

```
PK     K-X EA9       wallet-v4-code.fc#pragma version=0.2.0; ;; Wallet smart contract with plugins (slice, int) dict_get?(cell dict, int key_len, slice index) asm(index dict key_len) "DICTGET" "NULLSWAPIFNOT"; (cell, int) dict_add_builder?(cell dict, int key_len, slice index, builder value) asm(value index dict key_len) "DICTADDB"; (cell, int) dict_delete?(cell dict, int key_len, slice index) asm(index dict key_len) "DICTDEL"; () recv_internal(int msg_value, cell in_msg_cell, slice in_msg) impure { var cs = in_msg_cell.begin_parse(); var flags = cs~load_uint(4); ;; int_msg_info$0 ihr_disabled:Bool bounce:Bool bounced:Bool if (flags & 1) { ;; ignore all bounced messages return (); } if (in_msg.slice_bits() < 32) { ;; ignore simple transfers return (); } int op = in_msg~load_uint(32); if (op != 0x706c7567) & (op != 0x64737472) { ;; "plug" & "dstr" ;; ignore all messages not related to plugins return (); } slice s_addr = cs~load_msg_addr(); (int wc, int addr_hash) = parse_std_addr(s_addr); slice wc_n_address = begin_cell().store_int(wc, 8).store_uint(addr_hash, 256).end_cell().begin_parse(); var ds = get_data().begin_parse().skip_bits(32 + 32 + 256); var plugins = ds~load_dict(); var (_, success?) = plugins.dict_get?(8 + 256, wc_n_address); if ~(success?) { ;; it may be a transfer return (); } int query_id = in_msg~load_uint(64); var msg = begin_cell(); if (op == 0x706c7567) { ;; request funds (int r_toncoins, cell r_extra) = (in_msg~load_grams(), in_msg~load_dict()); [int my_balance, _] = get_balance(); throw_unless(80, my_balance - msg_value >= r_toncoins); msg = msg.store_uint(0x18, 6).store_slice(s_addr).store_grams(r_toncoins).store_dict(r_extra).store_uint(0, 4 + 4 + 64 + 32 + 1 + 1).store_uint(0x706c7567 | 0x80000000, 32).store_uint(query_id, 64); send_raw_message(msg.end_cell(), 64); } } if (op == 0x64737472) { ;; remove plugin by its request plugins~dict_delete?(8 + 256, wc_n_address); var ds = get_data().begin_parse().first_bits(32 + 32 + 256); set_data(begin_cell().store_slice(ds).store_dict(plugins).end_cell()); ;; return coins only if bounce expected if (flags & 2) { msg = msg.store_uint(0x18, 6).store_slice(s_addr).store_grams(0).store_uint(0, 1 + 4 + 4 + 64 + 32 + 1 + 1).store_uint(0x64737472 | 0x80000000, 32).store_uint(query_id, 64); send_raw_message(msg.end_cell(), 64); } } } () recv_external(slice in_msg) impure { var signature = in_msg~load_bits(512); var cs = in_msg; var (subwallet_id, valid_until, msg_seqno) = (cs~load_uint(32), cs~load_uint(32), cs~load_uint(32)); throw_if(36, valid_until <= now()); var ds = get_data().begin_parse(); var (stored_seqno, stored_subwallet, public_key, plugins) = (ds~load_uint(32), ds~load_uint(32), ds~load_uint(256), ds~load_dict()); ds.end_parse(); throw_unless(33, msg_seqno == stored_seqno); throw_unless(34, subwallet_id == stored_subwallet); throw_unless(35, check_signature(slice_hash(in_msg), signature, public_key)); accept_message(); set_data(begin_cell().store_uint(stored_seqno + 1, 32).store_uint(stored_subwallet, 32).store_uint(public_key, 256).store_dict(plugins).end_cell()); commit(); cs~touch(); int op = cs~load_uint(8); if (op == 0) { ;; simple send while (cs.slice_refs()) { var mode = cs~load_uint(8); send_raw_message(cs~load_ref(), mode); } return (); ;; have already saved the storage } if (op == 1) { ;; deploy and install plugin int plugin_workchain = cs~load_int(8); int plugin_balance = cs~load_grams(); (cell state_init, cell body) = (cs~load_ref(), cs~load_ref()); int plugin_address = cell_hash(state_init); slice wc_n_address = begin_cell().store_int(plugin_workchain, 8).store_uint(plugin_address, 256).end_cell().begin_parse(); var msg = begin_cell().store_uint(0x18, 6).store_uint(4, 3).store_slice(wc_n_address).store_grams(plugin_balance).store_uint(4 + 2 + 1, 1 + 4 + 4 + 64 + 32 + 1 + 1 + 1).store_ref(state_init).store_ref(body); send_raw_message(msg.end_cell(), 3); (plugins, int success?) = plugins.dict_add_builder?(8 + 256, wc_n_address, begin_cell()); throw_unless(39, success?); } if (op == 2) { ;; install plugin slice wc_n_address = cs~load_bits(8 + 256); int amount = cs~load_grams(); int query_id = cs~load_uint(64); (plugins, int success?) = plugins.dict_add_builder?(8 + 256, wc_n_address, begin_cell()); throw_unless(39, success?); builder msg = begin_cell().store_uint(0x18, 6).store_uint(4, 3).store_slice(wc_n_address).store_grams(amount).store_uint(0, 1 + 4 + 4 + 64 + 32 + 1 + 1).store_uint(query_id, 64); send_raw_message(msg.end_cell(), 3); } if (op == 3) { ;; remove plugin slice wc_n_address = cs~load_bits(8 + 256); int amount = cs~load_grams(); int query_id = cs~load_uint(64); (plugins, int success?) = plugins.dict_delete?(8 + 256, wc_n_address); throw_unless(39, success?); builder msg = begin_cell().store_uint(0x18, 6).store_uint(4, 3).store_slice(wc_n_address).store_grams(amount).store_uint(0, 1 + 4 + 4 + 64 + 32 + 1 + 1).store_uint(0x64737472, 32); op.store_uint(query_id, 64); send_raw_message(msg.end_cell(), 3); } set_data(begin_cell().store_uint(stored_seqno + 1, 32).store_uint(stored_subwallet, 32).store_uint(public_key, 256).store_dict(plugins).end_cell()); }; ;; Get methods int seqno() method_id { return get_data().begin_parse().preload_uint(32); } int get_subwallet_id() method_id { return get_data().begin_parse().skip_bits(32).preload_uint(32); } int get_public_key() method_id { var cs = get_data().begin_parse().skip_bits(64); return cs.preload_uint(256); } int is_plugin_installed(int wc, int addr_hash) method_id { var ds = get_data().begin_parse().skip_bits(32 + 32 + 256); var plugins = ds~load_dict(); var (_, success?) = plugins.dict_get?(8 + 256, begin_cell().store_int(wc, 8).store_uint(addr_hash, 256).end_cell().begin_parse()); return success?; } tuple get_plugin_list() method_id { var list = null(); var ds = get_data().begin_parse().skip_bits(32 + 32 + 256); var plugins = ds~load_dict(); do { var (wc_n_address, _, f) = plugins~dict::delete_get_min(8 + 256); if (f) { (int wc, int addr) = (wc_n_address~load_int(8), wc_n_address~load_uint(256)); list = cons(pair(wc, addr), list); } } until (~ f); return list; } PK     K-X  C k7k7 stdlib.fc;; Standard library for funC ;; forall X -> tuple cons(X head, tuple tail) asm "CONS"; forall X -> (X, tuple) uncons(tuple list) asm "UNCONS"; forall X -> (tuple, X) list_next(tuple list) asm (-> 1 0) "UNCONS"; forall X -> X car(tuple list) asm "CAR"; tuple cdr(tuple list) asm "CDR"; tuple empty_tuple() asm "NIL"; forall X -> tuple tpush(tuple t, X value) asm "TPUSH"; forall X -> (tuple, ()) ~tpush(tuple t, X value) asm "TPUSH"; forall X -> [X] single(X x) asm "SINGLE"; forall X -> X unsingle([X] t) asm "UNSINGLE"; forall X, Y -> [X, Y] pair(X x, Y y) asm "PAIR"; forall X, Y -> (X, Y) unpair([X, Y] t) asm "UNPAIR"; forall X, Y, Z -> [X, Y, Z] triple(X x, Y y, Z z) asm "TRIPLE"; forall X, Y, Z -> (X, Y, Z) untriple([X, Y, Z] t) asm "UNTRIPLE"; forall X, Y, Z, W -> [X, Y, Z, W] tuple4(X x, Y y, Z z, W w) asm "4 TUPLE"; forall X, Y, Z, W -> (X, Y, Z, W) untuple4([X, Y, Z, W] t) asm "4 UNTUPLE"; forall X -> X first(tuple t) asm "FIRST"; forall X -> X second(tuple t) asm "SECOND"; forall X -> X third(tuple t) asm "THIRD"; forall X -> X fourth(tuple t) asm "3 INDEX"; forall X, Y -> X pair_first([X, Y] p) asm "FIRST"; forall X, Y -> Y pair_second([X, Y] p) asm "SECOND"; forall X, Y, Z -> Z triple_third([X, Y, Z] p) asm "THIRD"; forall X -> X null() asm "PUSHNULL"; forall X -> (X, ()) ~impure_touch(X x) impure asm "NOP"; int now() asm "NOW"; slice my_address() asm "MYADDR"; [int, cell] get_balance() asm "BALANCE"; int cur_lt() asm "LTIME"; int block_lt() asm "BLOCKLT"; int cell_hash(cell c) asm "HASHCU"; int slice_hash(slice s) asm "HASHSU"; int string_hash(slice s) asm "SHA256U"; int check_signature(int hash, slice signature, int public_key) asm "CHKSIGNU"; int check_data_signature(slice data, slice signature, int public_key) asm "CHKSIGNS"; (int, int, int) compute_data_size(cell c, int max_cells) impure asm "CDATASIZE"; (int, int, int) slice_compute_data_size(slice s, int max_cells) impure asm "SDATASIZE"; (int, int, int, int) compute_data_size?(cell c, int max_cells) asm "CDATASIZEQ NULLSWAPIFNOT2 NULLSWAPIFNOT"; (int, int, int, int) slice_compute_data_size?(cell c, int max_cells) asm "SDATASIZEQ NULLSWAPIFNOT2 NULLSWAPIFNOT"; ;; () throw_if(int excno, int cond) impure asm "THROWARGIF"; () dump_stack() impure asm "DUMPSTK"; cell get_data() asm "c4 PUSH"; () set_data(cell c) impure asm "c4 POP"; cont get_c3() impure asm "c3 PUSH"; () set_c3(cont c) impure asm "c3 POP"; cont bless(slice s) impure asm "BLESS"; () accept_message() impure asm "ACCEPT"; () set_gas_limit(int limit) impure asm "SETGASLIMIT"; () commit() impure asm "COMMIT"; () buy_gas(int gram) impure asm "BUYGAS"; int min(int x, int y) asm "MIN"; int max(int x, int y) asm "MAX"; (int, int) minmax(int x, int y) asm "MINMAX"; int abs(int x) asm "ABS"; slice begin_parser(cell c) asm "CTOS"; () end_parse(slice s) impure asm "ENDS"; (slice, cell) load_ref(slice s) asm(-> 1 0) "LDREF"; cell preload_ref(slice s) asm "PLDREF"; ;; (slice, int) ~load_int(slice s, int len) asm(s len -> 1 0) "LDIX"; ;; (slice, int) ~load_uint(slice s, int len) asm(-> 1 0) "LDUX"; ;; int preload_int(slice s, int len) asm "PLDIX"; ;; int preload_uint(slice s, int len) asm "PLDUX"; ;; (slice, slice) load_bits(slice s, int len) asm(s len -> 1 0) "LDSLICEX"; ;; slice preload_bits(slice s, int len) asm "PLDSLICEX"; (slice, int) load_grams(slice s) asm(-> 1 0) "LDGRAMS"; slice skip_bits(slice s, int len) asm "SDSKIPFIRST"; (slice, ()) ~skip_bits(slice s, int len) asm "SDSKIPFIRST"; slice first_bits(slice s, int len) asm "SDCUTFIRST"; slice skip_last_bits(slice s, int len) asm "SDSKIPLAST"; (slice, ()) ~skip_last_bits(slice s, int len) asm "SDSKIPLAST"; slice slice_last(slice s, int len) asm "SDCUTLAST"; (slice, cell) load_dict(slice s) asm(-> 1 0) "LDDICT"; cell preload_dict(slice s) asm "PLDDICT"; slice skip_dict(slice s) asm "SKIPDICT"; (slice, cell) load_maybe_ref(slice s) asm(-> 1 0) "LDOPTREF"; cell preload_maybe_ref(slice s) asm "PLDOPTREF"; builder store_maybe_ref(builder b, cell c) asm(c b) "STOPTREF"; int cell_depth(cell c) asm "CDEPTH"; int slice_refs(slice s) asm "SREFS"; int slice_bits(slice s) asm "SBITS"; (int, int) slice_bits_refs(slice s) asm "SBITREFS"; int slice_empty?(slice s) asm "SEMPY"; int slice_data_empty?(slice s) asm "SEDP"; int slice_refs_empty?(slice s) asm "SREMPY"; int slice_depth(slice s) asm "SDEPT"; int slice_data_depth(slice s) asm "SDDPT"; int slice_data_refs(slice s) asm "SDDR"; int slice_data_refs_empty?(slice s) asm "SDDR_EMPTY"; int slice_data_refs_max(slice s) asm "SDDR_MAX"; int slice_data_refs_min(slice s) asm "SDDR_MIN"; int slice_data_refs_avg(slice s) asm "SDDR_AVG"; int slice_data_refs_std(slice s) asm "SDDR_STD"; int slice_data_refs_var(slice s) asm "SDDR_VAR"; int slice_data_refs_cov(slice s) asm "SDDR_COV"; int slice_data_refs_corr(slice s) asm "SDDR_CORR"; int slice_data_refs_pcc(slice s) asm "SDDR_PCC"; int slice_data_refs_pdc(slice s) asm "SDDR_PDC"; int slice_data_refs_psc(slice s) asm "SDDR_PSC"; int slice_data_refs_pcrc(slice s) asm "SDDR_PCRC"; int slice_data_refs_pccr(slice s) asm "SDDR_PCCR"; int slice_data_refs_pscr(slice s) asm "SDDR_PSCR"; int slice_data_refs_pccrc(slice s) asm "SDDR_PCCRC"; int slice_data_refs_pccrr(slice s) asm "SDDR_PCCRR"; int slice_data_refs_pscrr(slice s) asm "SDDR_PSCRR"; int slice_data_refs_pccrrc(slice s) asm "SDDR_PCCRRC"; int slice_data_refs_pccrrr(slice s) asm "SDDR_PCCRRR"; int slice_data_refs_pscrrc(slice s) asm "SDDR_PSCRRC"; int slice_data_refs_pscrrr(slice s) asm "SDDR_PSCRRR"; int slice_data_refs_pccrrrc(slice s) asm "SDDR_PCCRRRC"; int slice_data_refs_pccrrrr(slice s) asm "SDDR_PCCRRRR"; int slice_data_refs_pscrrrc(slice s) asm "SDDR_PSCRRRC";
```