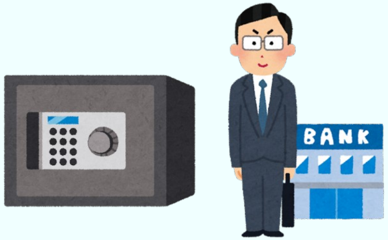
Contract Wallet using One time passward authentication/code payment UX.

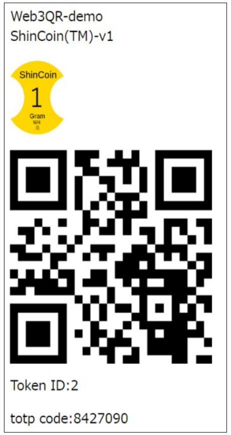
- ShinCoin Vault-

August 24 , 2023

SINGULION CORPORATION (8010001230232)

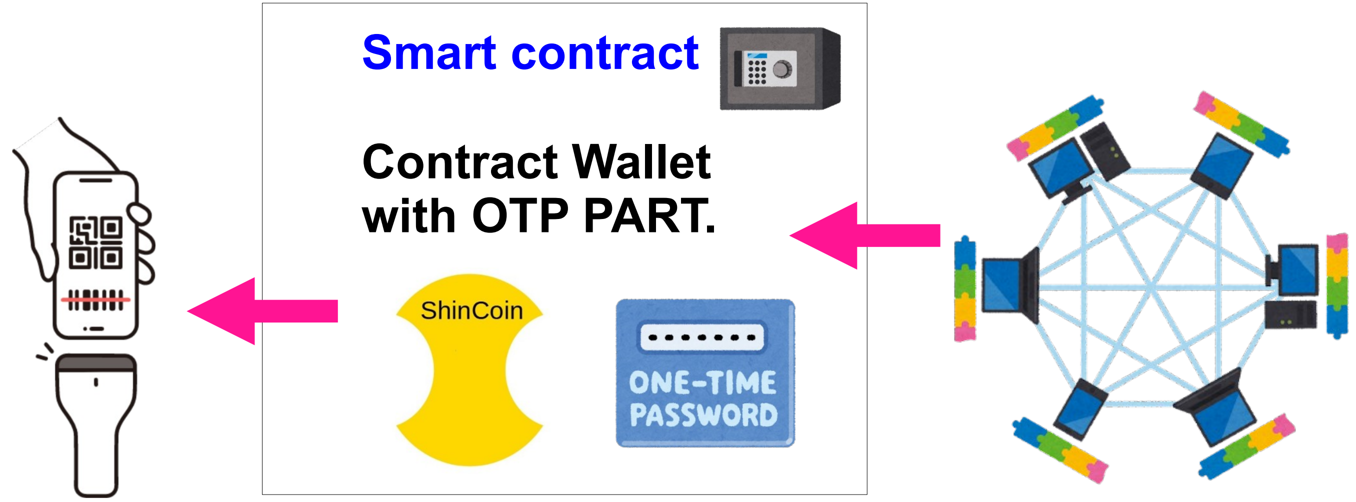
CEO Katsuya NISHIZAWA




Web3QR-demo
ShinCoin(TM)-v1

Token ID:2

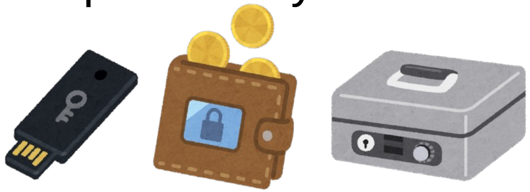
totp code:8427090

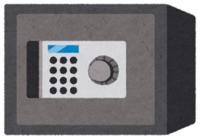

Smart contract

Contract Wallet with OTP PART.

<current wallet>
EOA and private key

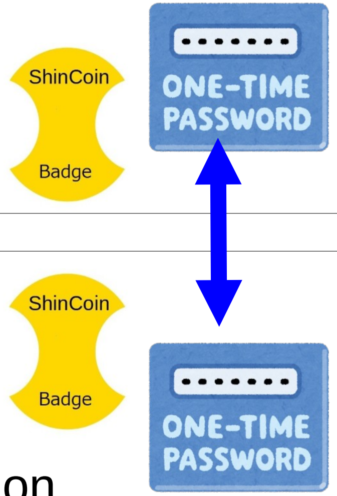
ID = private key = asset





<CAW/AA/ERC4337-CONTRACT>
Separation of keys and money.
ID ≠ private key ≠ asset.
Like a bank deposit in the name of the user?

We have onchain OTP solusion.
->Realize bank/vault like contracts with our OTP technology.

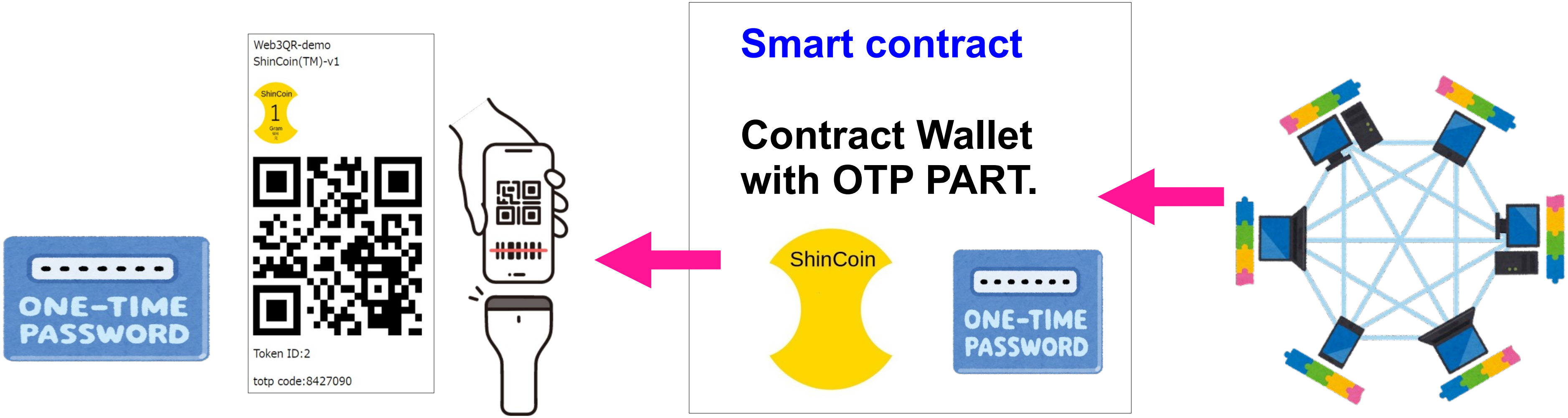


<EOA/private key>
Holding OTP token,
Have a digital ID.

OTP authentication,
Face-to-face code
authentication payment

Description

1. As a devtool, we provide an identity verification service using code authentication that is completed with WEB3.
(For the code authentication part, MPC is used to increase confidentiality.)



Web3QR-demo
ShinCoin(TM)-v1

Token ID:2

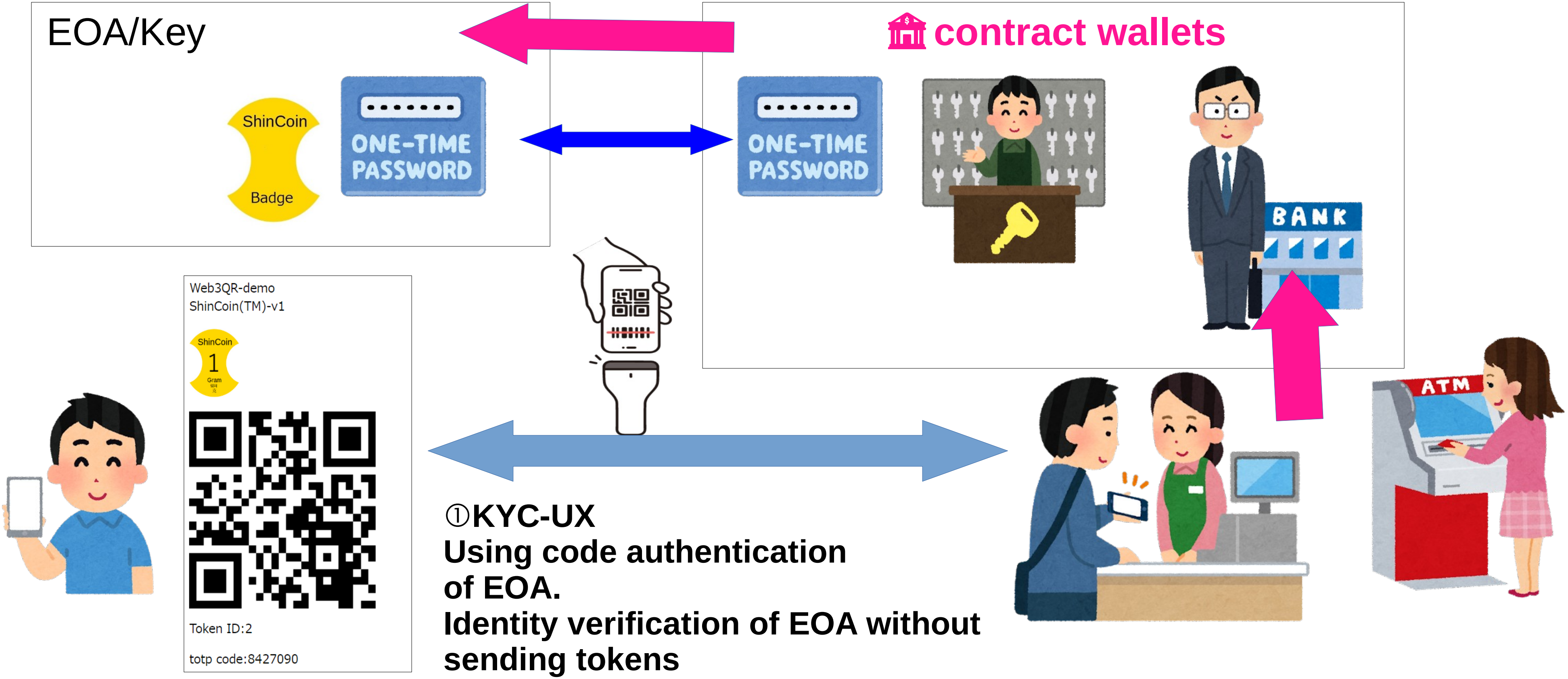
totp code:8427090

Smart contract

Contract Wallet with OTP PART.

OTP token issuance scheme for access in contract wallets

②After　STEP①,OTP token mint/Add



EOA/Key

contract wallets

Web3QR-demo
ShinCoin(TM)-v1

Token ID:2

totp code:8427090

①KYC-UX
Using code authentication of EOA.
Identity verification of EOA without sending tokens

https://singulion.net/qrUser/5500gen.html
https://singulion.net/qrUser/5500scan.html

2. When using a contract wallet, verify the identity of the wallet user “face-to-face” using code authentication.(Provides an easy and quick way to determine who is actually using the EOA and its private key)

3. Allow contract wallet users to pay using a code payment-like UX when paying with a wallet.(Increase the feeling of payment by eliminating the feeling of bank transfer)

[Security perspective]
Used to find out if the user in front of you really owns the NFT when reselling it at a secondhand store

Face-to-face NFT antiques trading and "Spoofing"

<Secondhand store>
(We are interacting face-to-face, but I'm worried)

<Manager of money laundering>
private key operations.
far away.Is it money laundering?

<Dark part-time job seller>
I don't have the private key, but I pretend to have sold it to an antique dealer under the direction of the manager.Name lending, face lending?

Therefore,
face-to-face NFT antiques trading
Seller impersonation
Our CPM certification to prevent.

<Secondhand store>
The NFT is moving on the smartphone of the person in front of me.

It is a holder who manipulates private keys and NFTs.
(Appearance, also recorded on security cameras)
Antique Dealer: Certainly, I was able to buy this person's possessions (items controlled by him) second-hand. So Let's remit the purchase price to this person's account / wallet.

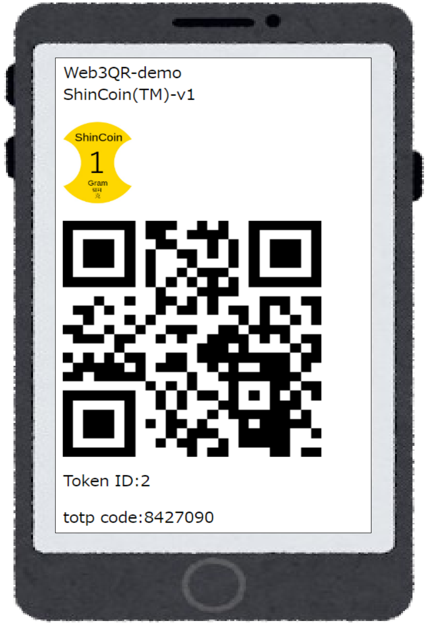
Challenges faced and Technology or Ideas used to solve them.

<Obstacles>
1.Culclating time variable otp code/value on smart contract/solidity
2.more random otp need oracle.
3.more secure/secret smart contract(OTP part and more , such as contract wallet part).

<Overcome>
1.Using blocknumber.
2.Using blockgaslimit value or value of node's voteing value.
3.Using technology such as MPC.(We want accsess such as SSS,MPC and more)

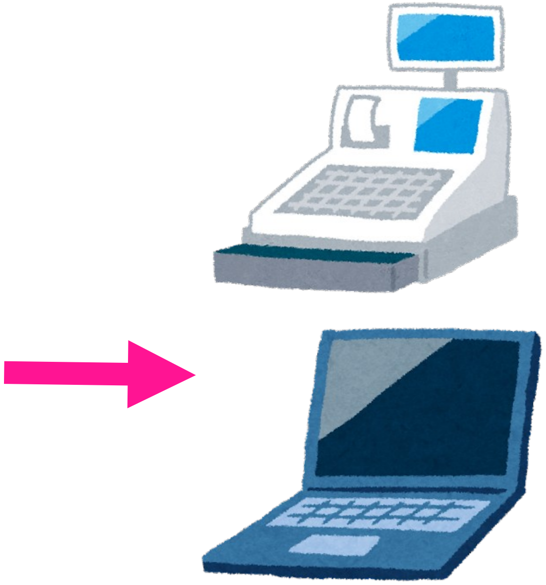
DEMO of OTP/CODE authentication
using my phone(OTP display) and my laptop(OTP reader)

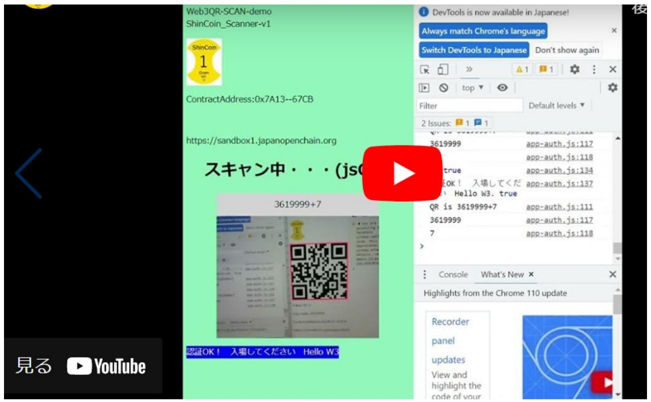
Block chain


Web3QR-demo
ShinCoin(TM)-v1

Token ID:2

totp code:8427090




Web3QR-SCAN-demo
ShinCoin_Scanner-v1

ContractAddress:0x7A13--67CB

https://sandbox1.japanopenchain.org

スキャン中・・・(js

3619999+7

認証OK！ 入場してください Hello W3

DevTools is now available in Japanese!

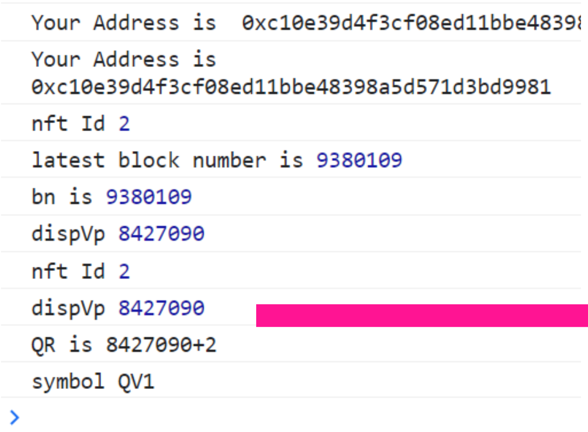
```
3619999                app-auth.js:117
                       app-auth.js:118
  true                 app-auth.js:134
 EOK！ 入場してくだ      app-auth.js:137
  Hello W3. true
QR is 3619999+7        app-auth.js:111
3619999                app-auth.js:117
7                      app-auth.js:118
```

Highlights from the Chrome 110 update

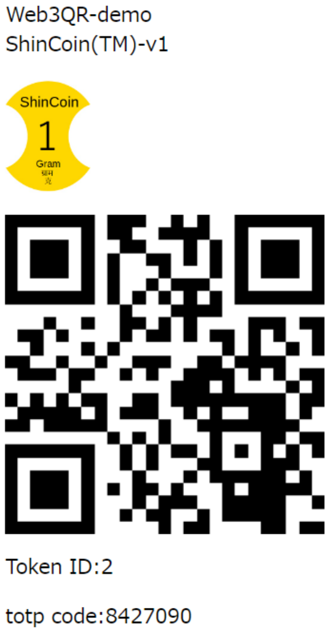
Recorder panel updates

View and highlight the code of your

<Appendix>



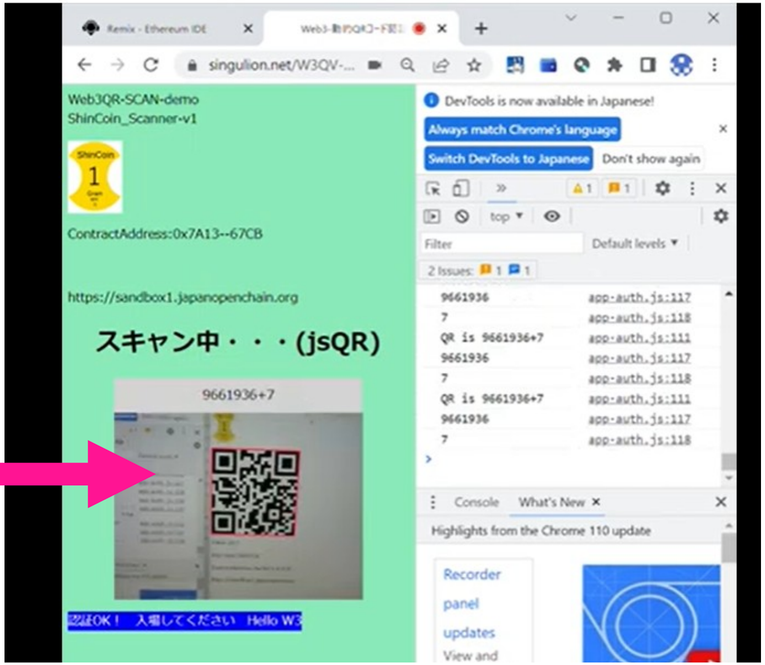
```
Your Address is  0xc10e39d4f3cf08ed11bbe48398
Your Address is
0xc10e39d4f3cf08ed11bbe48398a5d571d3bd9981
nft Id 2
latest block number is 9380109
bn is 9380109
dispVp 8427090
nft Id 2
dispVp 8427090
QR is 8427090+2
symbol QV1
>
```



Web3QR-demo
ShinCoin(TM)-v1

Token ID:2

totp code:8427090



Web3QR-SCAN-demo
ShinCoin_Scanner-v1

ContractAddress:0x7A13--67CB

https://sandbox1.japanopenchain.org

スキャン中・・・(jsQR)

9661936+7

認証OK！　入場してください　Hello W3

```
9661936            app-auth.js:117
7                  app-auth.js:118
QR is 9661936+7    app-auth.js:111
9661936            app-auth.js:117
7                  app-auth.js:118
QR is 9661936+7    app-auth.js:111
9661936            app-auth.js:117
7                  app-auth.js:118
>
```

Highlights from the Chrome 110 update