DIGITALSEAL:

A TRANSACTION AUTHENTICATION TOOL FOR ONLINE AND OFFLINE TRANSACTIONS

INHA UNIVERSITY

theVaulters

UNIVERSITY OF CENTRAL FLORIDA

Changhun Jung

Jeonil Kang

Aziz Mohaisen

DaeHun Nyang

Outlines

1. ABSTRACT
2. INTRODUCTION
3. DIGITALSEAL
4. USER STUDY
5. SECURITY AND COST ANALYSIS
6. CONCLUDING REMARKS

ABSTRACT

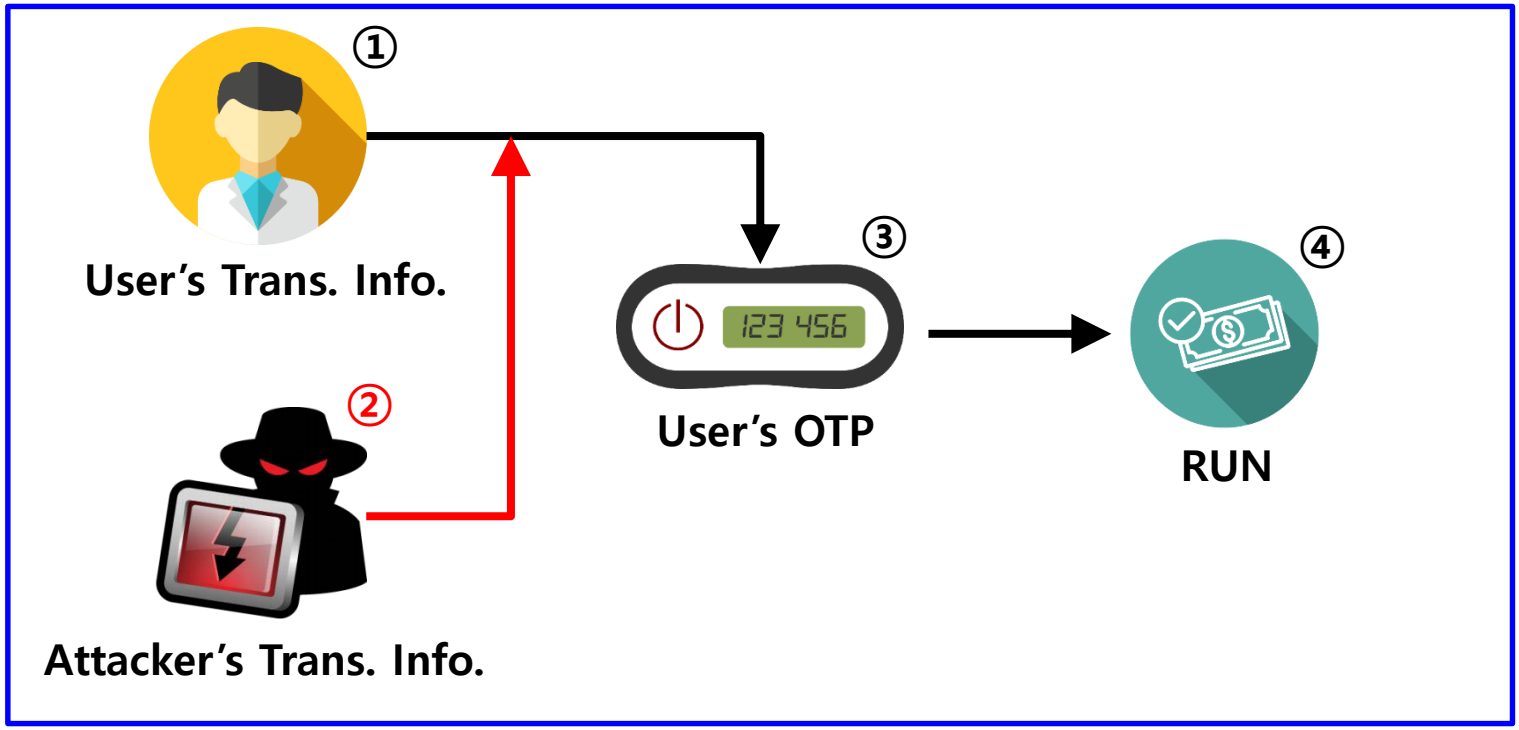
ABSTRACT

- **Abstract**
  - **Existing various OTPs have a shortcomings against MitM, MitB.**
  - **DigitalSeal can scan a barcode which includes transaction information and then make a HOTP's Tag, The HOTP's Tag can be used to make up the shortcomings.**
  - **DigitalSeal is built by using a Arduino etc and can be used to online and offline transactions.**

INTRODUCTION

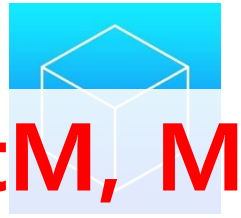
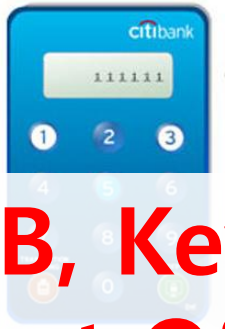
INTRODUCTION

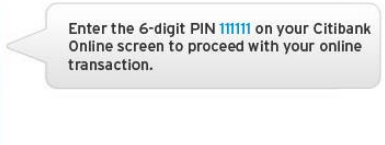
- **Shortcomings of existing OTP**
  - **Existing various OTPs have a shortcomings against MitM, MitB.**



INTRODUCTION

- **Shortcomings of various Authentication Tools**
  - **Google Authenticator, Free OTP, Citibank OTP, RSA's secureID, Dell's defender, Secure Card and Ezio Optical Reader have a various vulnerability.**

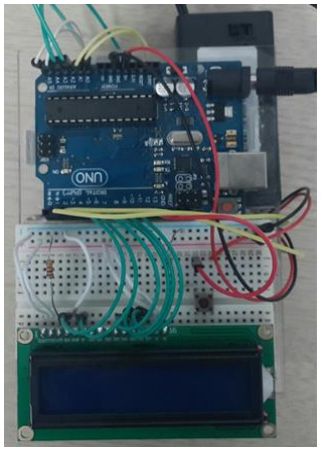




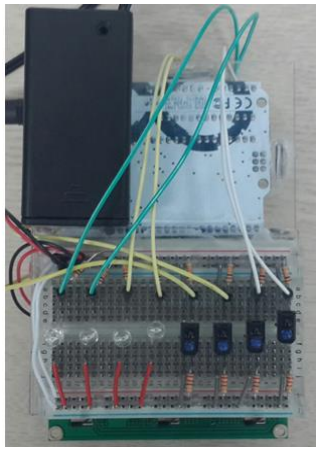


MitM, MitB, Key Management, Not Support Offline Transaction


INTRODUCTION

- **DigitalSeal**
  - **We introduce DigitalSeal, a transaction authentication tool that works in both online and offline scenarios.**
  - **DigitalSeal is capable of reading information viewed on paper, computer monitors, kiosk monitors and smartphone.**





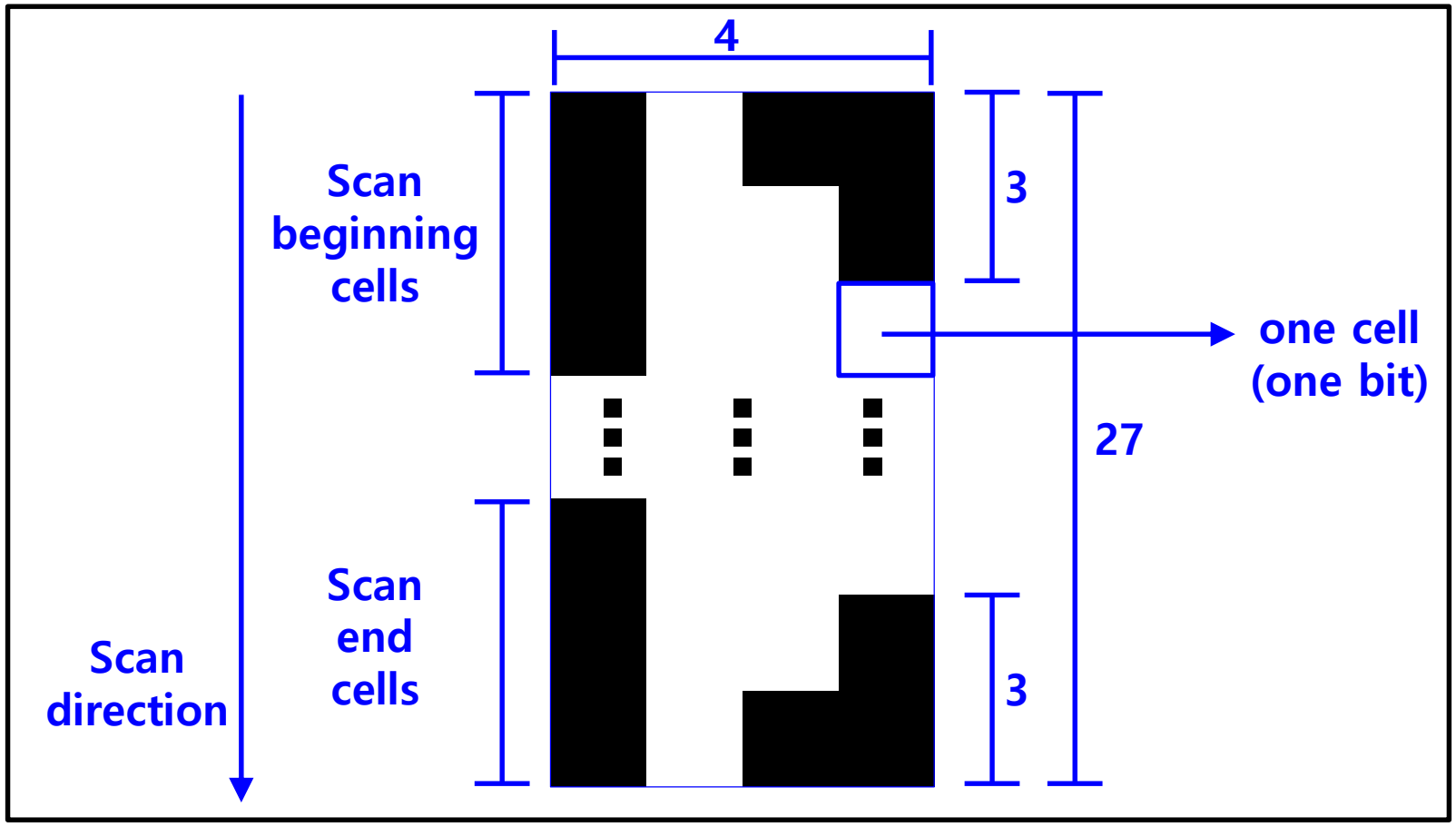
DIGITALSEAL

DIGITALSEAL

- **DigitalSeal**
  - **In DigitalSeal, a user swipes DigitalSeal downward so that it can scan a crafted barcode on a screen or piece of paper.**
  - **The crafted barcode contains the transaction information, such as recipient name, amount of transaction, etc., and DigitalSeal displays a HOTP's tag calculated with a preshared key and transaction data on DigitalSeal's LCD screen.**

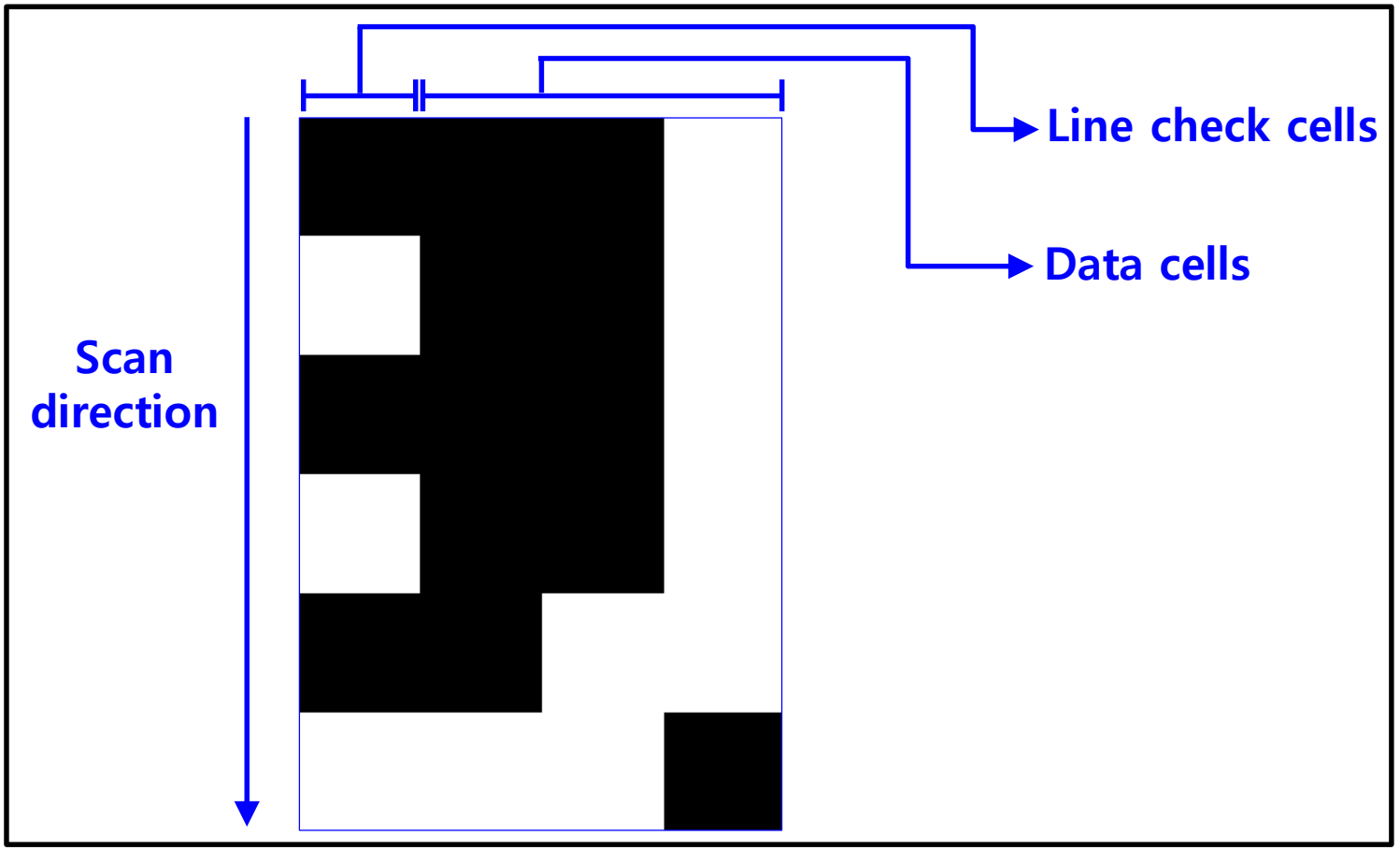
DIGITALSEAL

- The craft barcode for DigitalSeal



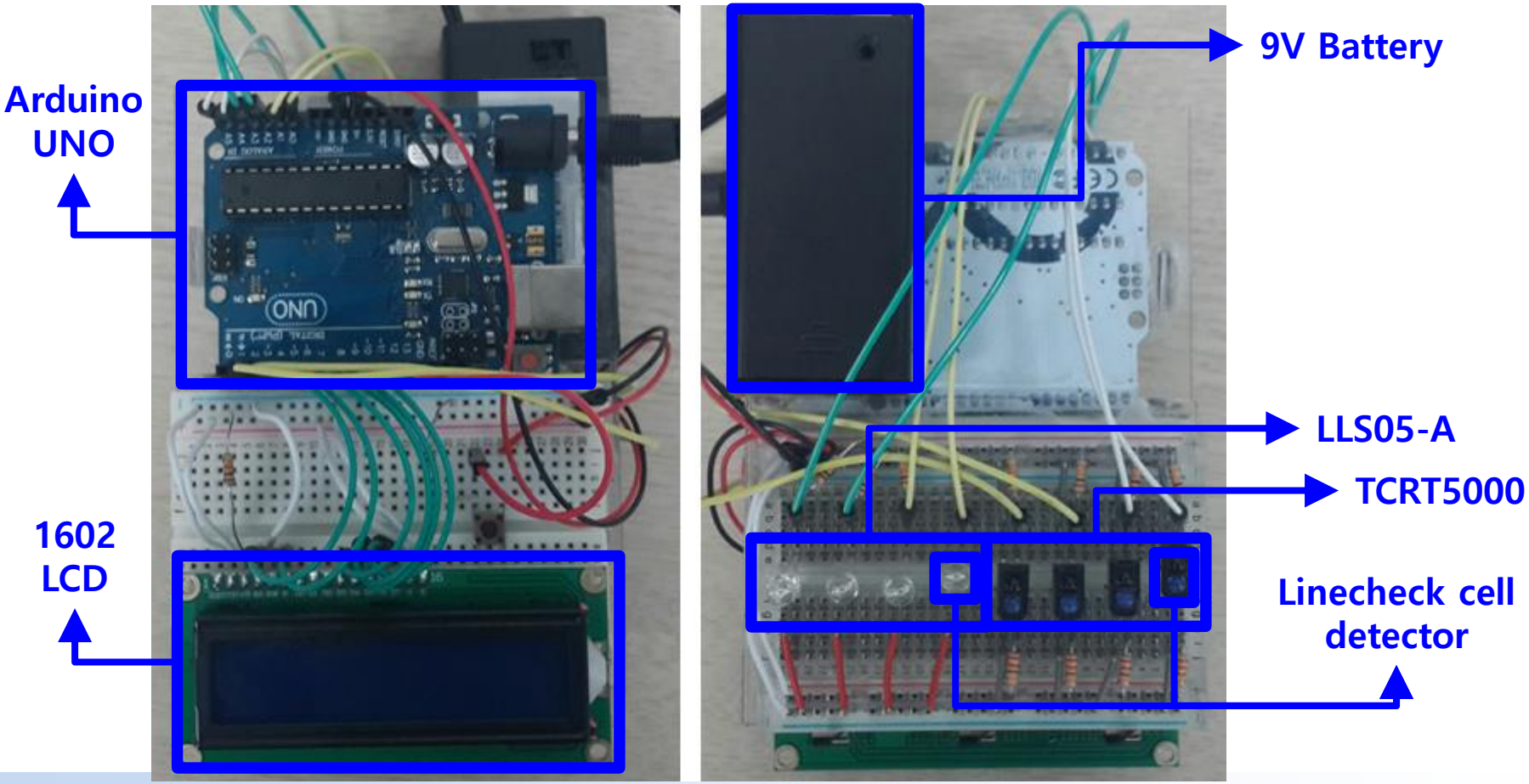
DIGITALSEAL

- The craft barcode for DigitalSeal



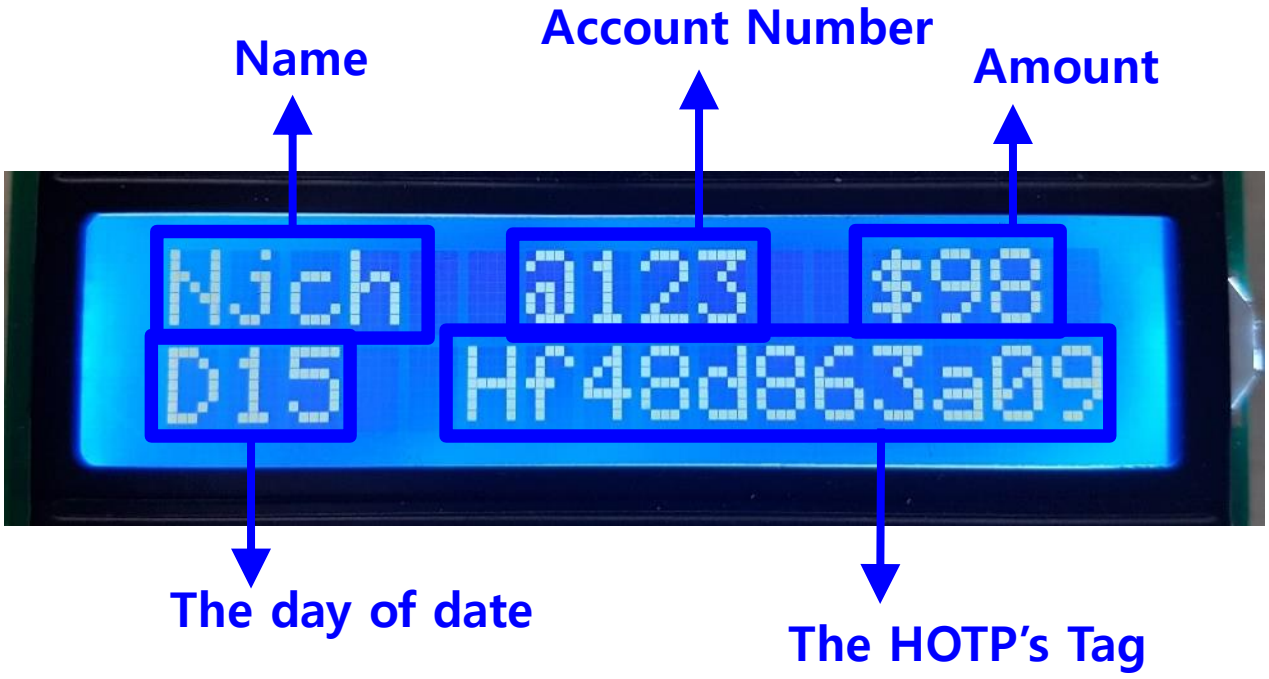
DIGITALSEAL

- Components for DigitalSeal



DIGITALSEAL

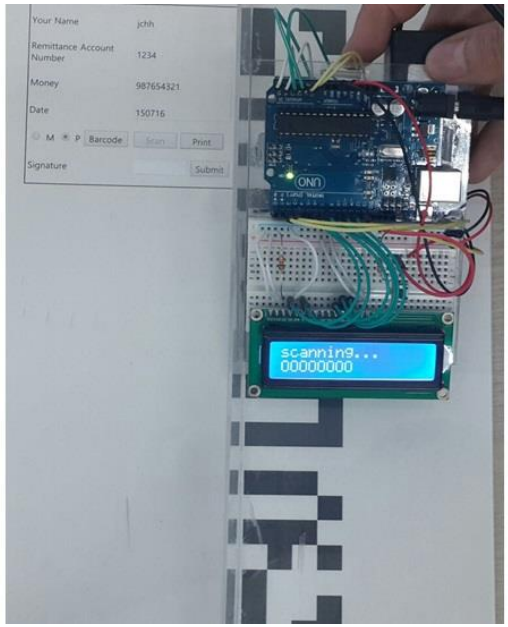
- Output Format on DigitalSeal LCD



DIGITALSEAL

- Using DigitalSeal

on Monitor

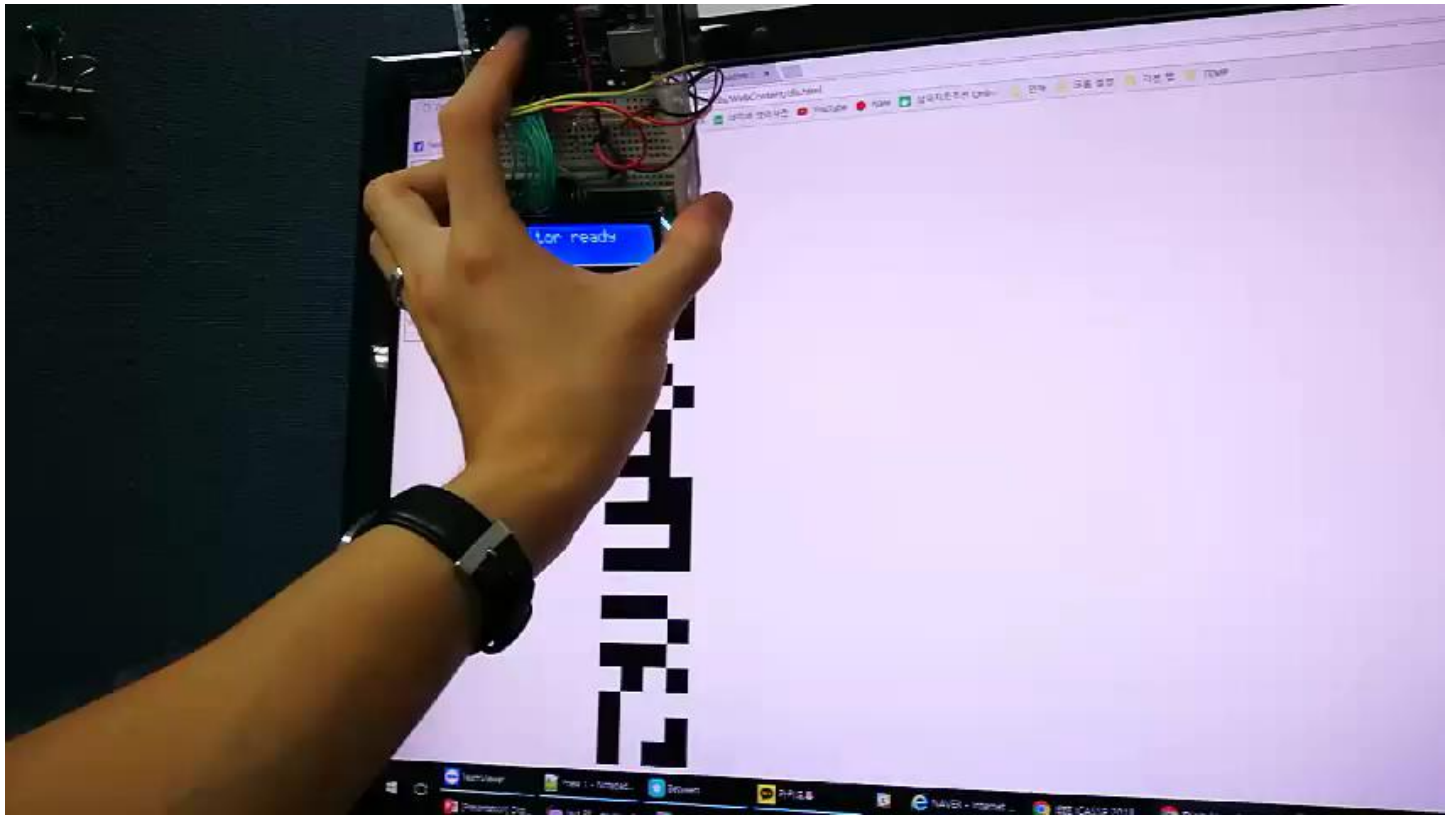


on Paper

on Smartphone

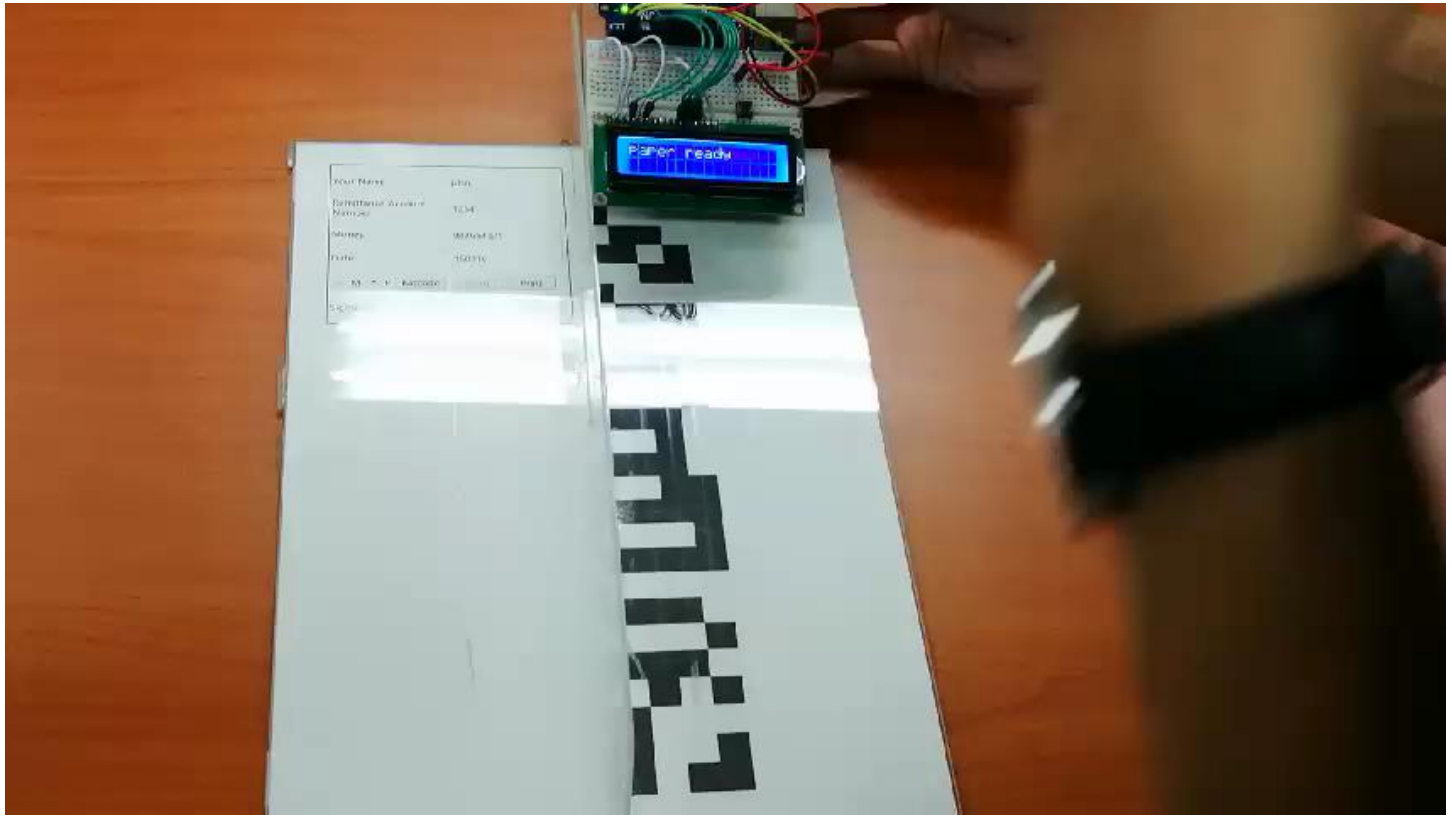
DIGITALSEAL

- Using DigitalSeal



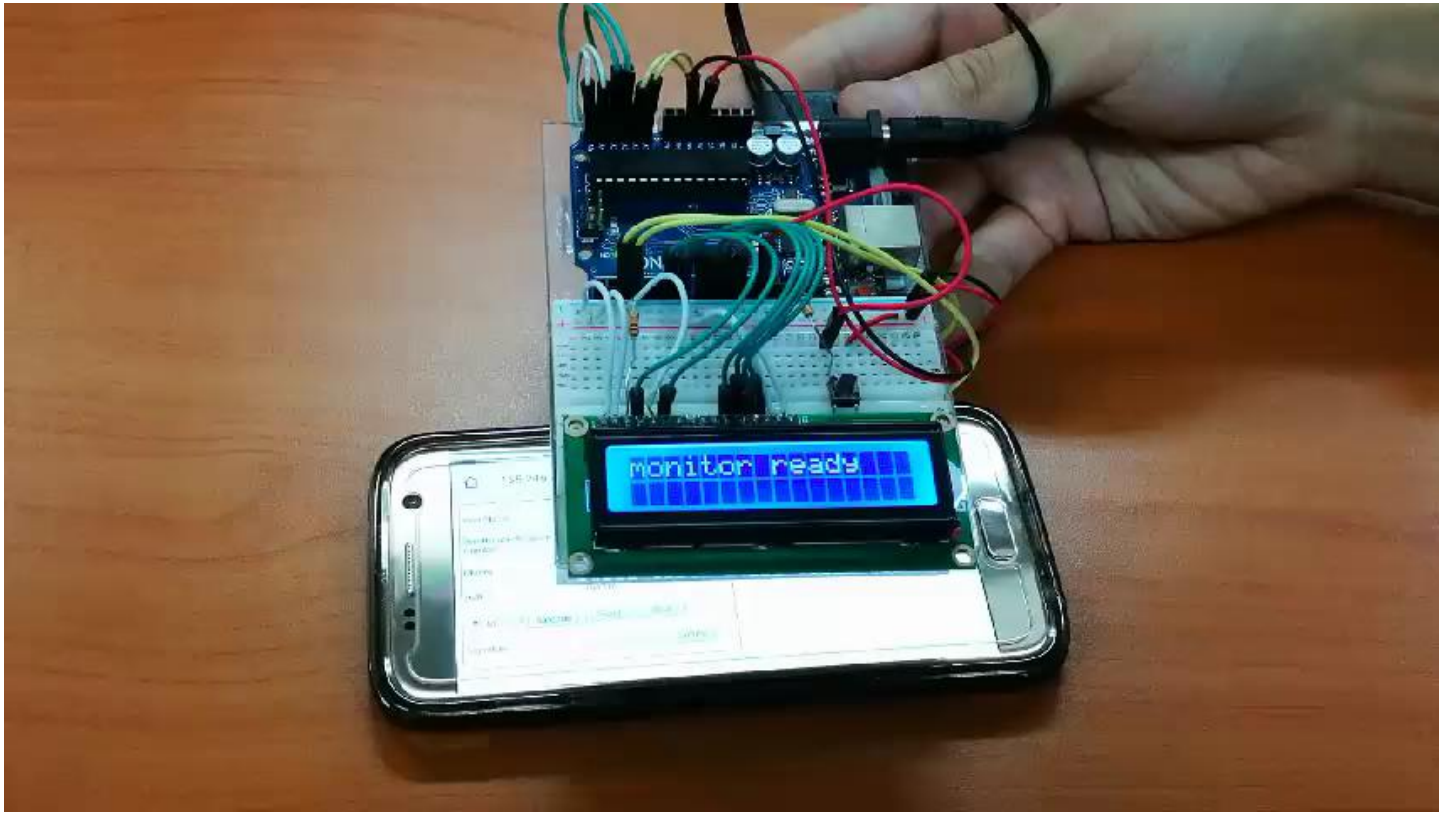
DIGITALSEAL

- Using DigitalSeal



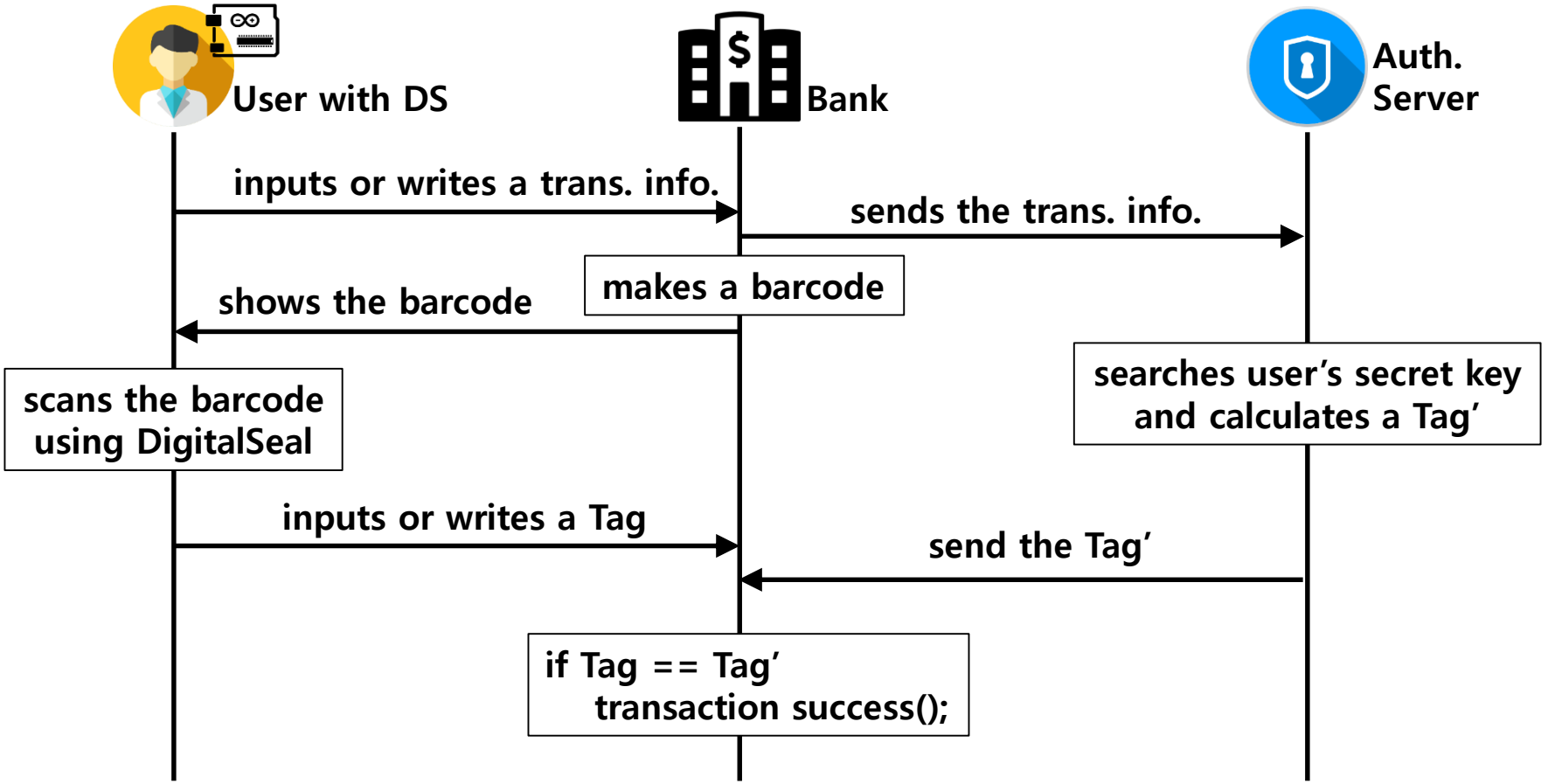
DIGITALSEAL

- Using DigitalSeal



DIGITALSEAL

- Using DigitalSeal



USER STUDY

USER STUDY

- **User Study**

monitor	participants	10
avg	success rates / scanning times	98% / 2.6s
paper	participants	10
avg	success rates / scanning times	94% / 3.2s

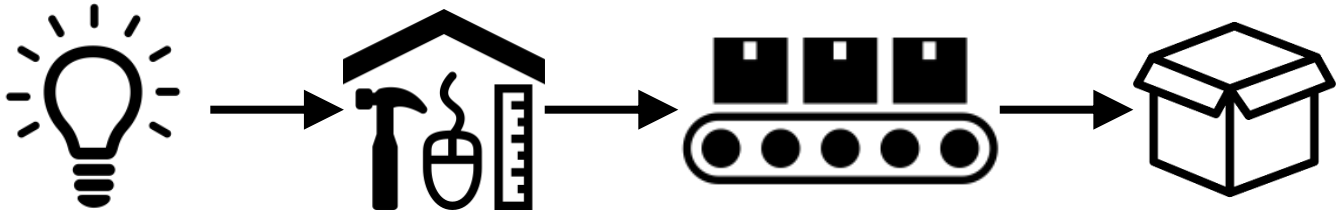
SECURITY AND COST ANALYSIS

SECURITY AND COST ANALYSIS

- **Security Analysis**
  - An attacker does not have a route to penetrate the device.
  - It is also strong against transaction fraud such as MitM and MitB attacks.
  - It is strong against replay attack.
  - It can reduce the forgeability of legal seal or signatures on paper.
  - Therefore, DigitalSeal can make more secure transactions as an authentication based on transaction information, not entity authentication.

SECURITY AND COST ANALYSIS

- **Cost Analysis**
  - **We expect that DigitalSeal can be implemented at a cost of about $1 USD when it is commercialized and manufactured with a mass production system (at scale).**



CONCLUDING REMARKS

CONCLUDING REMARKS

- **CONCLUDING REMARKS**
  - **We introduced DigitalSeal, a transaction authentication tool that works in both online and offline transactions.**
  - **DigitalSeal can scan the barcode included the transaction information on paper, computer monitors and smartphones.**
  - **We confirmed that DigitalSeal is usable and makes up the weak point of previous existing OTP.**
  - **In the future work, we will further explore other usability of DigitalSeal by large scale deployment, and ways to address unforeseen issues.**

Q & A

Thank you