

## 1) - Проблема индексации NFT айтемов (Логическая ошибка)

Тут, в файле `stbl_staking.fc`, происходит минт айтема, если стейка ещё не было

```
279     ;; if hasn't staked before
280     if (staker::staked_a == 0) {
281         cell item_message = begin_cell()
282             .store_slice(staker_address)           ;; item owner
283             .store_ref(self::nft_content)          ;; item content
284             .store_slice(self::initializer)        ;; editor
285         .end_cell();
286         cell nft_body = pack_nft_mint_message(msg::query_id, CONF::NFT_ITEM_AMOUNT, item_message);
287         cell nft_mint_msg = delib::int_msg(self::nft_collection_address, false, CONF::NFT_MINT_AMOUNT, nft_body, null());
288         send_raw_message(nft_mint_msg, MSG::SENDER_PAYS_FEES);
289     }
```

Проблема в том, что в файле `helpers.fc`, в функции, которая формирует сообщение, отправляемое на контракт коллекции при минте айтема, индекс представлен константой - 0 (95 строка)

```
90
91 cell pack_nft_mint_message(int query_id, int item_value, cell nft_message) inline {
92     return begin_cell()
93         .store_uint(op::nft::mint, 32)
94         .store_uint(query_id, 64)
95         .store_int(0, 64) ;; item_index
96         .store_coins(item_value) ;; ton to send to the item
97         .store_ref(nft_message)
98         .end_cell();
99 }
```

Поэтому айтем с помощью этой функции можно заминтить только один, под индексом 0, при попытке заминтить повторно - будет ошибка 402, ниже код из файла `nft_collection.fc`

```
102
103     if (op == 1) { ;; deploy new nft
104         int item_index = in_msg_body~load_uint(64);
105         throw_unless(402, item_index <= next_item_index); ;; sanity check
106         deploy_nft_item(next_item_index, nft_item_code, in_msg_body~load_coins(), in_msg_body~load_ref());
107         next_item_index += 1;
108         save_data(owner_address, next_item_index, content, nft_item_code, royalty_params);
109         return ();
110     }
111     if (op == 2) { ;; batch deploy of new nfts
```

Поэтому нужно запоминать индекс последнего айтема, который мы заминтили и инкрементировать этот индекс для следующих минтов.

```
280
281     let nftData = await nftCollection.getCollectionData();
282     expect(nftData.nextItemId).toEqual(1);
283
284     // const userStakeSecond = await userWallet.sendTransfer(
285     //   user.getSender(),
286     //   toNano(0.5),
287     //   userJettons / 2n,
288     //   stblStaking.address,
289     //   user.address,
290     //   beginCell().endCell(),
291     //   toNano(0.4),
292     //   beginCell().endCell()
293     // );
294
295     expect(userStakeSecond.transactions).toHaveTransaction({
296       from: stblStaking.address,
297       to: nftCollection.address,
298       op: 1, // deploy new nft
299     });
300
301     expect(userStakeSecond.transactions).toHaveTransaction({
302       from: nftCollection.address,
303     });
304
305     nftData = await nftCollection.getCollectionData();
306     expect(nftData.nextItemId).toEqual(2);
307
308   });
309
310   it("should not accept small stake", async () => {
311     // console.log("Staking Address: ", stblStaking.address)
312     const userStake = await userWallet.sendTransfer(
313       user.getSender(),
314       toNano(0.5),
315       userJettons / 2n,
316       stblStaking.address,
317       user.address,
318       beginCell().endCell(),
319       toNano(0.4),
320       beginCell().endCell()
321     );
322
323     expect(userStake.transactions).toHaveTransaction({
324       from: stblStaking.address,
325       to: nftCollection.address,
326       op: 1, // deploy new nft
327     });
328
329     at Object.<anonymous> (tests/StblStaking.spec.ts:295:50)
330
331   Test Suites: 1 failed, 1 total
332   Tests:      1 failed, 7 passed, 8 total
333   Snapshots:  0 total
334   Time:       7.542 s, estimated 9 s
335   Ran all test suites.
```

При втором минте - индекс токена должен быть 2, но, как мы видим, вылетает ошибка

```
276
277     expect(userStake.transactions).toHaveTransaction({
278       from: nftCollection.address,
279     });
280
281     let nftData = await nftCollection.getCollectionData();
282     expect(nftData.nextItemId).toEqual(1);
283
284     // const userStakeSecond = await userWallet.sendTransfer(
285     //   user.getSender(),
286     //   toNano(0.5),
287     //   userJettons / 2n,
288     //   stblStaking.address,
289     //   user.address,
290     //   beginCell().endCell(),
291     //   toNano(0.4),
292     //   beginCell().endCell()
293     // );
294
295     expect(userStake.transactions).toHaveTransaction({
296       from: stblStaking.address,
297       to: nftCollection.address,
298       op: 1, // deploy new nft
299     });
300
301     expect(userStake.transactions).toHaveTransaction({
302       from: nftCollection.address,
303     });
304
305     nftData = await nftCollection.getCollectionData();
306     expect(nftData.nextItemId).toEqual(1);
307
308   });
309
310   it("should not accept small stake", async () => {
311     // console.log("Staking Address: ", stblStaking.address)
312     const userStake = await userWallet.sendTransfer(
313       user.getSender(),
314       toNano(0.5),
315       userJettons / 2n,
316       stblStaking.address,
317       user.address,
318       beginCell().endCell(),
319       toNano(0.4),
320       beginCell().endCell()
321     );
322
323     expect(userStake.transactions).toHaveTransaction({
324       from: stblStaking.address,
325       to: nftCollection.address,
326       op: 1, // deploy new nft
327     });
328
329     at Object.<anonymous> (tests/StblStaking.spec.ts:295:50)
330
331   Test Suites: 1 passed, 1 total
332   Tests:      8 passed, 8 total
333   Snapshots:  0 total
334   Time:       7.452 s, estimated 8 s
335   Ran all test suites.
```

Ошибок нет, если после второй транзакции ожидать значение 1, так как nextItemId не изменился, а следовательно, айтем не задеплоился

## 2) - Предпочтительнее использовать константы вместо ассемблерных примитивов (Использование лишнего газа)

Пример:

```
int op::transfer_ownership() asm "0x2da38aaf PUSHINT";  
const int op::transfer_ownership = 0x2da38aaf;
```

Стоит определять ошибки/оп-коды и прочие “константы” другим способом, не с помощью ассемблерных примитивов, а с помощью констант, так как второе помогает компилятору оптимизировать код самостоятельно, не стоит это делать за него лишний раз. Компилятор FunC внутри ассемблерной функции не смотрит. Например так, “256 PUSHINT” можно заменять на “8 PUSHPOW2”, компилятор может воспользоваться другим кодом, создать значение в другой момент (если так будет удобнее по стеку). Более того, нынешний подход расходует больше газа (<https://docs.ton.org/learn/tvm-instructions/instructions>).

Или же вот:

```
cell    delib::lc()      asm "<b> PUSHINT",      ;; creates an empty cell  
cell    delib::stc(slice s) asm "NEWC SWAP STSLICER ENDC"; ;; converts a slice into cell  
slice    delib::addr_pope() asm "b{00} PUSHSLICE";      ;; creates an addr_pope$00 slice
```

```
begin_cell()  
    .store_slice(s)  
.end_cell()
```

вместо `delib::stc(s)` почти наверняка будет не хуже.

Особенно интересно, зачем `SWAP STSLICER`(26 ед.газа), когда есть вполне нормальная операция `STSLICE`(18 ед. газа).

CE	STSLICE	s b - b'	Stores Slice s into Builder b.	18
CF16	STSLICER	b s - b'	Equivalent to SWAP STSLICE.	26

Это не все примеры, в коде полно функций, оформленных в виде ассемблерных примитивов, которые бездумно расходуют газ.

### 3) - inline/inline\_ref (Совет по оптимизации)

```
104 cell jetton_transfer(int amount, slice to_address, slice response_address,  
105                      slice jetton_wall, int ton_amount) inline {  
106  
107     cell body = pack_simple_jetton_transfer(msg::query_id, amount, to_address,  
108                                             response_address, CONF::JETTON_FWD_AMOUNT);  
109  
110     return delib::int_msg(jetton_wall, false, ton_amount, body, null());  
111 }  
112  
113 () throw_jettons_128(slice to, slice jetton_wall, int amount) impure inline {  
114     cell msg = jetton_transfer(amount, to, to, jetton_wall, 0);  
115     send_raw_message(msg, MSG::ALL_NOT_RESERVED + MSG::IGNORE_ERRORS);  
116  
117     commit();  
118     throw(ERR::NOT_ENOUGH);  
119 }  
120  
121 (slice, cell) calc_escrow_contract(slice staker_address) inline {  
122     cell contract_data = pack_escrow_data(my_address(), staker_address);  
123     cell contract_init = delib::basic_state_init(self::escrow_contract_code, contract_data);  
124     return (delib::addrstd_by_state(CONF::WC, contract_init), contract_init);  
125 }  
126  
127 () auth_by_escrow_contract(slice staker_address) impure inline {  
128     (slice escrow_address, _) = calc_escrow_contract(staker_address);  
129     throw_unless(ERR::ACCESS, equal_slice_bits(msg::sender, escrow_address));  
130 }  
131  
132 ;; contract constructor (can be called only once)  
133 () constructor(slice msg body) impure inline ref {
```

#### Inline\_ref specifier

The code of a function with the `inline_ref` specifier is put into a separate cell, and every time when the function is called, a `CALLREF` command is executed by TVM. So it's similar to `inline`, but because a cell can be reused in several places without duplicating it, it is almost always more efficient in terms of code size to use **`inline_ref` specifier instead of `inline` unless the function is called exactly once.** Recursive calls of `inline_ref`ed functions are still impossible because there are no cyclic references in the TVM cells.

Источник: (<https://docs.ton.org/develop/func/functions>)

Как сказано в документации: “с точки зрения размера кода почти всегда более эффективно использовать `inline_ref` спецификатор вместо `inline` если функция не вызывается ровно один раз.”, поэтому непонятно почему именно тут спецификатор `inline`, хоть функции вызываются много раз (>> 1).

#### 4) 432 строка в `stbl_staking.fc` (Непонятный комменттарий)

```
;; reserve jettons (target or balance - msg.value)
ctx::reserve(MAIN::TARGET);
```

почему написано, что функция резервирует жетоны, когда она резервирует количество TON на балансе контракта

```
msg::sender      = sender;
msg::balance     = balance;    ;; contract balance
msg::value       = value;      ;; msg value
```

```
() ctx::reserve(int target) impure inline {
|   raw_reserve(max(msg::balance - msg::value, target), 0);
| }
}
```