Toy example for fECDSA

This document reports on a toy example with the fECDSA simulator. It can be useful to understand the structure of blocks in the proposed blockchain.

Setting

We report an example we have obtained, by setting $N = 5$, $w = 256$, $X = 3$, $N^*_{\mathtt{RawTx}} = 3$. To generate the difficulty for the PoW mining, we have considered the following relation

$$\ell = \alpha + \left\lceil \log 2 \Big((4 * w + 1)\, (N^*_{\mathtt{RawTx}} - N_{\mathtt{RawTx}}) \Big) \right\rceil ,$$

where α corresponds to the parameter `difficulty_coefficient` in the code (defined in `main.py`, line 24). We report the results for $\ell = 4$.

We have launched our simulator considering an initial seed equal to 0; any reader can obtain our very same results by simply launching the script with the same seed value. Notice that, to obtain reproducible results, it is fundamental that line 22 of `blockchain_utils.py` is commented and line 23 is executed. Indeed, line 22 uses the current time and date to generate blocks, while line 23 generates a random timestamp. If line 22 is executed, instead of line 23, obviously, the values in this report will not be obtained.

For the hash of the genesis block in the chain, we have considered the default value

`0x0000000000000000000000000000000000000000000000000000000000000000`.

For the PRNG, we have selected at random an elliptic curve point; namely, in the code we release, $\widetilde{Q}$ has abscissa

`0xb6eeb6c0ed0fca8dc11f5656ab64aab7a6a3a001c1041cddee12e5e7b861688`,

and ordinate

`0x4e10fcdf768e6b21a71dd3126e8a17bdf69106b07d23d5c2577658ad934d77ba`.

First blocks in the chain

The parameters of the $N = 5$ enrolled users have been reported in Table 1. In Figures 1, 2 and 3 we report the parameters of the first three blocks in the chain (excluding the genesis block).

Table 1: Users parameters

User	Parameter	Value
0	$\hat{x}_0$	0xf728b4fa42485e3a0a5d2f346baa9455e3e70682c2094cac629f6fbed82c07cf
	Noise during enrollment	241
	Secret key during enrollment	0xf728b4fa42485e3a0a5d2f346baa9455e3e70682c2094cac629f6fbed82c08c0
	Public key	0x19c42d6c3f8ec52ea79c5d415f46f86b946edce053d4b7093abc1213b8252b22
1	$\hat{x}_1$	0x5ba91faf7a024204f7c1bd874da5e709d4713d60c8a70639eb1167b367a9c37a
	Noise during enrollment	-33
	Secret key during enrollment	0x5ba91faf7a024204f7c1bd874da5e709d4713d60c8a70639eb1167b367a9c359
	Public key	0xb165859efde2fc46d1e3e55e895418c70efdea5b6f14b7c5f9328274329405f0
2	$\hat{x}_2$	0xcca5a5a19e4d6e3c1846d424c17c627923c6612f4826867323a7711a81332878
	Noise during enrollment	0
	Secret key during enrollment	0xcca5a5a19e4d6e3c1846d424c17c627923c6612f4826867323a7711a81332878
	Public key	0x6a103f2e95145993ad50ee796df88a972ecd6b0a0a399b5a8afa7a41b762731e
3	$\hat{x}_3$	0xe6f4590b9a164106cf6a659eb4862b21fb97d43588561712e8e5216afcbd04c5
	Noise during enrollment	-106
	Secret key during enrollment	0xe6f4590b9a164106cf6a659eb4862b21fb97d43588561712e8e5216afcbd045b
	Public key	0x7812f5226354ff99d43d91576f51a60de95897eb7e79994ebf354f1b646cae56
4	$\hat{x}_4$	0x5487ce1eaf19922ad9b8a714e61a441c12e0c8b2bad640fb19488dec4f65d4db
	Noise during enrollment	227
	Secret key during enrollment	0x5487ce1eaf19922ad9b8a714e61a441c12e0c8b2bad640fb19488dec4f65d5be
	Public key	0xdb78ee24986c98fa4c75190c97c2197e30f033f67cd01a46b7fc55233fc50bd2

In the first block, there are three transactions, instantiated respectively by users 0, 0 and 4. The first transaction has been generated using the secret key $\hat{x}_0 - 161$. Given that this user enrolled with key $\hat{x}_0 + 241$, the first transactions would be cleared by $\Delta e = 241 - (-161) = 402$. The second transaction has been, again, submitted by user 0, using key $\hat{x}_0 - 192$; hence, the signature would be cleared by $\Delta e = 241 - (-192) = 433$. Finally, the third transaction has been initiated by user 4, using key $\hat{x}_4 + 42$: this transaction gets cleared by $\Delta e = 227 - 42 = 185$. Since this block contains the maximum number of transactions (that is, three in this example), the difficulty parameter ℓ is set to 0 and the corresponding nonce is empty (since the additional mining procedure is not required).

The second block in the chain has an analogous structure. The third block in the chain, instead, contains only two transactions; hence, an additional mining procedure is required. In this case, the difficulty of this step is

$$\ell = 4 + \lceil \log_2(4 \cdot 256 + 1) \rceil = 15.$$

```
{
    "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "blockNumber": 1,
    "NumTx": 3,
    "difficulty": 0,
    "nonce": ""
},
{
    "Tx#": 0,
    "identity": 0,
    "timestamp": "72572559719738032807806534630",
    "r": "0x983b551414d77213075e918d70b7a8833f60eabd0bd26287c6122cf5aab22cb",
    "s": "0x2fc61e3f63c469e2300c0964d556d9cefe97307d557b8b0b0e67de9a142e6548",
    "v": 0,
    "PoW": "0xd01cf93568032f7efef06b0468fc642af6f259264e60678b82f4b48a78a55d6b"
},
{
    "Tx#": 1,
    "identity": 0,
    "timestamp": "850140255162790205208404711458",
    "r": "0x2ff8ecea744e59c2e358dc93b734055bb68f321e00f4d322fa381ad55fbaf8bd",
    "s": "0xecdf8db6f1540b3a5d52ba9eb52b04f952e8d663fc0fcc1fe864c5bc9e179205",
    "v": 1,
    "PoW": "0x5fe537894c2bee79582b2090c40a044366639941a309b6888a84524d0c94499f"
},
{
    "Tx#": 2,
    "identity": 4,
    "timestamp": "721693915513941748165567722123",
    "r": "0x6c8ea6e23c0dd77be2124c9991687ccffd1dd20ff97823886520ef7e0a2887ca",
    "s": "0x81fe919b16b4960c079dfc6c2d0605e0dd409f8b5fb859f966d2d47d9b1b6adc",
    "v": 1,
    "PoW": "0x2ffe649bdbe9c598af1f92315695faf551e92de326dff821a35026fecdcff1e1"
},
{
    "hash": "0x04252be617ab4ac6c9d990838fbc1525fd199bdea65c23df87fbf5d14376dfad"
}
```

Figure 1: Block #1 in the example

```
{
    "parentHash": "0x04252be617ab4ac6c9d990838fbc1525fd199bdea65c23df87fbf5d14376dfad",
    "blockNumber": 2,
    "NumTx": 3,
    "difficulty": 0,
    "nonce": ""
},
{
    "Tx#": 0,
    "identity": 0,
    "timestamp": "41715005078842197440363051 2744",
    "r": "0x1dda6c961c7f5299cc4b5818883840b9e5e60521dd2144e97ed9d1f3cb7cd393",
    "s": "0xa655d927d485db3b5b835b91a5a88b447c41052a2354b6bf088dfc7021dfd233",
    "v": 0,
    "PoW": "0xe41804a163f79f50900718eb8da995c76364b9b707370615de97e0d1adac08fd"
},
{
    "Tx#": 1,
    "identity": 4,
    "timestamp": "82123350681873522336352425931 4",
    "r": "0x4bfabd28c5acd5a4151deee10dc9d2fa8c2f4057c073f98c7913cddbf61a5155",
    "s": "0x3e3c5392c17fcbf290dc1aaa58202a60a435b6bed20303ee08640dd7783d3a16",
    "v": 0,
    "PoW": "0xc4d6f82612be025a0546b70649bd46ceac1c7260507db7906f66eb661674534d"
},
{
    "Tx#": 2,
    "identity": 1,
    "timestamp": "894636792358148343616370367618",
    "r": "0x3f71cde47deef2ee961e9be53791965fdf5a2efab7ef75249c9cd9842ee1dc48",
    "s": "0xd03629da3fbb576dffdbbd74725334f86ba4b8b3f97e7a4e2bfcbf329ffcf70d",
    "v": 1,
    "PoW": "0xe4a7cb70e680b4ed69396e957c94278f2f225e7bcac96c1845237eb7adc8f23d"
},
{
    "hash": "0x358bef9b293e6f2b212a3dafaad5324c212bf4dcd9070acf0ca7732147200c26"
}
```

Figure 2: Block #2 in the example

```
{
    "parentHash": "0x358bef9b293e6f2b212a3dafaad5324c212bf4dcd9070acf0ca7732147200c26",
    "blockNumber": 3,
    "NumTx": 2,
    "difficulty": 15,
    "nonce": "0x7e964f875e42defb90b7ba1fdb57f3dbf1c016251d56e49bfa34bd33ff4603e7"
},
{
    "Tx#": 0,
    "identity": 2,
    "timestamp": "545838922376352528254452630669",
    "r": "0xb75a7f1c83ffa5e8b06968ae4a85e133905574761c5efec21651f70710a98b5e",
    "s": "0xbec89d2229f0e15f98a8e50ba4a752dc81122e441891d5ec163523effefd85c7",
    "v": 1,
    "PoW": "0x40332958e5f6629f7a8deea8500cf431b1eae53ea3cac3a40716a5b10aa6a18e"
},
{
    "Tx#": 1,
    "identity": 0,
    "timestamp": "235127720502957121919005548546",
    "r": "0x910086613b5a46beb9b4e4c5063944c6c7f4bdbb82ab815a53e0d9291ea1734c",
    "s": "0x58f136f133300713ec845a868c684555a235f5a664f96f7c5f10139e833d87e9",
    "v": 0,
    "PoW": "0xb56bfa9ce13ec6cecb83f88b578ee89d0c484252a35831b7ce72ab07c69ad8f6"
}
],
{
    "hash": "0x4d25377839d20aac7bfc53146dcf100bf47de7e9430a1500f310cf7f9797fd94"
}
```

Figure 3: Block #3 in the example