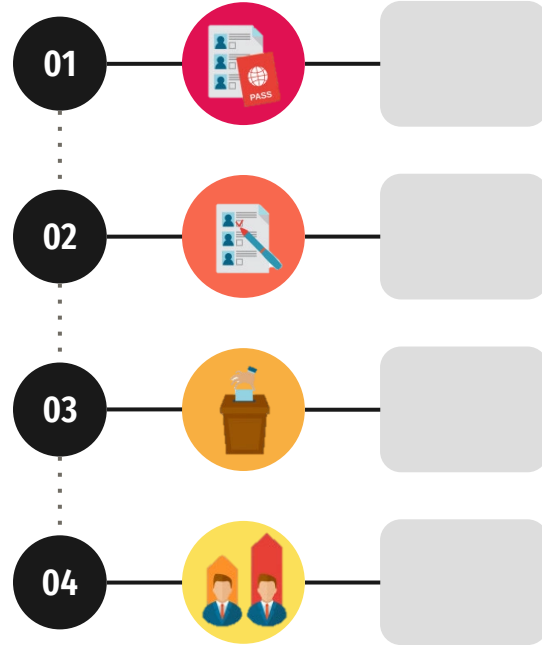


# ELECTION

E-voting blockchain solution



# Background

Traditional election



Blockchain solution

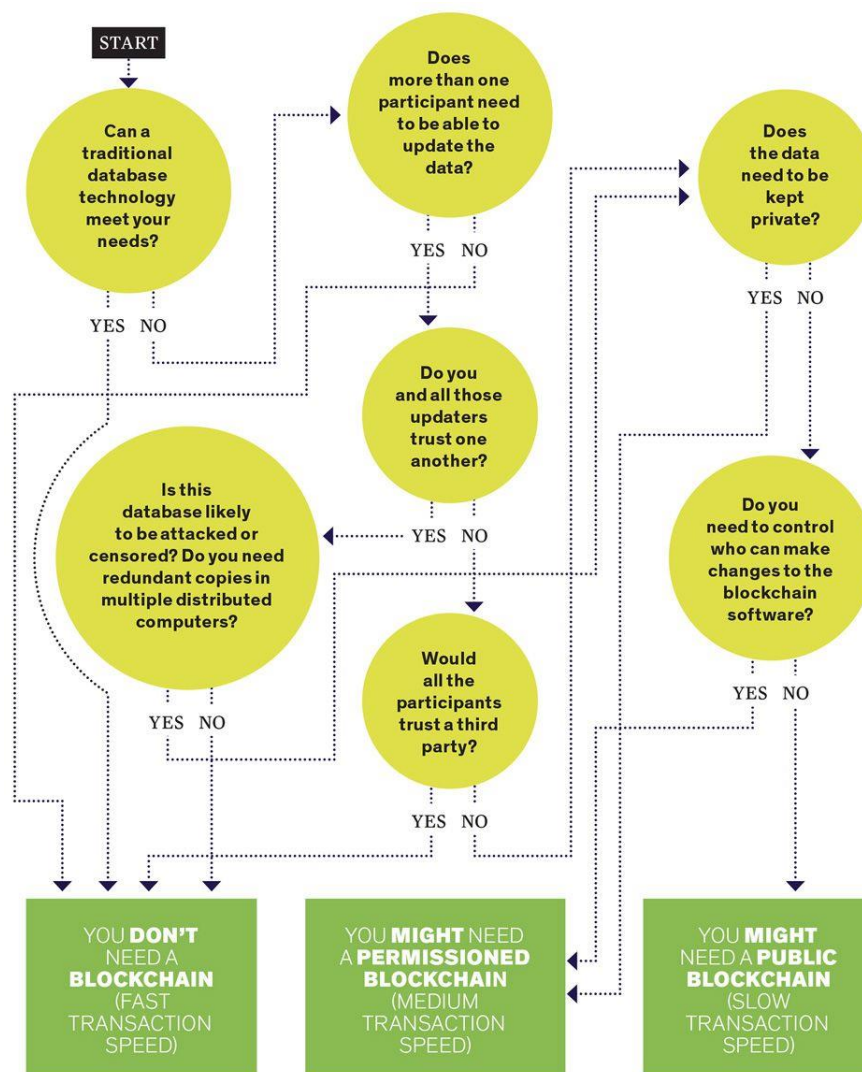


- Human error
- Corruption

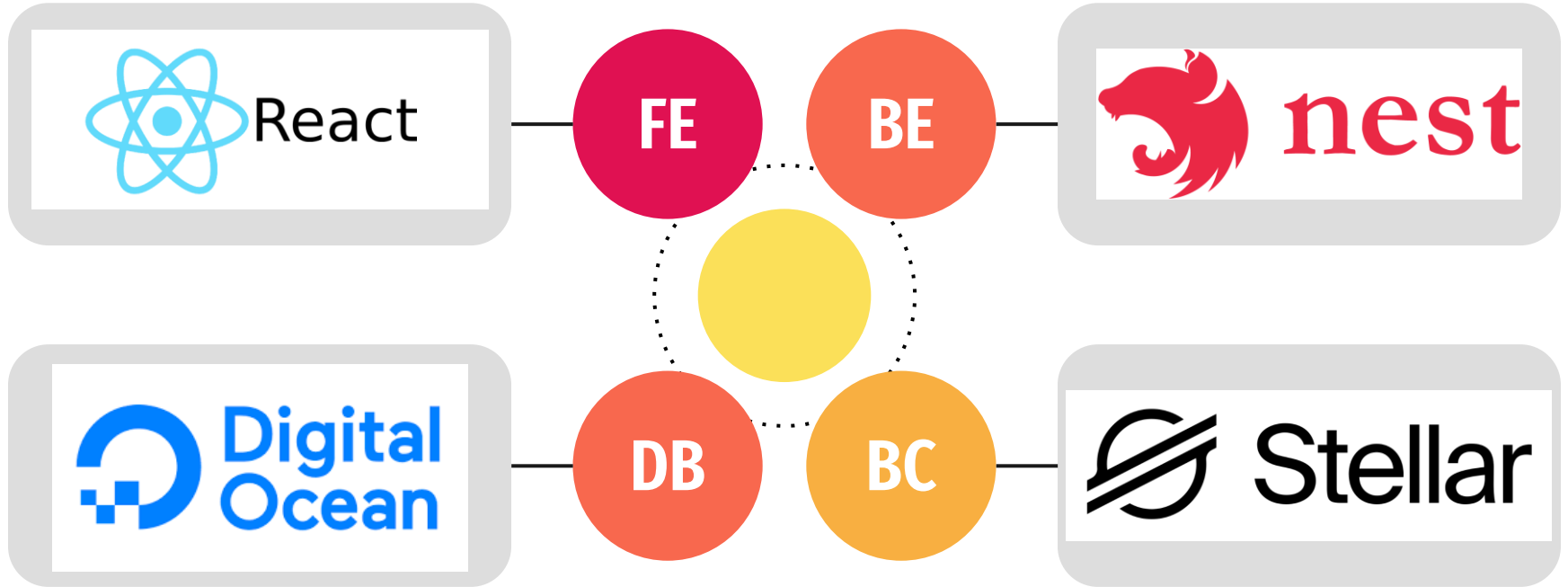


- Transparent
- Verifiable

# Why do we need blockchain



# Implementation



# Database



## Tables

### Gorv\_data

- Citizen ID and area that citizen can vote

### Candidate

- Candidate Info
- Candidate Account

### Issuer

- Issuer Account

# Roles



## Issuer

- Create election
- Create Coin and give to people
- Create candidate account



## People

- Verify Citizen ID
- Create account
- Vote candidate



## Candidates

- Register with issuer
- Get account from Issuer
- Wait for voting result

# Activity Flow

## Create Election

Create Issuer Account

01

Create Election

02

Add candidates

03

Recheck candidates information

04

Generate candidate account

05

Add information and account to database

06

Show information and account

07



### DashBoard

Issuer : None

Create Issuer

Create Election

Show Result

### DashBoard

Issuer : Created

Create Election

Show Result

account secret  
GBK6D2E2NJACIESHYRDJZN3KXPOY6YSIUB27AGJFHQ6GCSA SBMZYTEISFCJOBPCFTI5QCFLSQJCMNYQPIFKN7XJXJCYZ4WR

# Activity Flow

## Create Election

Create Issuer Account

01

Create Election

02

Add candidates

03

Recheck candidates information

04

Generate candidate account

05

Add information and account to database

06

Show information and account

07

\* ชื่อสนามเลือกตั้ง:

เลือกผู้แทนเขต

\* พื้นที่:

กรุงเทพ / บางกะปิ

ตกลง

ล้าง



# Activity Flow

## Create Election

Create Issuer Account

01

Create Election

02

Add candidates

03

Recheck candidates information

04

Generate candidate account

05

Add information and account to database

06

Show information and account

07

เลือกผู้แทนเขต พื้นที่ Bangkok เขต Payathai

หมายเลข 1

1112223334441

กันตภณ

ณ สงขลา

พรรค1



หมายเลข 2

1112223334442

ชยาพันธ์

กสิศเข็มทอง

พรรค2



+ เพิ่มผู้สมัคร

ตกลง

ล้าง

ย้อนกลับ

# Activity Flow

## Create Election

Create Issuer Account

01

Create Election

02

Add candidates

03

Recheck candidates information

04

Generate candidate account

05

Add information and account to database

06

Show information and account

07

### ตรวจสอบข้อมูล

1. ชื่อ กำนัน	นามสกุล ณ สงขลา	1112223334441	พรรค 1
2. ชื่อ ข้าราชการ	นามสกุล กสิดเขมทอง	1112223334442	พรรค 2

ย้อนกลับ

ถัดไป

# Activity Flow

## Create Election

Create Issuer Account

01

Create Election

02

Add candidates

03

Recheck candidates information

04

Generate candidate account

05

Add information and account to database

06

Show information and account

07

Execute Clear

Responses

Curl

```
curl -X 'GET' \
  'http://localhost:4000/stellar/createissuer' \
  -H 'accept: */*'
```

Request URL

http://localhost:4000/stellar/createissuer

Server response

Code	Details
200	<p>Response body</p> <pre>{   "account": "GB6LZQPMW4VETARYPTK112BEC3VFR3AQPC56U7HORYJOC2SKVM6ANI",   "secret": "S80BVP26KZFUNK2JFKXCV6H61K65GQ4F7XDZD5AOFKN31TRQTXOMQJLVD" }</pre> <p>Response headers</p> <pre>access-control-allow-origin: * connection: keep-alive content-length: 138 content-type: application/json; charset=utf-8 date: Wed, 24 Nov 2021 09:59:28 GMT etag: W/"8a-S8d8tteeIqn12kh/NS8+QhT750y4" keep-alive: timeout=5 x-powered-by: Express</pre>

Responses

Code	Description	Links
200		No links

## Activity Flow

## Create Election

## Create Issuer Account

01

## Create Election

02

## Add candidates

03

## Recheck candidates information

04

## Generate candidate account

05

## Add information and account to database

06

Show information and account

07

	citizenId	first_name	last_name	major_area_id	major_area_name	party	wallet_ad
1	1112223334442	ชยาเนห์	กสิดเข็มทอง	2	Payathai	พรรค2	GBIVFOGXBS
2	1112223334441	กันตภณ	ณ สงขลา	2	Payathai	พรรค1	GAWLBR67JE

# Activity Flow

## Create Election

Create Issuer Account

01

Create Election

02

Add candidates

03

Recheck candidates information

04

Generate candidate account

05

Add information and account to database

06

Show information and account

07

### ผลการสร้าง

1. ชื่อ ก็นดกณ นามสกุล ณ สงขลา 1112223334441 พรรค1

Address: GAWLBR67JE0BSQA74XOZHG7HQSNAHU3SEDIL434IZI3PFDE3EYQDUAMH

2. ชื่อ ชยานันท์ นามสกุล กสัดเข็มทอง 1112223334442 พรรค2

Address: GBIVFOGX85ZPCGMTXZHVUN5A2DYX43VKPKXMFOMDKGEFAK7QWUNYJ2W7

ตกลง

# Activity Flow

## Voting

Verify Citizen ID

01

Check available voting area

02

Create wallet and get coin

03

Choose candidate and vote

04

Show vote result

05

Show voting summary

06

### กกต

- 1 เช็กสิทธิ์  
ผู้มีสิทธิออกบัตรประชาชน  
เพื่อลงคะแนน
- 2 เช็กใบมีมติ  
ผู้มีสิทธิออกบัตรประชาชน  
มีใบมีมติออกบัตร  
ลงคะแนน
- 3 สร้างกระเป๋าเงิน  
ตัวประชาชน
- 4 ลงคะแนน  
ลงคะแนนเมื่อได้รับบัตร  
ลงคะแนน
- 5 แสดงผล  
แสดงผลการลงคะแนน  
ออกบัตร

กรอกเลขบัตรประชาชนเพื่อเช็กสิทธิ์

\* เลขบัตรประชาชน

7897897897897

ค้นหา

# Activity Flow

## Voting

Verify Citizen ID

01

Check available voting area

02

Create wallet and get coin

03

Choose candidate and vote

04

Show vote result

05

Show voting summary

06

กกต



การเลือกตั้งที่ท่านมีสิทธิ์ในการลง  
คะแนน

1. ท่านมีสิทธิ์ลง Payathai

2. ท่านมีสิทธิ์ลง Bangkok

	🔍 citizen_id 🔼🔼	🔍 area_name 🔼🔼	🗳 isvote 🔼🔼
1	7897897897897	Payathai	[ ]
2	7897897897897	Bangkapi	[ ]

# Activity Flow

## Voting

Verify Citizen ID

01

Check available voting area

02

Create wallet and get coin

03

Choose candidate and vote

04

Show vote result

05

Show voting summary

06

กกต

✓ เริ่มต้น  
ตรวจสอบและยืนยันตัวตน  
ประชาชน

✓ ตรวจสอบสิทธิ์  
ตรวจสอบสิทธิ์การลง  
คะแนน

1 สร้างกระเป๋าเงิน  
สร้างกระเป๋าเงิน

4 ลงคะแนนเสียง  
ลงคะแนนเสียง

สร้างกระเป๋าเงิน

\* เลขบัตรประชาชน  
7897897897897

\* เลขมือถือประชาชน  
09123456789

\* รหัสผ่านกระเป๋าเงิน  
\*\*\*\*\*

สร้าง

```
},
"balances": [
  {
    "balance": "1.0000000",
    "limit": "1.0000000",
    "buying_liabilities": "0.0000000",
    "selling_liabilities": "0.0000000",
    "last_modified_ledger": 1151591,
    "is_authorized": true,
    "is_authorized_to_maintain_liabilities": true,
    "asset_type": "credit_alphanum12",
    "asset_code": "Payathai",
    "asset_issuer": "GBK6D2E2NJACIESSHYRDJZN3KXPOYGYSIUB27AGJFHQ6GCSAHGUSIKRC"
  }
],
{
```



# Activity Flow

## Voting

Verify Citizen ID

01

Check available voting area

02

Create wallet and get coin

03

Choose candidate and vote

04

Show vote result

05

Show voting summary

06

กกต



ท่านต้องการลงคะแนนให้ผู้สมัครเลือก  
ตั้งท่านใด

1		ชมานันท์ กลัดเข็มทอง	พรรค2
2		กันตภณ ณ สงขลา	พรรค1

# Activity Flow

## Voting

Verify Citizen ID

01

Check available voting area

02

Create wallet and get coin

03

Choose candidate and vote

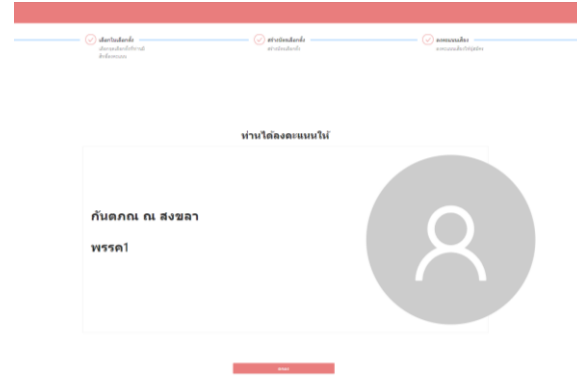
04

Show vote result

05

Show voting summary

06



```

"balances": [
  {
    "balance": "1.0000000",
    "limit": "922337203685.4775807",
    "buying_liabilities": "0.0000000",
    "selling_liabilities": "0.0000000",
    "last_modified_ledger": 1151687,
    "is_authorized": true,
    "is_authorized_to_maintain_liabilities": true,
    "asset_type": "credit_alphanum12",
    "asset_code": "Payathai",
    "asset_issuer": "GBK6D2E2NJACIESSHYRDJZN3KXP0Y6YSIUB27AGJFHQ6GCSAHGUSIKRC"
  },
  {
    "balance": "0.0000000",
    "limit": "922337203685.4775807",
    "buying_liabilities": "0.0000000",
    "selling_liabilities": "0.0000000",
    "last_modified_ledger": 1151687,
    "is_authorized": true,
    "is_authorized_to_maintain_liabilities": true,
    "asset_type": "credit_alphanum12",
    "asset_code": "Payathai",
    "asset_issuer": "GBK6D2E2NJACIESSHYRDJZN3KXP0Y6YSIUB27AGJFHQ6GCSAHGUSIKRC"
  }
]
```

# Activity Flow

## Voting

Verify Citizen ID

01

Check available voting area

02

Create wallet and get coin

03

Choose candidate and vote

04

Show vote result

05

Show voting summary

06

### ผลคะแนนการเลือกตั้ง

\* พื้นที่: กรุงเทพมหานคร

ย้อนกลับ

แสดง



ชยานันท์ กัลดะเข็มทอง  
พรรค2

0 คะแนน



กันตกรณ สงขลา  
พรรค1

2 คะแนน

```
"/balances": [  
  {  
    "balance": "2.0000000",  
    "limit": "922337203685.4775807",  
    "buying_liabilities": "0.0000000",  
    "selling_liabilities": "0.0000000",  
    "last_modified_ledger": 1151724,  
    "is_authorized": true,  
    "is_authorized_to_maintain_liabilities": true,  
    "asset_type": "credit_alphanum12",  
    "asset_code": "Payathai",  
    "asset_issuer": "GBK6D2E2NJACIESSHYRDJZN3KXPOY6YSIUB27AGJFHQ6GCSAHGUSIKRC"  
  },  
]
```

# Stellar Implementation

## Create Wallet

Generate Key Pair with citizen ID, laser ID, password

```
getKeyPair(UserWallet: CreateUserWallet) {  
  const citizenId = UserWallet.citizenId  
  const backCard = UserWallet.backCard  
  const password = UserWallet.password  
  const temp = citizenId + backCard + password  
  const seed = StellarSdk.StrKey.encodeEd25519SecretSeed(temp).substring(0,32)  
  const keyPair = StellarSdk.Keypair.fromRawEd25519Seed(seed);  
  return keyPair;  
}
```

Add fund to account

```
async addFund(account: string) {  
  return await axios.get("/friendbot", {  
    baseUrl: 'https://horizon-testnet.stellar.org',  
    params: { addr: account }  
  })  
}
```

Generate Key Pair with random

```
async createIssuer() {  
  const keyPair = StellarSdk.Keypair.random();  
  const secret = keyPair.secret();  
  const account = keyPair.publicKey();  
}
```



STELLAR LUMENS

# Stellar Implementation

## Create Coin and trust coin

### Issue new coin

```
const coin = new StellarSdk.Asset(coinName, issuer);
```

```
async trust(account: string, coin, secret) {  
  server  
  .loadAccount(account)  
  .then(function (receiver) {  
    var transaction = new StellarSdk.TransactionBuilder(receiver, {  
      fee: 100,  
      networkPassphrase: StellarSdk.Networks.TESTNET,  
    })  
    .addOperation(  
      StellarSdk.Operation.changeTrust({  
        asset: coin,  
      })),  
    )  
    .setTimeout(100)  
    .build();  
    transaction.sign(secret);  
    return server.submitTransaction(transaction);  
  })  
  .then(console.log)  
  .catch(function (error) {  
    console.error("Error!", error);  
  });  
}
```

### Trust Coin

- Make wallet trust new issued coin. So, the coin can be used by the wallet
- Limit can be added to trust to limit how much the wallet can keep the coin. If the limit is set to 0 then the wallet will untrust the coin
- Limit is max int64 by default

# Stellar Implementation

Create Coin and trust coin



# Stellar Implementation

## Send coin

```
async sendCoin(account, secret, coin, destination) {
  server
    .loadAccount(account)
    .then(function (voter) {
      var transaction = new StellarSdk.TransactionBuilder(voter, {
        fee: 100,
        networkPassphrase: StellarSdk.Networks.TESTNET,
      })
      .addOperation(
        StellarSdk.Operation.payment({
          destination: destination,
          asset: coin,
          amount: "1",
        }),
      )
      .addOperation(
        StellarSdk.Operation.changeTrust({
          asset: coin,
          limit: "0",
        }),
      )
    )
    .setTimeout(100)
    .build();
  transaction.sign(secret);
  return server.submitTransaction(transaction);
}
```

## Send Coin

- Send coin to destination wallet
- The transaction will fail if the destination wallet doesn't trust the coin

# Stellar Implementation

## Get Balance

```
async getBalance(account: Account) {  
  const sAccount = await server.loadAccount(account.account);  
  const balance = parseInt(sAccount.balances[0]["balance"]);  
  return balance;  
}
```

## Get Balance

- Will return all coins in the wallet

```
{  
  "balance": "2.0000000",  
  "limit": "922337203685.4775807",  
  "buying_liabilities": "0.0000000",  
  "selling_liabilities": "0.0000000",  
  "last_modified_ledger": 1151724,  
  "is_authorized": true,  
  "is_authorized_to_maintain_liabilities": true,  
  "asset_type": "credit_alphanum12",  
  "asset_code": "Payathai",  
  "asset_issuer": "GBK6D2E2NJACIESSHYRDJZN3KXPOY6YSIUB27AGJFHQ6GCSAHGUSIKRC"  
},  
{  
  "balance": "9999.9999900",  
  "buying_liabilities": "0.0000000",  
  "selling_liabilities": "0.0000000",  
  "asset_type": "native"  
}
```



# Concern

## Real-time score

เนื่องจากการโหวตโดยใช้ Blockchain ทำให้ข้อมูลการโหวตทั้งหมดเป็น public และสามารถดูแบบ real-time ได้ ซึ่งสามารถนำไปสู่การชักจูงได้

วิธีการแก้ปัญหาคือ ไม่เปิดผลโหวตแบบ real-time ณ จุดลงคะแนนเลือกตั้ง เพื่อไม่ให้เกิดการชักจูง

## Identifiable Private Key

เนื่องจากการสร้าง wallet account จะใช้ ed25519 ในการ hash รหัสบัตรประชาชน, เลขหลังบัตร, และ รหัสผ่าน เพื่อใช้เป็น private key ดังนั้นหากรู้ข้อมูลเหล่านี้จะสามารถระบุได้ว่าเจ้าของ wallet โหวตใครไป ซึ่งอาจนำไปสู่ปัญหาการซื้อเสียงที่สามารถยืนยันได้

# Concern

## Duplicate coin

เนื่องจาก Issuer หรือคนออกเหรียญสามารถออกเหรียญให้เหรียญโดยไม่จำเป็นต้องมีเหรียญของตนในบัญชีได้ ดังนั้นกรณีที่ถูกรู้ key ของ Issuer จะทำให้เกิดการส่งเหรียญให้กับผู้สมัครได้

วิธีการแก้คือ ให้ Issuer สร้างเหรียญและส่งไปยัง account สนามเลือกตั้งตามจำนวนผู้มีสิทธิเลือกตั้งในพื้นที่นั้น ๆ จากนั้นในการขอเหรียญของ ประชาชน จะขอจาก account สนามเลือกตั้งแทน

## Delay

เนื่องจากในการโหวตใช้ Blockchain ทำให้ในการสร้าง account, การโอนเหรียญจะต้องใช้เวลาในการ validate ทำให้มี delay เกิดขึ้น