



Version 2020-07-22
gufmar@gmail.com

This is a concept description, with overviews of the three basic action areas and the data flow. Detailed data formats, processes and schemas follow

ITN Pool Owners

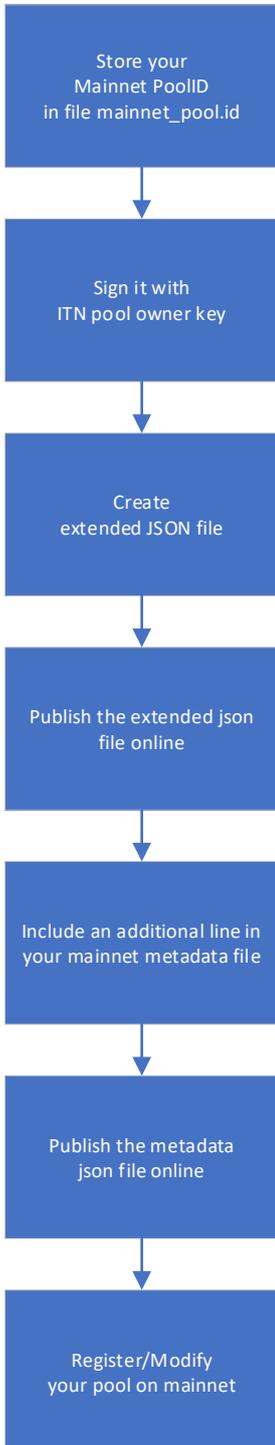
Pre-requisites (stored in <files>)

Your Mainnet PoolID

Your ITN Pool owner
secret key
ed25519_sk1...

Your ITN Pool owner
public key
ed25519_pk1...

Examples



```
1caa23f3c2f2cddcd60510b01750e7aac16feb077fa0aae148d22cfa
```

```
jcli key sign --secret-key <owner.skey> <mainnet_pool.id> --output  
<mainnet_pool.sig>  
  
cat mainnet_pool.sig  
ed25519_sig1sn32v3zdvhwdwq493nd318x7mvsm3anz4jzmv7aefw32kvn3kgdvrl  
a6s6qx8anyqmvnq2v0d7xeq2fu64549vurvpfuncr4d72rg7rc6gs
```

```
{  
  "itn": {  
    "owner": "ed25519_pk1....",  
    "witness": "ed25519_sig1...."  
  }  
}
```

<https://www.mypool.com/extended-metadata.json>

```
{  
  "name": "My Pool",  
  "ticker": "ABCDE",  
  "description": "whatever, the whole file cannot exceed 512bytes",  
  "homepage": "https://www.mypool.com",  
  "extended": "https://www.mypool.com/extended-metadata.json"  
}
```

<https://www.mypool.com/metadata.json>

Result:

ITN Pool operators publish an extended metadata file containing the proof of ownership

Metadata Proxies

Pre-requisites

Pools registered on chain
with published
extended metadata

Jormungandr node
running in explorer mode
OR
CardanoFoundations's
stake-pool-registry repository

SMASH
or other processor

Examples



```
PoolID: 1caa23f3c2f2cddcd60510b01750e7aac16feb077fa0aae148d22cfa  
Metadata URL: https://www.mypool.com/metadata.json  
Metadata Hash: 2ecfcb903544e6.....02877872ff2d2fe195bf02c
```

```
{  
  "name": "My Pool",  
  "ticker": "ABCDE",  
  "description": "whatever, the whole file cannot exceed 512bytes",  
  "homepage": "https://www.mypool.com",  
  "extended": "https://www.mypool.com/extended-metadata.json"  
}
```

```
{  
  "itn": {  
    "owner": "ed25519_pk1....",  
    "witness": "ed25519_sig1...."  
  }  
}
```

```
jcli key verify --public-key <owner.pub> --signature <witness.sig>  
<mainnet_poolID.txt>  
  
(ITN owner public key and Ticker from CF's stakepool registry repo)
```

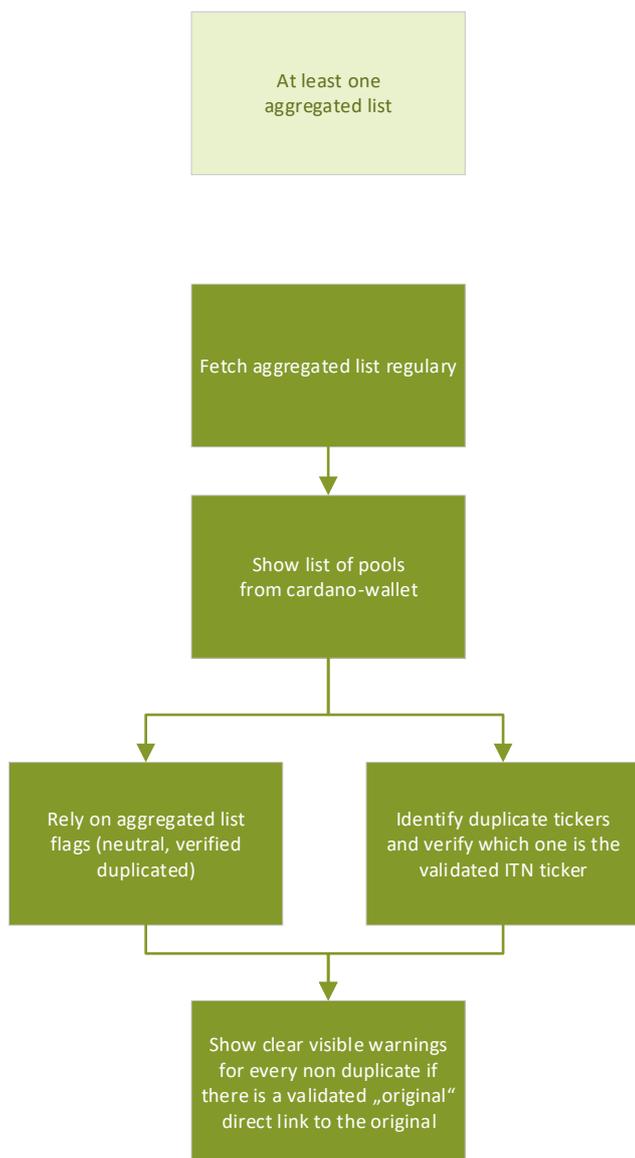
```
{  
  "validated_tickers": [ {  
    "ticker": "ABCDE",  
    "poolID": "1caa23f3c2f2cddcd6...b077fa0aae148d22cfa",  
    "status": "verified"  
  }  
 ]  
}
```

Result

Aggregated list of validated ownerships

ToDo: Applications (Wallets, Explorers, MobileApps,...)

Pre-requisites



Result

Wallet delegations centers show clear warnings for duplicate Tickers, when an original proof of ownership is published