

Riddle & Code

LIBRDDL SDK

Table of Contents

1 DESCRIPTION.....	3
2 SOFTWARE ARCHITECTURE	4
3.1 API FUNCTIONS.....	4
3 TESTS	7

Table of Figures

Figure 1: General System Overview	4
Figure 2: flowchart of runRDLLNotarizationWorkflow function	5
Figure 3: Message for Trusted Anchor that has not registered the network.....	7
Figure 4: Registration Request for Trusted Anchor	7
Figure 5: Sending coin to the device.....	8
Figure 6: Registiration of Seed	9
Figure 7: Data Transaction into RDDDL Network.....	9

1 DESCRIPTION

This document includes usage method, software architecture and test results of RDDDL SDK.

< What is RDDDL SDK? Purpose of RDDDL SDK>

< Mention libRDDDL repo >

< Mention Planetmint and Liquid>

2 SOFTWARE ARCHITECTURE

Figure 1 indicates library structure. The library consists of 3 layers:

- ⑩ libRddlAPI: This layer includes user functions.
- ⑩ libRddlAbst: This layer includes hardware specific functions
- ⑩ libRddl: This layer includes common software function which are platform independent.

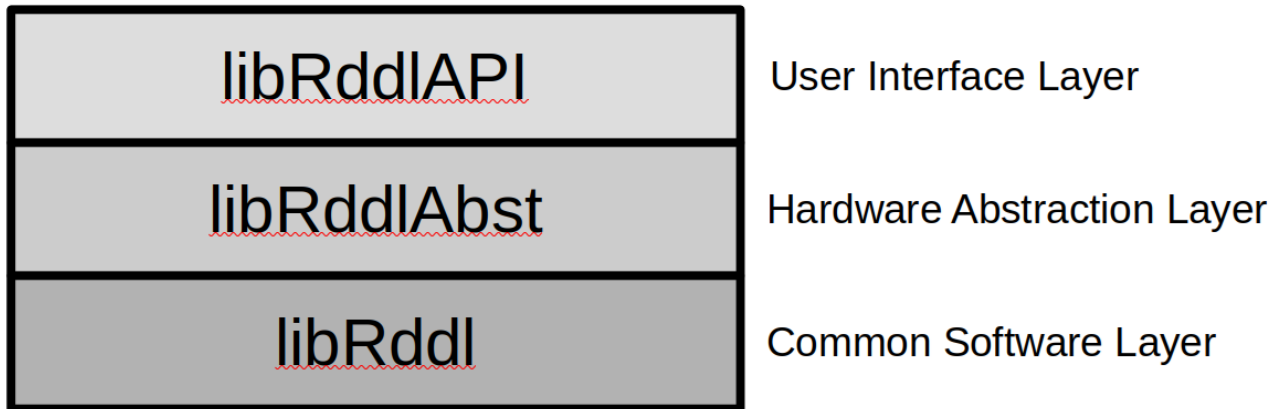


Figure 1: General System Overview

3.1 API FUNCTIONS

User can call libRddlAPI functions to use the library:

void runRDDLNotarizationWorkflow(const char* data_str, size_t data_length): This function has two separate tasks. If the device is registered to the network, it creates a transaction using the given data and broadcasts it. If the device is not registered to the network, it creates a registration transaction and broadcasts it. Figure 2 gives flowchart of this function.

The getPlntmntKeys function prepares public and private keys to be used in other functions. It generates the master key from the seed stored in the device. It generates planetmint keys from masterkey with the following derivation path /44'/8680'/0'/0/0 and liquid keys from /44'/1776'/0'/0/0. It also derives the public key from the private key embedded in the machine.

The hasMachineBeenAttested function checks whether the device has been registered before by querying https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key. It uses the planetmint external public key for the query which is serialized of planetmint node with PLANETMINT_PMP version.

The registerMachine function creates a message in the google protobuf structure containing machine information. This machine information includes the generated public keys, the machine's domain and device information.

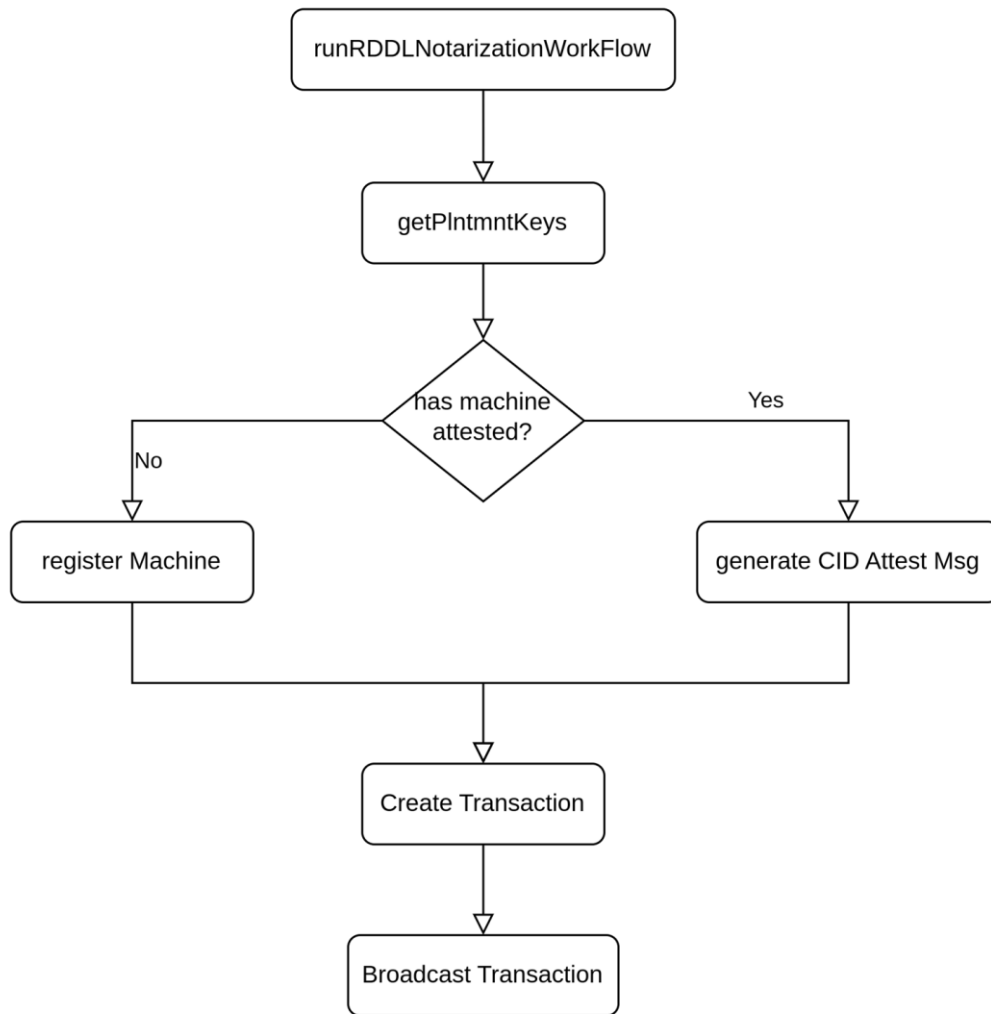


Figure 2: flowchart

of *runRDDLLNotarizationWorkflow* function

The create transaction function prepares the transaction using the generated message in the google protobuf structure, planetmint keys, denom, sequence, chain id and account id. Denom and chain-id information are retrieved from the device. If it is not saved in the device, default values are used which are plmnt and planetmint-testnet-1 respectively. Sequence and account id information is retrieved by querying https://testnet-api.rddl.io/cosmos/auth/v1beta1/account_info/. The hash160 version of the planetmint public key is used for this query. If the query returns negative, information is retrieved from the device. If it is not saved in the device, default values are used which are 0.

Finally, broadcast transaction function sends the created transaction to <https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs> address.

char* sdkSetSeed (**char*** pMnemonic, **size_t** len): Generates seed for the device from the given mnemonic. If a mnemonic is not given, it generates itself. Returns the used mnemonic.

void sdkStoreSeed (**char*** new_seed): Writes the seed to the non-volatile memory of the device. If new_seed is NULL, it writes the seed produced by sdkSetSeed function. If it is not NULL, it writes the value in new_seed.

void sdkReadSeed (**char*** seed_arr, **int*** seed_size): Returns embedded seed value and it's size. The size of seed is currently 64 bytes.

3 TESTS

Compile library with following command on the project directory. It will also generate test executable.

```
bash build.sh
```

To run test code, use following command on the project directory:

```
bash runTest.sh
```

If the test device is not registered to the network, the following errors will be received when the test program is run.

```
Fatih@Fatih-ThinkPad-L480: ~/Desktop/RiddleNetwork/Repos/rddl-sdk/build$ ./test/testRddlSDK
Machine Public Key: 03FD11A9F8E0203025CF3418822EE4F8C593CF80A8EC9C34FF920A6261A66F473C

curl -X GET "https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key/pmpb7u0ZMFAM4TrgEqYrYoAHvx2Gegw5hERKCewaVl3t7QCntXAGfVfswR8DDe968Y
mLV4XTfXUfMmrtsH7XB8VHAaBCxWcjZEJ5yufilfsZu8Cd" -H "accept: application/json"
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 53 100 53 0 0 52 0:00:01 0:00:01 0:00:01 52
{"code":5,"message":"machine not found","details":{}}
Register: Machine
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 119 100 119 0 0 203 0:00:01 0:00:01 0:00:01 203
ERROR readfile! Couldnt open file ./machinecid{"info":{"address":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","pub_key":null,"account_number":"58","s
equence":"0"}}
ERROR readfile! Couldnt open file ./planetmintdenomERROR readfile! Couldnt open file ./planetmintchainid
curl -X POST "https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs" -H "accept: application/json" -H "Content-Type: application/json" -d '{"tx_bytes": "C
sIFCr8FcYvcGxhbmV0bWludGdvLn1hY2hpbmUuTXNnQXR0ZXN0TFJgaGluZkRlZkR0QscGxtbnQxcXY2azVzdDU5a3p0Nmp1cmRrYzQzeGRuZHBkeng2d3J6cHN2d3Y54wQKLHBsbW50MXF2Nms1c3Q1
OWt6dZqdZk2M0N3hkbmRwZHp4NndyenBzdnY2G9sYWIucjNjLn5ldHdvcmsoATAIOM9wbXBIN3VEWk1GQU06VHJnRXFyWw9BSHZ4Mkd1Z3c1aEVSS0NLV2FwaTN0N1FDbnRYQUdmVnZzd1I4RGR
FOTZChw1MwJrYVY2YVZmZnN0XJ0c0g3WE14VkhBYUJDaFjdjalpFS1N5dmZpTGZzWnVCY8RCb3hwdH12R1NRVnFtaHxZzh1XUTc1TLZwcHBKszJxdU51VWVvRkd0MmtucmJnVnltVGtva2ZyNE5DZEJBU3
Q5OUZCR3NYkSMN0RzVEFOw2MeGpZcGRVejFRU3RVTrJaM2cyRU5xRDFCakFhUWQ2c0pCMNCRDExQTLCOEUWnjazMD11Q0YzNDE4ODIyRUU0RjhDNTkzQ0Y4MEE4RU50Zm9RkY5MjBBNjI2MUE2N
KX0NzNDUKUSL3sitWfudwZhy3R1cnVyiJogTlJfEREwLLCJTZXJpYwI0JvdGhlcnNlcmh0Cj9h3711Z1cnNpb241OIAIMC4xIn1YAwKAALVBMtBBMjRJCQUCMDfGNTJDRUJGNTk1Q0ExRkRREMET1
QjUwOUJrZjdGQzZmMUU0MzdFRDLEOTg0RUJ0E0KRBNTHyM0Q5MDE0E0TixRdEdH2NGMkU0MEY5RUVDOTZDREJCQzAyRDI5OUNDMZCZHUQ2QUY4M0NDOTMwRjBFRkFCOTgzaXwbG1udDFxdjZrNXN0NTl
renQ2anVyzGtjNDN4ZG5kcGR6eDZ3cnpcw3Z2NhJlck4KRgofL2Nvc21vcy5JcnldG8uc2VjCDI1NmSL1B1YktleRIjclECXp6di2ieANXPie8p0owRbZi5zGyONrFG4S12QTOCM4SBAoCCAESA
oKcGvmbG1udBIBMHdAngwaQlyKeSn3YZfPpHxkxsp9059jbrZLaGvTYJoXP3zwREUUNdHAlDXqOx+PRB2h0FJhvwR1L3TqUqBvVBrWw4kfk=","mode":"BROADCAST_MODE_SYNC"}'
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1523 100 306 100 1217 519 2064 0:00:01 0:00:01 0:00:01 2585
CURL RESPONSE:
{"tx_response":{"height":"0","txhash":"30B499EDC39AAB5DAD1E0E83CE4301230B2A9470A2D365F8DDFB088B8720C1B9","codespace":"machine","code":3,"data":"","raw
_log":{"error during CheckTx or ReCheckTx: trust anchor not found","logs":[],"info":"","gas_wanted":"0","gas_used":"0","tx":null,"timestamp":"","events":
[]}}
/home/fatih/Desktop/RiddleNetwork/Repos/rddl-sdk/test/testRddlSDK.c:55: testNotarizationFlow:PASS
```

Figure 3: Message for Trusted Anchor that has not registered the network

The first message in the red frame indicates that the seed of device is not registered to the network. Second one indicates that the Trusted Anchor used is also not known by the network. Note that Trust Anchor's private key is embedded in the code. If it will be used as a different device, it must be changed. It is called `private_key_machine_id` under `rddl.c` file.

First, Trust Anchor needs to be registered to the network. To register the Trusted Anchor, we must send a request to the network using the 32-digit Hex number specified by the "Machine Public Key" in Figure 3. This number is public key of Trusted Anchor. To send registration request, we need to use the following message;

```
curl -X POST https://testnet-ta.rddl.io/register/<32DigitHexMachinePubKey>
```

```
Fatih@Fatih-ThinkPad-L480: ~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ curl -X POST https://testnet-ta.rddl.io/register/303F98F8EE26BB54384D1627E3A5E238D8031838183786A22E877C298A736FEA
```

Figure 4: Registration Request for Trusted Anchor

After registering the machine to the network, we will load some coins on it so that it can pay the transaction fees. Otherwise, transactions will be rejected due to insufficient coins.

To do this, open https://testnet-faucet.rddl.io/#/default/post_. Then click POST and Try it out, respectively and upload money to the account ID. The Address is the value specified with “address:” and starting with plmnt as in Figure 3. After entering the address as shown in Figure 5 and writing down how much you will send to the coin section, you can click Execute and load the coin.

POST / Send tokens to receiver account

Parameters Cancel

Name	Description
body required	Send coins request object

body object (body)

After making a sample execution by the 'Try it out' button in the right corner, visit the following link to see the difference in sample account's balance:
<http://localhost:1317/bank/balances/plmnt1lwvk7sfcjww73wvxqgz4vh23fwa5njnsrdqh>

Edit Value | Model

```
{
  "address": "plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6",
  "coins": [
    "20plmnt"
  ]
}
```

Cancel

Parameter content type
application/json

Execute Clear

Figure 5: Sending coin to the device

Now, when we run the same test code again, it will first perform the registration process as in Figure 6.


```

Fatih@Fatih-ThinkPad-L480: ~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ ./test/testRddlSDK
Machine Public Key: 03FD1A9F8E0203025CF3418822EE4F8C593CF80A8EC9C34FF920A6261A66F473C

curl -X GET "https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key/pmpb7u0ZMFAM4TrgEqYrYoAhvx2Gegw5hERKCeWvI3t7QcNtXAGfVfswR8DdE96BYnL44XTXUFmrtstH7XB8VHAaBCxWkZEJ5yufILfsZuBcD" -H "accept: application/json"
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 53 100 53 0 0 41 0 0:00:01 0:00:01 --:--:-- 41
{"code":5,"message":"machine not found","details":{}}
Register: Machine
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 119 100 119 0 0 179 0 --:--:-- --:--:-- --:--:-- 179
ERROR readfile! Couldnt open file ./machinecid{"info":{"address":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","pub_key":null,"account_number":"58","sequence":"0"}}
ERROR readfile! Couldnt open file ./planetmintdenomERROR readfile! Couldnt open file ./planetmintchainid
curl -X POST "https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs" -H "accept: application/json" -H "Content-Type: application/json" -d '{"tx_bytes": "C
sIFCr8FCYVcGxhbmV0bWludGdvLm1hY2hpbmUuTXNnQXR0ZXN0TWFjaGluzRkUBQoscGxtbnQxcXY2azVzdU5a3p0Nmp1cmRrYzQzeGRuZHBkeng2d3J6cHN2djY54wQKLHBSbW50MXF2Nms1c3Q1
OWT6dDZqdXka2M0M3hkbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
FOTZCWR1MVjRyVGY2YVZmN3hkbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
Q5OUZCR3M3Ykd5NN0RzVEFoM2tMcGpZcGRVeJFRU3RVnTnJaM2cyRU5xRDFCakFhUWQ2c0pCMdNGRDExQTlGOEUwMjAzMDI1Q0YzNDE4ODIyRUU0RjhDNTkzQ0Y4MEE4RUM5QzW0RkY5MjBjBNj1ZMUe2N
kY0NzNDUKUSL3siTfUdWzhY3R1cmVYIjogILJEREWL3JTX3pYVWoiJvdGhcnLm1hbc39Ch37JlZlcnNpb24iOiAiMC4xIn1YAAUAVBMTBBMjRCQCFMDFGNtJDRUZGMtK1Q0EXRkREMEI1
QjUwOUZrjdQzQ2M0M3hkbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
renQ2anVyZGtjNDM4ZG5kGR6eD23cnpmw3Z2NhJiCk4KRgoFL2Nvc21vcy5jcnldG8uc2VjcDI1NmsxL1B1YktleRIjclCECP6di2ieIAMXPiE8pOowRbZi5zGyOWrFG4S12QTCW4SBAoCCAESA
oKCGvNbG1udBIBh8dAmgwaQlyKeSn3YZFPpHxkwxpx9o59jbrZLaGvTYJoXp3zwREUUNdHAlDXqOx+PRB2hOFJhVhR13tQuBVBVRhw4kqfk=","mode":"BROADCAST_MODE_SYNC"}'

% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1461 100 244 100 1217 359 1792 --:--:-- --:--:-- --:--:-- 2151
CURL RESPONSE:
{"tx_response":{"height":"0","txhash":"30B499EDC39AAB5DAD1E0E83CE4301230B2A9470A2D365FBDDFB08B8720C1B9","codespace":"","code":0,"data":"","raw_log":["
"],"logs":[]},"info":"","gas_wanted":"0","gas_used":"0","tx":null,"timestamp":"","events":[]}}
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:55:testNotarizationFlow:PASS

```

Figure 6: Registration of Seed

After the seed is registered, every time we call the test code, it will perform a transaction that contains the data as in Figure 7.

```

Fatih@Fatih-ThinkPad-L480: ~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ ./test/testRddlSDK
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:38:testMnemonic:PASS
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:39:testSeedOperation:PASS
Machine Public Key: 03E58EC4AE9860564EDF51A1C9BCF759C63B276D236CD5F15B02FD226AC2CE3F

curl -X GET "https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key/pmpb7u0ZMFAM4TrgEqYrYoAhvx2Gegw5hERKCeWvI3t7QcNtXAGfVfswR8DdE96BYnL44XTXUFmrtstH7XB8VHAaBCxWkZEJ5yufILfsZuBcD" -H "acc
ept: application/json"
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 867 100 867 0 0 2164 0 --:--:-- --:--:-- --:--:-- 2167
{"machine":{"name":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","ticker":"","domain":"lab.f3c.network","reissue":false,"amount":"1","precision":"8","issuerPlanetmint":"pmpb7u0ZMFAM4TrgEqYrYoAhvx2Gegw5hERK
CeWvI3t7QcNtXAGfVfswR8DdE96BYnL44XTXUFmrtstH7XB8VHAaBCxWkZEJ5yufILfsZuBcD","issuerLiquid":"xupb6F50bqhvgemQ73W0ppK2quHuEoFCG2knrbYlnKofr4nCBAS599FbCoxNW9DsAh3kxjYpDz10StnR23pZEnQd1BjAaoQds","
machineid":"03FD1A9F8E0203025CF3418822EE4F8C593CF80A8EC9C34FF920A6261A66F473C","metadata":{"gps":"","device":{"Manufacturer":"","Model":"","Device":"","Version":"","
1"},"additionalDataCID":"","type":"1","machineidSignature":"EA10A248A801F52CEFF195CA1FD085B509B3F7FC301E437ED90984EBDBDA532309080921D7033F2E40F9EECA6CDB8C02D299C0FB1D6AF83CCA30F0EAB983","address":"plmn
tiqv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6"}}
SUCCESS
,"Hash":"1B30E4F9285BA5F380A58D5EACEBC38393E629E5611230A6825A141EB859"
,"Signature":"Ec75C00158C45A07585804772AE2A812709E338371D99C170FA074CEB449866801B3ADE21DC46B7DEBCC817218D9660F80A80CAF634414DC17535A734B082"
,"PublicKey":"029E9322A1E2FD06E43FACAA20E8F01A07EB2396718C04F59E3E8F39025B52D63"
Notarize: CID Asset
TX processing:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 212 100 212 0 0 691 0 --:--:-- --:--:-- --:--:-- 690
{"info":{"address":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","pub_key":{"@type":"/cosmos.crypto.secp256k1.PubKey","key":"AlzYtonogDfzyHwKtqFkM2YucxsjlxrEtcdkTglu"},"account_number":"58","sequence":
12}}
TX broadcast:

curl -X POST "https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs" -H "accept: application/json" -H "Content-Type: application/json" -d '{"tx_bytes": "CpYBcPbCQvcGxhbmV0bWludGdvLm1hY2hpbmUuTXNnQXR0ZXN0TWFjaGluzRkUBQoscGxtbnQxcXY2azVzdU5a3p0Nmp1cmRrYzQzeGRuZHBkeng2d3J6cHN2djY54wQKLHBSbW50MXF2Nms1c3Q1
OWT6dDZqdXka2M0M3hkbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
FOTZCWR1MVjRyVGY2YVZmN3hkbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
Q5OUZCR3M3Ykd5NN0RzVEFoM2tMcGpZcGRVeJFRU3RVnTnJaM2cyRU5xRDFCakFhUWQ2c0pCMdNGRDExQTlGOEUwMjAzMDI1Q0YzNDE4ODIyRUU0RjhDNTkzQ0Y4MEE4RUM5QzW0RkY5MjBjBNj1ZMUe2N
kY0NzNDUKUSL3siTfUdWzhY3R1cmVYIjogILJEREWL3JTX3pYVWoiJvdGhcnLm1hbc39Ch37JlZlcnNpb24iOiAiMC4xIn1YAAUAVBMTBBMjRCQCFMDFGNtJDRUZGMtK1Q0EXRkREMEI1
QjUwOUZrjdQzQ2M0M3hkbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
jCjZlZjA3aGVhZG9ka2hpbmRwZHp4NDYnBzdY2G9sYIucjNjLn5ldHdvcmsoATAI0m9wbXBIN3VEWk1GQU0VHJnRXFyW9BSHZ4MkdLZ3c1aEVSS0NlV2FwaTN0N1FDbnRYQudmVmZd1I4RGR
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 721 100 244 100 477 766 1497 --:--:-- --:--:-- --:--:-- 2267
CURL RESPONSE:
{"tx_response":{"height":"0","txhash":"34F350AC33F242E27273B4AEAS0D1C3A7B951F5B2EC25DAB589341568AB38E9C","codespace":"","code":0,"data":"","raw_log":["
"],"logs":[]},"info":"","gas_wanted":"0","gas_used":"0","tx":null,"timestamp":"","events":[]}}
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:40:testNotarizationFlow:PASS

3 Tests 0 Failures 0 Ignored
OK

```

Figure 7: Data Transaction into RDDL Network