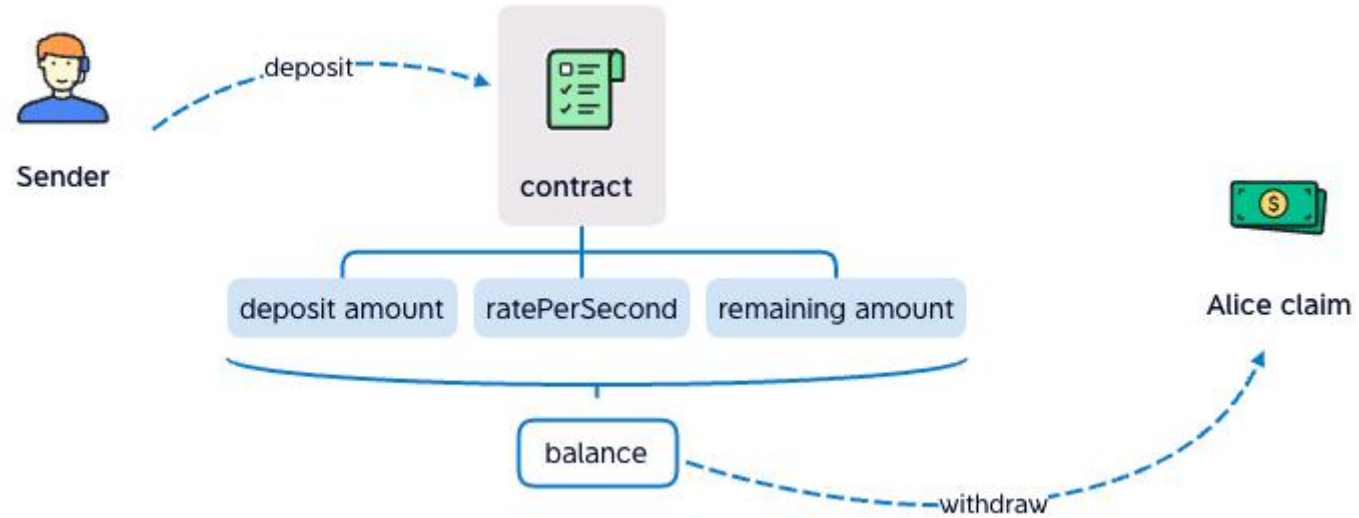
## Hide the high salary

split \$3000 into 3 payment(address)





## Streaming Pay



### **Claim salary every sec**

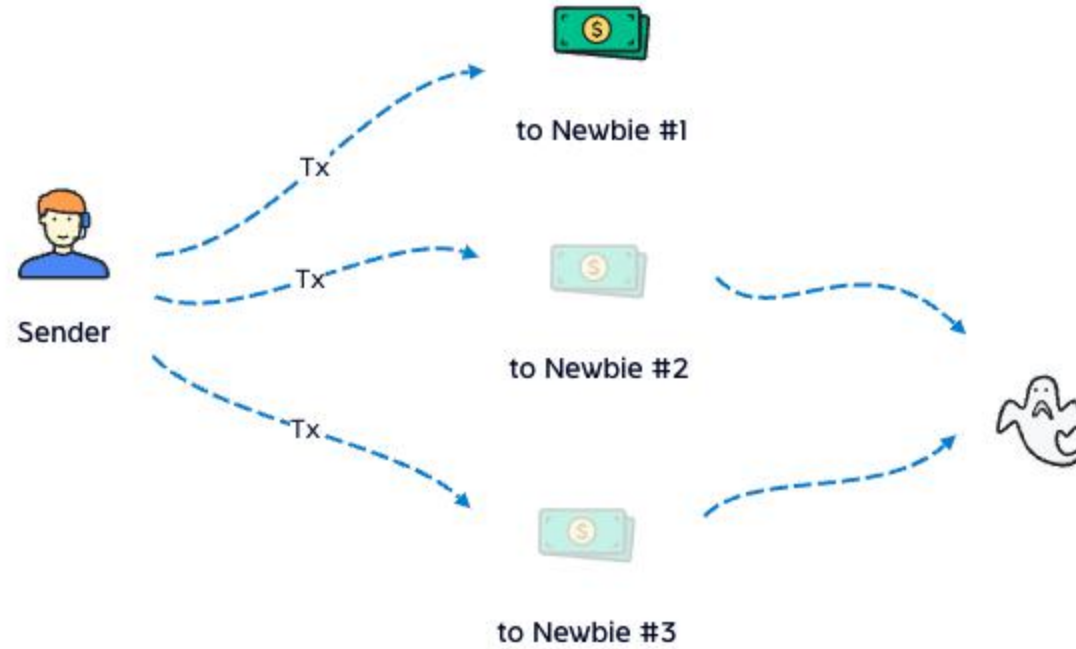
sender deposit to contract

recipient withdraw from contract

contract calculates how much (balance) the recipient can claim



# S a f e B o x

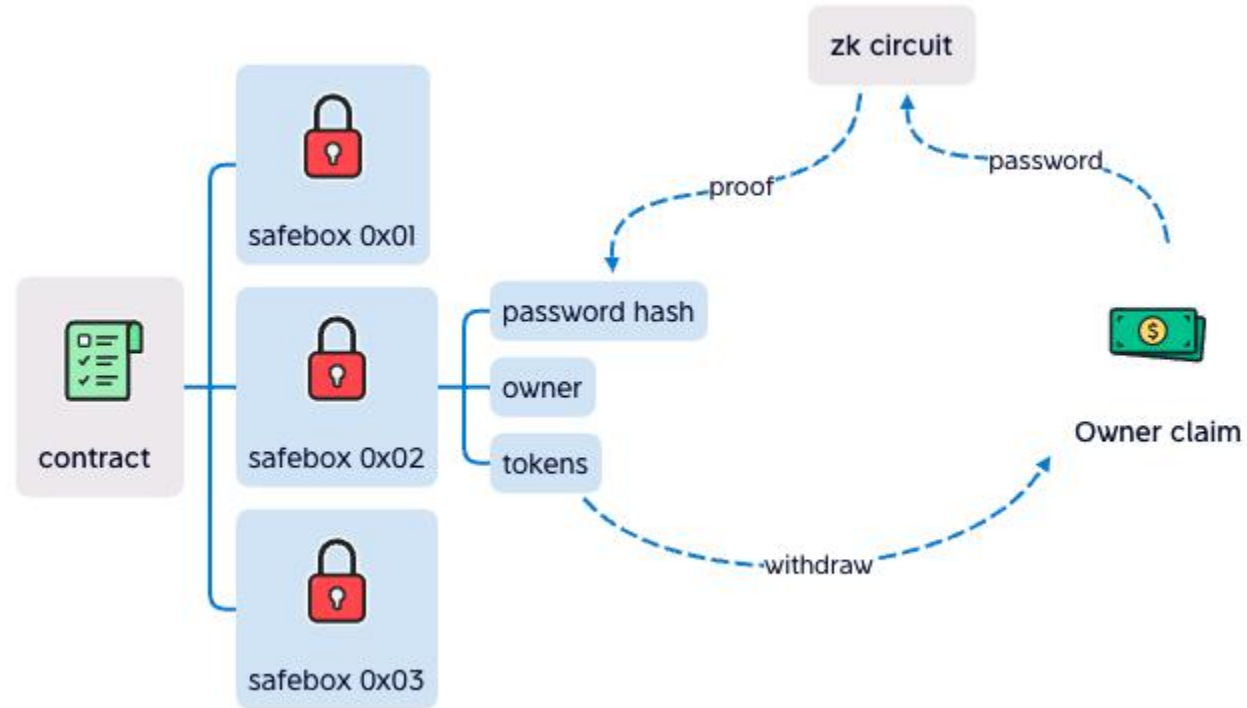


## Is your wallet safe enough?

We recognize that the newbie's first salary is much easier to be stole  
In fact, there're many ways to take our private key



# Safe Box



## It hides password

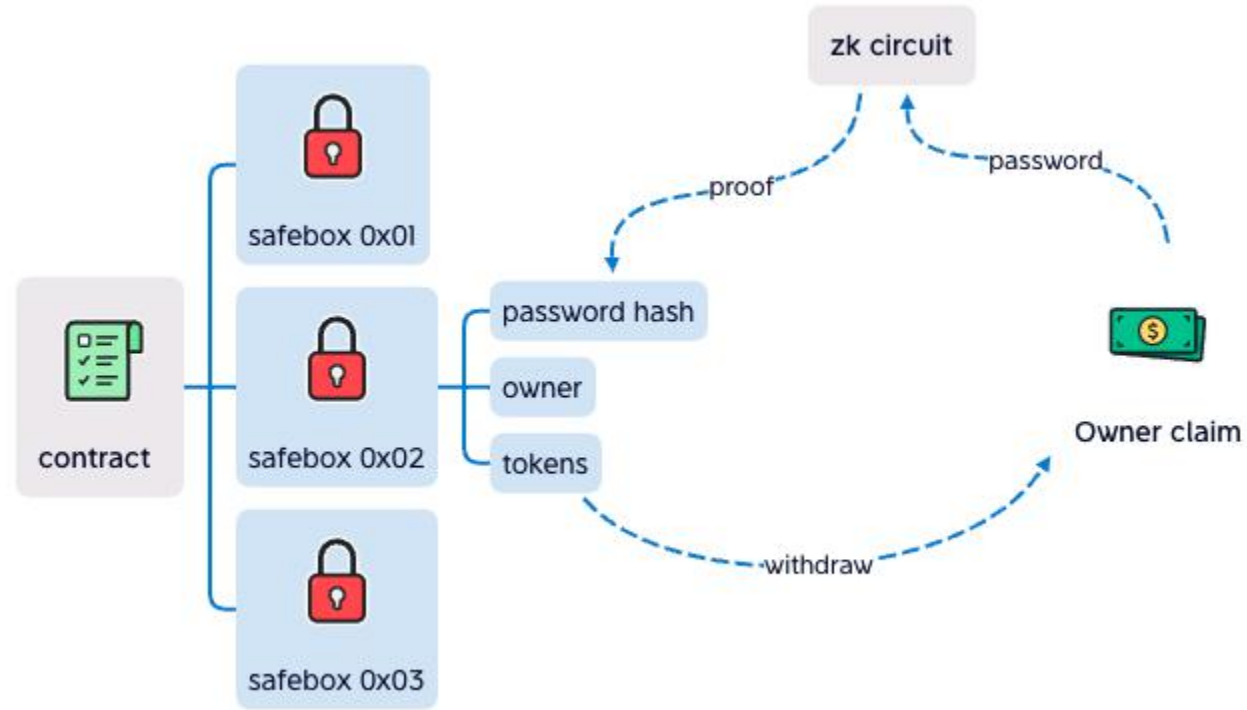
user input password to zk circuit at frontend

zk circuit calculate the proof to contract

contract verify success, withdraw to user



# S a f e B o x



## Double Security

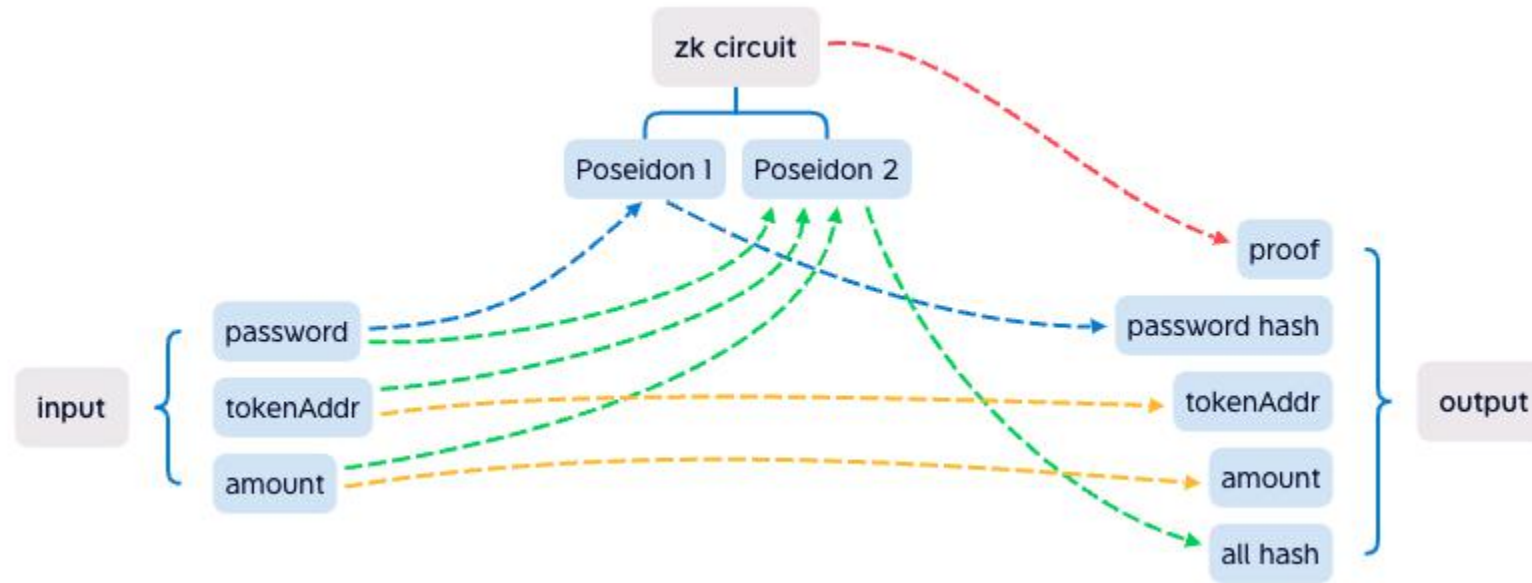
private key is taken, safebox is still safe

password is taken, safebox is still safe

both private key and password are taken, that's so bad



# S a f e B o x



## zk circuit

it's complex, but it's done, and works well  
we'll try to upgrade it, make it harder to calculate  
anti brute force cracking





# T e a m



George

10+ years full stack develop  
4 years solidity develop  
boring coder



BlackRabbit

10+ years full stack develop  
2 years web3 develop  
another boring coder



2022

谢谢观看

THANK YOU

<https://github.com/busyapedao/zkpayroll-contract>