```
1 // SPDX-License-Identifier: AGPL-3.0-or-later
                                                           1 // SPDX-License-Identifier: AGPL-3.0-or-later
 2 pragma solidity 0.7.5;
                                                            2 pragma solidity 0.7.5;
4 library LowGasSafeMath {
                                                           4 library LowGasSafeMath {
                                                                /// @notice Returns x + y, reverts if sum over
     /// @notice Returns x + y, reverts if sum over
   flows uint256
                                                              flows uint256
     /// @param x The augend
                                                                 /// @param x The augend
      /// @param y The addend
                                                                 /// @param y The addend
      /// @return z The sum of x and y
                                                                 /// @return z The sum of x and y
     function add(uint256 x, uint256 y) internal pu
                                                                function add(uint256 x, uint256 y) internal pu
   re returns (uint256 z) {
                                                              re returns (uint256 z) {
          require((z = x + y) >= x);
                                                           10
                                                                     require((z = x + y) >= x);
11
                                                           11
12
                                                           12
      function add32(uint32 x, uint32 y) internal pu
                                                                 function add32(uint32 x, uint32 y) internal pu
                                                          13
   re returns (uint32 z) {
                                                              re returns (uint32 z) {
        require((z = x + y) >= x);
                                                                   require((z = x + y) >= x);
                                                           14
15
                                                           15
16
                                                           16
      /// @notice Returns x - y, reverts if underflo
                                                                 /// @notice Returns x - y, reverts if underflo
      /// @param x The minuend
                                                                 /// @param x The minuend
18
                                                           18
      /// @param y The subtrahend
                                                                 /// @param y The subtrahend
19
                                                           19
       /// @return z The difference of x and y
                                                                  /// @return z The difference of x and y
20
                                                           20
       function sub(uint256 x, uint256 y) internal pu
                                                                 function sub(uint256 x, uint256 y) internal pu
   re returns (uint256 z) {
                                                              re returns (uint256 z) {
        require((z = x - y) \le x);
                                                                     require((z = x - y) \le x);
23
                                                           23
24
                                                           24
     function sub32(uint32 x, uint32 y) internal pu
                                                                function sub32(uint32 x, uint32 y) internal pu
                                                           25
   re returns (uint32 z) {
                                                              re returns (uint32 z) {
26
          require((z = x - y) \le x);
                                                           26
                                                                     require((z = x - y) <= x);
27
                                                           27
28
                                                           28
      /// @notice Returns x * y, reverts if overflow
                                                                  /// @notice Returns x * y, reverts if overflow
      /// @param x The multiplicand
                                                                 /// @param x The multiplicand
30
                                                           30
      /// @param y The multiplier
                                                                  /// @param y The multiplier
31
                                                           31
      /// @return z The product of x and y
                                                           32
                                                                  /// @return z The product of x and y
      function mul(uint256 x, uint256 y) internal pu
                                                                 function mul(uint256 x, uint256 y) internal pu
   re returns (uint256 z) {
                                                              re returns (uint256 z) {
       require(x == 0 || (z = x * y) / x == y);
                                                           34
                                                                     require(x == 0 || (z = x * y) / x == y);
35
                                                           35
36
                                                           36
     /// @notice Returns x + y, reverts if overflow
                                                                 /// @notice Returns x + y, reverts if overflow
                                                           37
   s or underflows
                                                              s or underflows
      /// @param x The augend
                                                           38
                                                                 /// @param x The augend
      /// @param y The addend
                                                                  /// @param y The addend
                                                           39
      /// @return z The sum of x and y
                                                                  /// @return z The sum of x and y
      function add(int256 x, int256 y) internal pure
                                                                 function add(int256 x, int256 y) internal pure
   returns (int256 z) {
                                                              returns (int256 z) {
42
          require((z = x + y) >= x == (y >= 0));
                                                                     require((z = x + y) >= x == (y >= 0));
                                                          42
43
                                                           43
      /// @notice Returns x - y, reverts if overflow
                                                                 /// @notice Returns x - y, reverts if overflow
   s or underflows
                                                              s or underflows
      /// @param x The minuend
                                                                 /// @param x The minuend
      /// @param y The subtrahend
                                                           47
                                                                 /// @param y The subtrahend
     /// @return z The difference of x and y
                                                                 /// @return z The difference of x and y
                                                          48
     function sub(int256 x, int256 y) internal pure
                                                                function sub(int256 x, int256 y) internal pure
  returns (int256 z) {
                                                            returns (int256 z) {
50
     require((z = x - y) \le x == (y >= 0));
                                                          50
                                                                 require((z = x - y) \le x == (y >= 0));
                                                           51
```

```
function div(uint256 x, uint256 y) internal pu
                                                                   function div(uint256 x, uint256 y) internal pu
53
                                                            53
  re returns(uint256 z){
                                                               re returns(uint256 z){
54
          require(y > 0);
                                                            54
                                                                       require(y > 0);
55
           z=x/y;
                                                            55
                                                                       z=x/y;
56
                                                            56
       }
57 }
                                                            57 }
58
                                                            58
59 library Address {
                                                            59 library Address {
60
                                                            60
        * @dev Returns true if `account` is a contrac
                                                                     * @dev Returns true if `account` is a contrac
61
                                                            61
   t.
                                                               t.
62
                                                            62
63
       * [IMPORTANT]
                                                            63
                                                                    * [IMPORTANT]
                                                            64
        * It is unsafe to assume that an address for
                                                            65
                                                                     * It is unsafe to assume that an address for
    which this function returns
                                                                which this function returns
       * false is an externally-owned account (EOA)
                                                                     * false is an externally-owned account (EOA)
66
                                                            66
    and not a contract.
                                                                and not a contract.
67
                                                            67
       * Among others, `isContract` will return fals
                                                                    * Among others, `isContract` will return fals
   e for the following
                                                               e for the following
       * types of addresses:
                                                                    * types of addresses:
70
                                                            70
       * - an externally-owned account
                                                            71
                                                                   * - an externally-owned account
71
        ^{\star} - a contract in construction
                                                                     ^{\star} - a contract in construction
                                                            72
        ^{\star}\,\, - an address where a contract will be crea
                                                                    ^{\star}\,\, - an address where a contract will be crea
     * - an address where a contract lived, but w
                                                                 * - an address where a contract lived, but w
   as destroyed
                                                               as destroyed
75
                                                            75
        */
                                                                    */
76
                                                            76
       function isContract(address account) internal
                                                                   function isContract(address account) internal
    view returns (bool) {
                                                                view returns (bool) {
          // This method relies in extcodesize, whic
                                                                       // This method relies in extcodesize, whic
                                                               h returns 0 for contracts in
   h returns 0 for contracts in
          // construction, since the code is only st
                                                                      // construction, since the code is only st
   ored at the end of the
                                                               ored at the end of the
          // constructor execution.
                                                            80
                                                                       // constructor execution.
80
                                                            81
82
          uint256 size:
                                                            82
                                                                       uint256 size:
83
          // solhint-disable-next-line no-inline-ass
                                                            83
                                                                       // solhint-disable-next-line no-inline-ass
   embly
                                                               embly
           assembly { size := extcodesize(account) }
                                                                       assembly { size := extcodesize(account) }
85
           return size > 0;
                                                            85
                                                                       return size > 0;
86
     }
                                                            86
                                                                   }
87
                                                            87
88
                                                            88
       * @dev Replacement for Solidity's `transfer`:
                                                                    * @dev Replacement for Solidity's `transfer`:
                                                            89
   sends `amount` wei to
                                                               sends `amount` wei to
      * `recipient`, forwarding all available gas a
                                                                   * `recipient`, forwarding all available gas a
   nd reverting on errors.
                                                               nd reverting on errors.
91
                                                            91
       * https://eips.ethereum.org/EIPS/eip-1884[EIP
                                                            92
                                                                     * https://eips.ethereum.org/EIPS/eip-1884[EIP
92
   1884] increases the gas cost
                                                               1884] increases the gas cost
      * of certain opcodes, possibly making contrac
                                                                   * of certain opcodes, possibly making contrac
   ts go over the 2300 gas limit
                                                               ts go over the 2300 gas limit
       * imposed by `transfer`, making them unable t
                                                                   * imposed by `transfer`, making them unable t
   o receive funds via
                                                               o receive funds via
      * `transfer`. {sendValue} removes this limita
                                                                   * `transfer`. {sendValue} removes this limita
   tion.
                                                               tion.
96
                                                            96
       * https://diligence.consensys.net/posts/2019/
                                                                    * https://diligence.consensys.net/posts/2019/
   09/stop-using-soliditys-transfer-now/[Learn more].
                                                             09/stop-using-soliditys-transfer-now/[Learn more].
                                                            98
       * IMPORTANT: because control is transferred t
                                                                    * IMPORTANT: because control is transferred t
   o `recipient`, care must be
                                                               o `recipient`, care must be
```

```
ies. Consider using
                                                                ies. Consider using
        * {ReentrancyGuard}
101
                                                           101
                                                                     * {ReentrancyGuard}
102
                                                           102
       function sendValue(address payable recipient,
                                                                   function sendValue(address payable recipient,
103
                                                           103
     uint256 amount) internal {
                                                                 uint256 amount) internal {
       require(address(this).balance >= amount,
                                                                   require(address(this).balance >= amount,
     "Address: insufficient balance");
                                                                 "Address: insufficient balance");
                                                           105
105
           // solhint-disable-next-line avoid-low-lev
                                                                        // solhint-disable-next-line avoid-low-lev
106
                                                           106
    el-calls, avoid-call-value
                                                                el-calls, avoid-call-value
107
      (bool success, ) = recipient.call{ value:
                                                           107
                                                                       (bool success, ) = recipient.call{ value:
     amount }("");
                                                                 amount }("");
      require(success, "Address: unable to send
                                                                   require(success, "Address: unable to send
     value, recipient may have reverted");
                                                                 value, recipient may have reverted");
109
       }
                                                           109
                                                                    }
110
                                                            110
111
                                                           111
        * @dev Performs a Solidity function call usin
                                                                    * @dev Performs a Solidity function call usin
112
                                                           112
    g a low level `call`. A
                                                                q a low level `call`. A
        * plain`call` is an unsafe replacement for a
                                                                    * plain`call` is an unsafe replacement for a
     function call: use this
                                                                 function call: use this
114
        * function instead.
                                                           114
                                                                    * function instead.
115
                                                           115
                                                                   * If `target` reverts with a revert reason, i
       * If `target` reverts with a revert reason, i
116
    t is bubbled up by this
                                                                t is bubbled up by this
       * function (like regular Solidity function ca
                                                                    * function (like regular Solidity function ca
    lls).
                                                                lls).
118
119
         * Requirements:
                                                            119
                                                                     * Requirements:
120
                                                           120
         * - `target` must be a contract.
                                                                     * - `target` must be a contract.
121
                                                           121
         ^{\star} - calling 'target' with 'data' must not rev
                                                                     ^{\star} - calling 'target' with 'data' must not rev
122
    ert.
                                                                ert.
123
                                                           123
         * _Available since v3.1._
                                                            124
                                                                     * Available since v3.1.
125
                                                           125
      function functionCall(address target, bytes me
                                                                  function functionCall(address target, bytes me
                                                           126
    mory data) internal returns (bytes memory) {
                                                                mory data) internal returns (bytes memory) {
        return functionCall(target, data, "Address:
                                                                    return functionCall(target, data, "Address:
                                                           127
     low-level call failed");
                                                                 low-level call failed");
                                                            128
128
129
                                                           129
        * @dev Same as {xref-Address-functionCall-add
                                                                     * @dev Same as {xref-Address-functionCall-add
                                                           131
    ress-bytes-}[`functionCall`], but with
                                                                ress-bytes-}[`functionCall`], but with
         * `errorMessage` as a fallback revert reason
                                                                     * `errorMessage` as a fallback revert reason
     when `target` reverts.
                                                                 when `target` reverts.
133
                                                            133
        * _Available since v3.1._
                                                                     * _Available since v3.1._
134
                                                            134
                                                            135
136
      function functionCall(
                                                           136
                                                                    function functionCall(
          address target,
                                                           137
                                                                       address target,
137
           bytes memory data,
                                                           138
                                                                        bytes memory data,
138
139
           string memory errorMessage
                                                           139
                                                                       string memory errorMessage
140
      ) internal returns (bytes memory) {
                                                           140
                                                                   ) internal returns (bytes memory) {
          return _functionCallWithValue(target, dat
                                                                      return _functionCallWithValue(target, dat
    a, 0, errorMessage);
                                                                a, 0, errorMessage);
142
       }
                                                           142
                                                                    }
143
                                                           143
144
                                                           144
        * @dev Same as {xref-Address-functionCall-add
                                                                    * @dev Same as {xref-Address-functionCall-add
                                                           145
    ress-bytes-}[`functionCall`],
                                                               ress-bytes-}[`functionCall`],
                                                           146
        * but also transferring `value` wei to `targe
                                                                    * but also transferring `value` wei to `targe
146
    tì.
         * Requirements:
                                                                     * Requirements:
148
                                                            148
149
                                                            149
```

\* taken to not create reentrancy vulnerabilit

100

\* taken to not create reentrancy vulnerabilit

```
ance of at least `value`.
                                                                 ance of at least `value`.
151
        * - the called Solidity function must be `pay
                                                             151
                                                                      * - the called Solidity function must be `pay
    able`.
                                                                 able`.
152
                                                             152
         * _Available since v3.1._
                                                                      * _Available since v3.1._
153
                                                             153
154
                                                             154
       function functionCallWithValue(address target,
                                                                    function functionCallWithValue(address target,
    bytes memory data, uint256 value) internal returns
                                                                 bytes memory data, uint256 value) internal returns
    (bytes memory) {
                                                                 (bytes memory) {
                                                                        return functionCallWithValue(target, data,
           return functionCallWithValue(target, data,
    value, "Address: low-level call with value faile
                                                                 value, "Address: low-level call with value faile
                                                                 d");
157
                                                             157
                                                             158
159
                                                             159
         * @dev Same as {xref-Address-functionCallWith
                                                                      * @dev Same as {xref-Address-functionCallWith
160
                                                            160
    Value-address-bytes-uint256-}[`functionCallWithVal
                                                                 Value-address-bytes-uint256-}[`functionCallWithVal
         * with `errorMessage` as a fallback revert re
                                                                      * with `errorMessage` as a fallback revert re
    ason when `target` reverts.
                                                                 ason when `target` reverts.
162
163
         * Available since v3.1.
                                                             163
                                                                      * Available since v3.1.
164
                                                             164
165
        function functionCallWithValue(
                                                            165
                                                                     function functionCallWithValue(
166
          address target,
                                                            166
                                                                         address target,
           bytes memory data,
                                                            167
                                                                         bytes memory data,
167
           uint256 value,
                                                                         uint256 value,
168
                                                            168
169
           string memory errorMessage
                                                            169
                                                                        string memory errorMessage
170
        ) internal returns (bytes memory) {
                                                                    ) internal returns (bytes memory) {
                                                            170
           require(address(this).balance >= value, "A
                                                                         require(address(this).balance >= value, "A
                                                            171
    ddress: insufficient balance for call");
                                                                 ddress: insufficient balance for call");
           require(isContract(target), "Address: call
                                                                         require(isContract(target), "Address: call
172
                                                            172
    to non-contract");
                                                                 to non-contract");
173
                                                            173
            // solhint-disable-next-line avoid-low-lev
                                                                         // solhint-disable-next-line avoid-low-lev
    el-calls
                                                                 el-calls
           (bool success, bytes memory returndata) =
175
                                                            175
                                                                         (bool success, bytes memory returndata) =
     target.call{ value: value }(data);
                                                                  target.call{ value: value }(data);
           return _verifyCallResult(success, returnda
                                                                        return _verifyCallResult(success, returnda
176
                                                            176
    ta, errorMessage);
                                                                 ta, errorMessage);
177
                                                             177
                                                             178
        {\tt function} \ \_{\tt functionCallWithValue(}
                                                             179
                                                                     function _functionCallWithValue(
           address target,
                                                            180
                                                                         address target,
180
            bytes memory data,
                                                            181
                                                                         bytes memory data,
181
            uint256 weiValue,
                                                            182
                                                                         uint256 weiValue,
183
           string memory errorMessage
                                                            183
                                                                         string memory errorMessage
184
        ) private returns (bytes memory) {
                                                             184
                                                                     ) private returns (bytes memory) {
           require(isContract(target), "Address: call
                                                                         require(isContract(target), "Address: call
                                                             185
    to non-contract");
                                                                 to non-contract");
186
                                                             186
            // solhint-disable-next-line avoid-low-lev
                                                                         // solhint-disable-next-line avoid-low-lev
187
                                                            187
    el-calls
                                                                 el-calls
188
            (bool success, bytes memory returndata) =
                                                            188
                                                                         (bool success, bytes memory returndata) =
     target.call{ value: weiValue }(data);
                                                                  target.call{ value: weiValue }(data);
189
          if (success) {
                                                             189
                                                                        if (success) {
               return returndata;
190
                                                             190
                                                                             return returndata;
191
           } else {
                                                             191
                                                                         } else {
192
               // Look for revert reason and bubble i
                                                            192
                                                                             // Look for revert reason and bubble i
    t up if present
                                                                 t up if present
              if (returndata.length > 0) {
                                                                            if (returndata.length > 0) {
193
                                                            193
                   // The easiest way to bubble the r
                                                            194
                                                                                // The easiest way to bubble the r
    evert reason is using memory via assembly
                                                                 evert reason is using memory via assembly
                                                            195
195
                                                                                 // solhint-disable-next-line no-in
                    // solhint-disable-next-line no-in
                                                             196
    line-assembly
                                                                 line-assembly
197
                    assembly {
                                                             197
                                                                                 assembly {
```

\* - the calling contract must have an ETH bal

\* - the calling contract must have an ETH bal

```
let returndata size := mload(r
                                                                                      let returndata size := mload(r
    eturndata)
                                                                  eturndata)
                        revert(add(32, returndata), re
                                                             199
                                                                                      revert(add(32, returndata), re
    turndata_size)
                                                                  turndata_size)
200
                                                             200
                    }
                                                                                 }
                } else {
                                                             201
                                                                             } else {
202
                    revert(errorMessage);
                                                             202
                                                                                  revert(errorMessage);
203
                }
                                                             203
                                                                              }
                                                             204
204
            }
                                                                         }
205
        }
                                                             205
                                                                     }
206
                                                             206
207
                                                             207
                                                             208
         * @dev Same as {xref-Address-functionCall-add
                                                                      * @dev Same as {xref-Address-functionCall-add
    ress-bytes-}[`functionCall`],
                                                                  ress-bytes-}[`functionCall`],
         * but performing a static call.
                                                                       * but performing a static call.
210
                                                             210
         * _Available since v3.3._
                                                                       * _Available since v3.3._
211
                                                             211
212
                                                             212
        function functionStaticCall(address target, by
                                                                      function functionStaticCall(address target, by
    tes memory data) internal view returns (bytes memo
                                                                  tes memory data) internal view returns (bytes memo
            return functionStaticCall(target, data, "A
                                                                         return functionStaticCall(target, data, "A
    ddress: low-level static call failed");
                                                                  ddress: low-level static call failed");
215
        }
                                                             215
216
217
                                                             217
         * @dev Same as \{xref-Address-functionCall-add
                                                                      * @dev Same as \{xref-Address-functionCall-add
                                                             218
218
    ress-bytes-string-}[`functionCall`],
                                                                  ress-bytes-string-}[`functionCall`],
219
         * but performing a static call.
                                                                      * but performing a static call.
220
                                                             220
         * _Available since v3.3._
                                                                       * _Available since v3.3._
221
                                                             221
         */
222
                                                             222
223
        function functionStaticCall(
                                                             223
                                                                     function functionStaticCall(
224
          address target,
                                                             224
                                                                         address target,
           bytes memory data,
225
                                                             225
                                                                         bytes memory data,
           string memory errorMessage
                                                                         string memory errorMessage
227
        ) internal view returns (bytes memory) {
                                                             227
                                                                      ) internal view returns (bytes memory) {
           require(isContract(target), "Address: stat
                                                                         require(isContract(target), "Address: stat
228
    ic call to non-contract");
                                                                  ic call to non-contract");
229
                                                             229
            // solhint-disable-next-line avoid-low-lev
                                                                         // solhint-disable-next-line avoid-low-lev
    el-calls
                                                                  el-calls
231
           (bool success, bytes memory returndata) =
                                                             231
                                                                         (bool success, bytes memory returndata) =
     target.staticcall(data);
                                                                   target.staticcall(data);
           return _verifyCallResult(success, returnda
                                                                         return _verifyCallResult(success, returnda
    ta, errorMessage);
                                                                  ta, errorMessage);
        }
                                                                     }
234
                                                             234
235
         * @dev Same as {xref-Address-functionCall-add
                                                                      * @dev Same as {xref-Address-functionCall-add
    ress-bytes-}[`functionCall`],
                                                                  ress-bytes-}[`functionCall`],
237
         * but performing a delegate call.
                                                             237
                                                                       * but performing a delegate call.
         * _Available since v3.3._
                                                                       * _Available since v3.3._
239
                                                             239
240
                                                             240
241
        function functionDelegateCall(address target,
                                                             241
                                                                     function functionDelegateCall(address target,
     bytes memory data) internal returns (bytes memor
                                                                   bytes memory data) internal returns (bytes memor
           return functionDelegateCall(target, data,
                                                                         return functionDelegateCall(target, data,
     "Address: low-level delegate call failed");
                                                                   "Address: low-level delegate call failed");
243
                                                             243
        }
                                                                     }
244
                                                             244
245
                                                             245
         * @dev Same as \{xref-Address-functionCall-add
                                                                       * @dev Same as \{xref-Address-functionCall-add
246
                                                             246
    ress-bytes-string-}[`functionCall`],
                                                                  ress-bytes-string-}[`functionCall`],
         * but performing a delegate call.
                                                             247
                                                                      * but performing a delegate call.
248
                                                             248
249
         * _Available since v3.3._
                                                             249
                                                                       * _Available since v3.3._
```

```
251
        function functionDelegateCall(
                                                               251
                                                                       function functionDelegateCall(
252
            address target,
                                                               252
                                                                            address target,
253
            bytes memory data,
                                                              253
                                                                            bytes memory data,
254
            string memory errorMessage
                                                              254
                                                                            string memory errorMessage
                                                                       ) internal returns (bytes memory) {
         ) internal returns (bytes memory) {
                                                               255
            require(isContract(target), "Address: dele
                                                                            require(isContract(target), "Address: dele
    gate call to non-contract");
                                                                   gate call to non-contract");
257
                                                               257
258
             // solhint-disable-next-line avoid-low-lev
                                                                            // solhint-disable-next-line avoid-low-lev
                                                               258
    el-calls
                                                                   el-calls
259
            (bool success, bytes memory returndata) =
                                                              259
                                                                           (bool success, bytes memory returndata) =
     target.delegatecall(data);
                                                                     target.delegatecall(data);
            return _verifyCallResult(success, returnda
                                                                            return _verifyCallResult(success, returnda
    ta, errorMessage);
                                                                   ta, errorMessage);
261
        }
                                                               261
                                                                       }
262
                                                               262
        function _verifyCallResult(
                                                                       {\tt function \_verifyCallResult(}
263
                                                               263
264
            bool success,
                                                              264
                                                                           bool success,
265
            bytes memory returndata,
                                                              265
                                                                            bytes memory returndata,
             string memory errorMessage
                                                                            string memory errorMessage
                                                               266
        ) private pure returns(bytes memory) {
                                                                       ) private pure returns(bytes memory) {
            if (success) {
                                                              268
                                                                           if (success) {
                                                              269
                 return returndata:
                                                                                return returndata:
                                                               270
             } else {
                                                                            } else {
                 // Look for revert reason and bubble i
                                                                                // Look for revert reason and bubble i
     t up if present
                                                                   t up if present
                 if (returndata.length > 0) {
                                                                                if (returndata.length > 0) {
272
                                                               272
                     \ensuremath{\text{//}} The easiest way to bubble the r
                                                                                    // The easiest way to bubble the r
    evert reason is using memory via assembly
                                                                   evert reason is using memory via assembly
274
                                                               274
                     // solhint-disable-next-line no-in
                                                                                    // solhint-disable-next-line no-in
275
                                                              275
     line-assembly
                                                                    line-assembly
276
                     assembly {
                                                              276
                                                                                    assembly \{
                         let returndata_size := mload(r
                                                                                        let returndata_size := mload(r
    eturndata)
                                                                    eturndata)
                         revert(add(32, returndata), re
                                                                                        revert(add(32, returndata), re
    turndata_size)
                                                                   turndata_size)
279
                                                               279
                     }
                                                                                    }
280
                 } else {
                                                              280
                                                                                } else {
281
                     revert(errorMessage);
                                                              281
                                                                                    revert(errorMessage);
282
                                                               282
                 }
                                                               283
283
                                                                           }
284
285
                                                               285
         function addressToString(address _address) int
                                                                       function addressToString(address _address) int
286
    ernal pure returns(string memory) {
                                                                   ernal pure returns(string memory) {
287
             bytes32 _bytes = bytes32(uint256(_addres
                                                               287
                                                                            bytes32 _bytes = bytes32(uint256(_addres
    s));
                                                                   s));
288
             bytes memory HEX = "0123456789abcdef";
                                                              288
                                                                            bytes memory HEX = "0123456789abcdef";
             bytes memory _addr = new bytes(42);
                                                                            bytes memory _addr = new bytes(42);
                                                               289
290
                                                               290
             _addr[0] = '0';
                                                               291
                                                                            _addr[0] = '0';
291
292
             addr[1] = 'x';
                                                               292
                                                                            addr[1] = 'x':
             for(uint256 i = 0; i < 20; i++) {
                                                               294
                                                                            for(uint256 i = 0; i < 20; i++) {
                 \_addr[2+i*2] = HEX[uint8(\_bytes[i + 1
                                                                                \_addr[2+i*2] = HEX[uint8(\_bytes[i + 1
                                                                   2] >> 4)];
                 \_addr[3+i*2] = HEX[uint8(\_bytes[i + 1
                                                                                \_addr[3+i*2] = HEX[uint8(\_bytes[i + 1
    2] & 0x0f)];
                                                                   2] & 0x0f)];
297
            }
                                                               297
                                                                            }
             return string(_addr);
                                                                            return string(_addr);
                                                               300
300
301
                                                               301
                                                               302 }
302 }
303
                                                               303
304 interface IERC20 {
                                                               304 interface IERC20 {
305
                                                               305
```

```
e.
                                                               е.
                                                            307
307
308
    function totalSupply() external view returns (ui
                                                            308 function totalSupply() external view returns (ui
309
                                                            309
310
                                                            310
      * @dev Returns the amount of tokens owned by `a
                                                                   * @dev Returns the amount of tokens owned by `a
                                                            311
    ccount`.
                                                                ccount`.
312
                                                            312
    function balanceOf(address account) external vie
                                                            313 function balanceOf(address account) external vie
313
    w returns (uint256);
                                                                w returns (uint256);
314
                                                            314
315
                                                            315
      * @dev Moves `amount` tokens from the caller's
                                                            316
                                                                   * @dev Moves `amount` tokens from the caller's
     account to `recipient`.
                                                                 account to `recipient`.
317
                                                            317
       * Returns a boolean value indicating whether th
                                                                   * Returns a boolean value indicating whether th
318
                                                            318
    e operation succeeded.
                                                                e operation succeeded.
319
                                                            319
      * Emits a {Transfer} event.
                                                                   * Emits a {Transfer} event.
320
                                                            320
     function transfer(address recipient, uint256 amo
                                                            322 function transfer(address recipient, uint256 amo
    unt) external returns (bool);
                                                                unt) external returns (bool);
                                                            323
323
324
                                                            324
      * @dev Returns the remaining number of tokens t
                                                                   * @dev Returns the remaining number of tokens t
325
                                                            325
    hat `spender` will be
                                                                hat `spender` will be
      * allowed to spend on behalf of `owner` through
                                                                   * allowed to spend on behalf of `owner` through
    {transferFrom}. This is
                                                                 {transferFrom}. This is
327
       * zero by default.
                                                            327
                                                                    * zero by default.
328
                                                            328
       * This value changes when {approve} or {transfe
                                                                   ^{\star} This value changes when {approve} or {transfe}
329
                                                            329
    rFrom} are called.
                                                                rFrom} are called.
330
                                                            330
     function allowance(address owner, address spende
                                                                  function allowance(address owner, address spende
    r) external view returns (uint256);
                                                                r) external view returns (uint256);
332
                                                            332
333
                                                            333
      * @dev Sets `amount` as the allowance of `spend
                                                                   * @dev Sets `amount` as the allowance of `spend
                                                            334
    er` over the caller's tokens.
                                                                 er` over the caller's tokens.
335
                                                            335
      * Returns a boolean value indicating whether th
                                                                   * Returns a boolean value indicating whether th
    e operation succeeded.
                                                                 e operation succeeded.
337
                                                            337
       * IMPORTANT: Beware that changing an allowance
                                                                   * IMPORTANT: Beware that changing an allowance
338
                                                            338
     with this method brings the risk
                                                                 with this method brings the risk
      * that someone may use both the old and the new
                                                                   * that someone may use both the old and the new
339
                                                            339
    allowance by unfortunate
                                                                allowance by unfortunate
      * transaction ordering. One possible solution t
                                                                   * transaction ordering. One possible solution t
    o mitigate this race
                                                                o mitigate this race
      * condition is to first reduce the spender's al
                                                                   * condition is to first reduce the spender's al
    lowance to 0 and set the
                                                                lowance to 0 and set the
                                                                    * desired value afterwards:
       * desired value afterwards:
342
                                                            342
       * https://github.com/ethereum/EIPs/issues/20#is
                                                                    * https://github.com/ethereum/EIPs/issues/20#is
                                                            343
    suecomment-263524729
                                                                 suecomment - 263524729
344
                                                            344
       * Emits an {Approval} event.
                                                                   * Emits an {Approval} event.
                                                            345
      function approve(address spender, uint256 amoun
                                                                  function approve(address spender, uint256 amoun
    t) external returns (bool);
                                                                t) external returns (bool):
348
                                                            348
349
                                                            349
      * @dev Moves `amount` tokens from `sender` to `
                                                                   * @dev Moves `amount` tokens from `sender` to `
350
                                                            350
    recipient` using the
                                                                recipient` using the
      * allowance mechanism. `amount` is then deducte
                                                                   * allowance mechanism. `amount` is then deducte
    d from the caller's
                                                                d from the caller's
352
       * allowance.
                                                            352
                                                                   * allowance.
```

\* @dev Returns the amount of tokens in existenc

306

\* @dev Returns the amount of tokens in existenc

```
353
                                                            353
       * Returns a boolean value indicating whether th
354
                                                            354
                                                                   * Returns a boolean value indicating whether th
    e operation succeeded.
                                                                 e operation succeeded.
355
                                                            355
      * Emits a {Transfer} event.
                                                                   * Emits a {Transfer} event.
356
                                                            356
357
                                                            357
     function transferFrom(address sender, address re
                                                                  function transferFrom(address sender, address re
    cipient, uint256 amount) external returns (bool);
                                                                 cipient, uint256 amount) external returns (bool);
359
                                                            359
360
                                                            360
      * @dev Emitted when `value` tokens are moved fr
                                                                   * @dev Emitted when `value` tokens are moved fr
361
                                                            361
    om one account (`from`) to
                                                                 om one account (`from`) to
      * another (`to`).
                                                            362
                                                                   * another (`to`).
362
                                                            363
      * Note that `value` may be zero.
                                                                   * Note that `value` may be zero.
364
                                                            364
365
                                                            365
     event Transfer(address indexed from, address ind
                                                            366 event Transfer(address indexed from, address ind
366
    exed to, uint256 value);
                                                                 exed to, uint256 value);
367
368 /**
                                                            368
      * @dev Emitted when the allowance of a `spender
                                                                   * @dev Emitted when the allowance of a `spender
                                                            369
    ` for an `owner` is set by
                                                                ` for an `owner` is set by
* a call to {approve}. `value` is the new allow
                                                                   * a call to {approve}. `value` is the new allow
    ance.
                                                                 ance.
                                                            371
371
     event Approval(address indexed owner, address in
                                                                  event Approval(address indexed owner, address in
    dexed spender, uint256 value);
                                                                 dexed spender, uint256 value);
                                                            373 }
373 }
                                                            374
374
375 abstract contract ERC20
                                                            375 abstract contract ERC20
376
                                                            376
377
      IERC20
                                                            377
                                                                    IERC20
378
                                                            378
379
                                                            379
380
      using LowGasSafeMath for uint256;
                                                            380
                                                                  using LowGasSafeMath for uint256;
381
                                                            381
      // TODO comment actual hash value.
                                                            382
                                                                  // TODO comment actual hash value.
383
      bytes32 constant private ERC20TOKEN_ERC1820_INTE
                                                            383
                                                                   bytes32 constant private ERC20TOKEN_ERC1820_INTE
    RFACE_ID = keccak256( "ERC20Token" );
                                                                 RFACE_ID = keccak256( "ERC20Token" );
384
                                                            384
385
      mapping (address => uint256) internal _balances;
                                                            385
                                                                   mapping (address => uint256) internal _balances;
386
                                                            386
387
      mapping (address => mapping (address => uint25
                                                            387
                                                                   mapping (address => mapping (address => uint25
    6)) internal _allowances;
                                                                 internal _allowances;
                                                            388
389
      uint256 internal _totalSupply;
                                                            389
                                                                   uint256 internal _totalSupply;
390
                                                            390
391
      string internal name;
                                                            391
                                                                   string internal name;
392
                                                            392
393
      string internal _symbol;
                                                            393
                                                                   string internal _symbol;
394
                                                            394
      uint8 internal _decimals;
                                                                   uint8 internal _decimals;
395
                                                            395
396
                                                            396
397
                                                            397
      * @dev Sets the values for {name} and {symbol},
                                                                   * @dev Sets the values for {name} and {symbol},
398
                                                            398
    initializes {decimals} with
                                                                 initializes {decimals} with
      * a default value of 18.
399
                                                            399
                                                                   * a default value of 18.
400
                                                            400
       * To select a different value for {decimals}, u
                                                                    * To select a different value for {decimals}, u
    se {_setupDecimals}.
                                                                 se \{\_setupDecimals\}.
402
                                                            402
       * All three of these values are immutable: they
                                                                    * All three of these values are immutable: they
                                                            403
    can only be set once during
                                                                 can only be set once during
       * construction.
                                                                   ^{\star} construction.
404
                                                            404
405
                                                            405
     constructor (string memory name_, string memory
                                                                  constructor (string memory name_, string memory
                                                            406
     symbol_, uint8 decimals_) {
                                                                  symbol_, uint8 decimals_) {
407
       _name = name_;
                                                            407
                                                                    _name = name_;
       _symbol = symbol_;
408
                                                            408
                                                                    _symbol = symbol_;
```

```
_decimals = decimals_;
                                                                     _decimals = decimals_;
410
      }
                                                            410
                                                                   }
411
                                                             411
412
                                                            412
       * @dev Returns the name of the token.
                                                                   * @dev Returns the name of the token.
413
                                                            413
                                                             414
      function name() public view returns (string memo
                                                                   function name() public view returns (string memo
    ry) {
416
       return _name;
                                                            416
                                                                     return name;
417
                                                             417
      }
                                                                   }
418
                                                             418
419
                                                             419
      * @dev Returns the symbol of the token, usually
420
                                                            420
                                                                   * @dev Returns the symbol of the token, usually
    a shorter version of the
                                                                 a shorter version of the
421
                                                             421
422
                                                             422
     function symbol() public view returns (string me
                                                                  function symbol() public view returns (string me
423
                                                            423
    morv) {
                                                                 morv) {
424
      return _symbol;
                                                            424
                                                                    return symbol;
425
      }
                                                            425
                                                                   }
426
                                                             426
427
                                                             427
     * @dev Returns the number of decimals used to g
                                                                  * @dev Returns the number of decimals used to g
    et its user representation.
                                                                et its user representation.
       * For example, if `decimals` equals `2`, a bala
                                                                   * For example, if `decimals` equals `2`, a bala
429
                                                            429
    nce of `505` tokens should
                                                                nce of `505` tokens should
                                                                   * be displayed to a user as `5,05` (`505 / 10 *
       * be displayed to a user as `5,05` (`505 / 10 *
430
                                                            430
    * 2`).
                                                                 * 2`).
431
                                                             431
       * Tokens usually opt for a value of 18, imitati
                                                                   * Tokens usually opt for a value of 18, imitati
    ng the relationship between
                                                                ng the relationship between
     * Ether and Wei. This is the value {ERC20} use
                                                                  * Ether and Wei. This is the value {ERC20} use
    s, unless {_setupDecimals} is
                                                                 s, unless {_setupDecimals} is
       * called.
                                                                   * called.
434
                                                            434
435
                                                            435
       * NOTE: This information is only used for _disp
                                                                    * NOTE: This information is only used for _disp
    lay_ purposes: it in
                                                                 lay_ purposes: it in
     * no way affects any of the arithmetic of the c
                                                                    * no way affects any of the arithmetic of the c
437
                                                            437
    ontract, including
                                                                 ontract, including
       * {IERC20-balanceOf} and {IERC20-transfer}.
                                                                    * {IERC20-balanceOf} and {IERC20-transfer}.
438
                                                            438
439
                                                            439
440
     function decimals() public view returns (uint8)
                                                            440
                                                                  function decimals() public view returns (uint8)
     {
                                                                  {
441
        return _decimals;
                                                             441
                                                                     return _decimals;
442
      }
                                                            442
                                                                   }
443
                                                            443
444
                                                            444
       * @dev See {IERC20-totalSupply}.
                                                                    * @dev See {IERC20-totalSupply}.
445
                                                            445
446
                                                            446
      function totalSupply() public view override retu
                                                                   function totalSupply() public view override retu
447
                                                             447
    rns (uint256) {
                                                                 rns (uint256) {
      return _totalSupply;
                                                             448
                                                                     return _totalSupply;
449
                                                             449
      }
                                                                   }
450
                                                             450
451
                                                            451
       * @dev See {IERC20-balanceOf}.
452
                                                            452
                                                                    * @dev See {IERC20-balanceOf}.
453
                                                            453
      function balanceOf(address account) public view
                                                             454
                                                                   function balanceOf(address account) public view
     virtual override returns (uint256) {
                                                                  virtual override returns (uint256) {
455
       return _balances[account];
                                                            455
                                                                     return _balances[account];
456
      }
                                                            456
                                                                   }
457
                                                             457
458
                                                            458
       * @dev See {IERC20-transfer}.
459
                                                            459
                                                                    * @dev See {IERC20-transfer}.
460
                                                             460
       * Requirements:
                                                             461
                                                                    * Requirements:
462
                                                             462
       * - `recipient` cannot be the zero address.
                                                                    * - `recipient` cannot be the zero address.
463
                                                            463
```

```
`amount`.
                                                                   `amount`.
465
                                                             465
466
      function transfer(address recipient, uint256 amo
                                                             466
                                                                   function transfer(address recipient, uint256 amo
    unt) public virtual override returns (bool) {
                                                                 unt) public virtual override returns (bool) {
      _transfer(msg.sender, recipient, amount);
                                                                     _transfer(msg.sender, recipient, amount);
467
                                                             467
      return true;
                                                             468
469 }
                                                             469
                                                                   }
470
                                                             470
471
                                                             471
        * @dev See {IERC20-allowance}.
                                                                      * @dev See {IERC20-allowance}.
                                                             472
472
473
                                                             473
474
        function allowance(address owner, address spen
                                                             474
                                                                     function allowance(address owner, address spen
    der) public view virtual override returns (uint25
                                                                  der) public view virtual override returns (uint25
           return _allowances[owner][spender];
                                                             475
                                                                         return _allowances[owner][spender];
476
                                                             476
        }
                                                                     }
477
                                                             477
478
                                                             478
         * @dev See {IERC20-approve}.
                                                                      * @dev See {IERC20-approve}.
479
                                                             479
                                                             480
480
         * Requirements:
                                                                      * Requirements:
                                                             481
482
                                                             482
483
         * - `spender` cannot be the zero address.
                                                             483
                                                                      * - `spender` cannot be the zero address.
                                                             484
484
        function approve(address spender, uint256 amou
                                                             485
                                                                     function approve(address spender, uint256 amou
    nt) public virtual override returns (bool) {
                                                                 nt) public virtual override returns (bool) {
            _approve(msg.sender, spender, amount);
                                                             486
                                                                         _approve(msg.sender, spender, amount);
486
487
            return true;
                                                             487
                                                                         return true;
488
                                                             488
        }
                                                                     }
489
                                                             489
490
                                                             490
         * @dev See {IERC20-transferFrom}.
                                                                      * @dev See {IERC20-transferFrom}.
491
                                                             491
492
                                                             492
        * Emits an {Approval} event indicating the up
                                                                      ^{\star} Emits an {Approval} event indicating the up
    dated allowance. This is not
                                                                  dated allowance. This is not
       * required by the EIP. See the note at the be
                                                                      * required by the EIP. See the note at the be
                                                             494
    ginning of {ERC20}.
                                                                 ginning of {ERC20}.
495
                                                             495
         * Requirements:
                                                                       * Requirements:
496
                                                             496
497
                                                             497
108
         \mbox{\ensuremath{\star}} - `sender` and `recipient` cannot be the ze
                                                             108
                                                                      * - `sender` and `recipient` cannot be the ze
                                                                 ro address.
       * - `sender` must have a balance of at least
                                                                      ^{\star} - `sender` must have a balance of at least
     `amount`.
                                                                   `amount`.
         * - the caller must have allowance for ``send
                                                                       * - the caller must have allowance for ``send
500
                                                             500
    er``'s tokens of at least
                                                                 er``'s tokens of at least
         * `amount`.
                                                                      * `amount`.
501
                                                             501
502
                                                             502
       function transferFrom(address sender, address
                                                                     function transferFrom(address sender, address
                                                             503
     recipient, uint256 amount) public virtual overrid
                                                                  recipient, uint256 amount) public virtual overrid
    e returns (bool) {
                                                                  e returns (bool) {
            _transfer(sender, recipient, amount);
504
                                                             504
                                                                         _transfer(sender, recipient, amount);
           _approve(sender, msg.sender, _allowances[s
                                                                         _approve(sender, msg.sender, _allowances[s
505
                                                             505
    ender][msg.sender]
                                                                 ender][msg.sender]
506
              .sub(amount));
                                                             506
                                                                            .sub(amount));
            return true;
                                                             507
                                                                         return true;
507
508
       }
                                                             508
                                                                     }
509
                                                             509
510
                                                             510
        * @dev Atomically increases the allowance gra
                                                                     * @dev Atomically increases the allowance gra
                                                             511
    nted to `spender` by the caller.
                                                                 nted to `spender` by the caller.
512
                                                             512
        * This is an alternative to {approve} that ca
                                                                      * This is an alternative to {approve} that ca
    n be used as a mitigation for
                                                                 n be used as a mitigation for
      * problems described in {IERC20-approve}.
                                                                      * problems described in {IERC20-approve}.
                                                             515
515
```

\* - the caller must have a balance of at least

464

\* - the caller must have a balance of at least

```
* Emits an {Approval} event indicating the up
                                                             516
                                                                     * Emits an {Approval} event indicating the up
    dated allowance.
                                                                  dated allowance.
517
                                                             517
                                                                       * Requirements:
         * Requirements:
518
                                                             518
519
                                                             519
         * - `spender` cannot be the zero address.
                                                                       * - `spender` cannot be the zero address.
520
                                                             520
                                                             521
       function increaseAllowance(address spender, ui
                                                                     function increaseAllowance(address spender, ui
    nt256 addedValue) public virtual returns (bool) {
                                                                  nt256 addedValue) public virtual returns (bool) {
            _approve(msg.sender, spender, _allowances
                                                                          _approve(msg.sender, spender, _allowances
    [msg.sender][spender].add(addedValue));
                                                                  [msg.sender][spender].add(addedValue));
                                                                          return true;
524
            return true:
                                                             524
                                                             525
525
                                                             526
526
527
                                                             527
        * @dev Atomically decreases the allowance gra
                                                                      * @dev Atomically decreases the allowance gra
                                                                  nted to `spender` by the caller.
    nted to `spender` by the caller.
529
                                                             529
         ^{\star} This is an alternative to {approve} that ca
                                                                       * This is an alternative to {approve} that ca
                                                             530
    n be used as a mitigation for
                                                                  n be used as a mitigation for
         * problems described in {IERC20-approve}.
                                                                       * problems described in {IERC20-approve}.
532
                                                             532
         * Emits an {Approval} event indicating the up
                                                                       * Emits an {Approval} event indicating the up
533
                                                             533
    dated allowance.
                                                                  dated allowance.
534
                                                             534
         * Requirements:
                                                                       * Requirements:
535
                                                             535
                                                             536
536
         * - `spender` cannot be the zero address.
                                                                       * - `spender` cannot be the zero address.
                                                             537
         ^{\star} - `spender` must have allowance for the cal
                                                                       ^{\star} - `spender` must have allowance for the cal
    ler of at least
                                                                  ler of at least
         * `subtractedValue`.
                                                                       * `subtractedValue`.
539
                                                             539
540
                                                             540
541
       function decreaseAllowance(address spender, ui
                                                                     function decreaseAllowance(address spender, ui
    nt256 subtractedValue) public virtual returns (boo
                                                                  nt256 subtractedValue) public virtual returns (boo
            _approve(msg.sender, spender, _allowances
                                                                          _approve(msg.sender, spender, _allowances
    [msq.sender][spender]
                                                                  [msq.sender][spender]
              .sub(subtractedValue));
                                                                             .sub(subtractedValue));
543
                                                             543
            return true;
                                                             544
                                                                          return true;
544
545
      }
                                                             545
                                                                      }
                                                             546
546
547
                                                             547
      * @dev Moves tokens `amount` from `sender` to `
                                                                    * @dev Moves tokens `amount` from `sender` to `
    recipient`.
                                                                  recipient`.
549
                                                             549
       * This is internal function is equivalent to {t
                                                                     * This is internal function is equivalent to {t
550
                                                             550
    ransfer}, and can be used to
                                                                  ransfer}, and can be used to
551
      * e.g. implement automatic token fees, slashing
                                                             551
                                                                     * e.g. implement automatic token fees, slashing
    mechanisms, etc.
                                                                  mechanisms, etc.
552
                                                             552
       * Emits a {Transfer} event.
                                                                     * Emits a {Transfer} event.
553
                                                             553
554
                                                             554
       * Requirements:
                                                                     * Requirements:
555
                                                             555
556
                                                             556
       \mbox{\scriptsize \star} - 'sender' cannot be the zero address.
                                                                     ^{\star} - `sender` cannot be the zero address.
557
                                                             557
       ^{\star} - `recipient` cannot be the zero address.
                                                                     * - `recipient` cannot be the zero address.
558
                                                             558
       * - `sender` must have a balance of at least `a
                                                                     * - `sender` must have a balance of at least `a
    mount`.
                                                                  mount`.
560
                                                             560
561
      function transfer(address sender, address recip
                                                             561
                                                                    function _transfer(address sender, address recip
    ient, uint256 amount) internal virtual {
                                                                  ient, uint256 amount) internal virtual {
562
       require(sender != address(0), "ERC20: transfer
                                                             562
                                                                     require(sender != address(0), "ERC20: transfer
    from the zero address");
                                                                  from the zero address");
      require(recipient != address(0), "ERC20: trans
                                                                    require(recipient != address(0), "ERC20: trans
    fer to the zero address");
                                                                  fer to the zero address");
564
                                                             564
565
        \_before Token Transfer (sender, recipient, amoun
                                                                      \_before Token Transfer (sender, recipient, amoun
                                                             565
```

t);

516

t);

```
_balances[sender] = _balances[sender].sub(amou
                                                             567
                                                                      _balances[sender] = _balances[sender].sub(amou
567
    nt):
                                                                  nt):
568
        _balances[recipient] = _balances[recipient].ad
                                                             568
                                                                      _balances[recipient] = _balances[recipient].ad
    d(amount);
                                                                  d(amount);
569
      emit Transfer(sender, recipient, amount);
                                                             569
                                                                     emit Transfer(sender, recipient, amount);
570
                                                             570
571
                                                             571
                                                                      /** @dev Creates `amount` tokens and assigns t
        /** @dev Creates `amount` tokens and assigns t
                                                             572
572
    hem to `account`, increasing
                                                                  hem to `account`, increasing
         * the total supply.
                                                                      * the total supply.
573
                                                             573
574
                                                             574
575
         * Emits a {Transfer} event with `from` set to
                                                             575
                                                                       ^{\star} Emits a {Transfer} event with `from` set to
    the zero address.
                                                                  the zero address.
                                                             576
577
         * Requirements:
                                                             577
                                                                       * Requirements:
578
                                                             578
         * - `to` cannot be the zero address.
                                                                       * - `to` cannot be the zero address.
579
                                                             579
580
                                                             580
       function _mint(address account_, uint256 ammou
                                                                     function _mint(address account_, uint256 ammou
    nt_) internal virtual {
                                                                  nt_) internal virtual {
           require(account_ != address(0), "ERC20: mi
                                                                         require(account_ != address(0), "ERC20: mi
    nt to the zero address");
                                                                  nt to the zero address");
            beforeTokenTransfer(address( this ), acco
                                                                          _beforeTokenTransfer(address( this ), acco
    unt , ammount );
                                                                  unt , ammount );
584
            _totalSupply = _totalSupply.add(ammount_);
                                                             584
                                                                          _totalSupply = _totalSupply.add(ammount_);
            _balances[account_] = _balances[account_].
                                                                          _balances[account_] = _balances[account_].
    add(ammount_);
                                                                  add(ammount_);
            emit Transfer(address( 0 ), account_, ammo
                                                                          emit Transfer(address( 0 ), account_, ammo
    unt_);
                                                                  unt_);
587
                                                             587
        }
                                                                      }
588
                                                             588
589
                                                             589
        * @dev Destroys `amount` tokens from `account
                                                                      * @dev Destroys `amount` tokens from `account
     , reducing the
                                                                   , reducing the
        * total supply.
                                                                      * total supply.
591
                                                             591
592
                                                             592
         * Emits a {Transfer} event with `to` set to t
                                                                       * Emits a {Transfer} event with `to` set to t
593
                                                             593
    he zero address.
                                                                  he zero address.
594
                                                             594
         * Requirements:
                                                                       ^{\star} Requirements:
595
                                                             595
                                                             596
596
         * - `account` cannot be the zero address.
                                                                       * - `account` cannot be the zero address.
                                                             597
         * - `account` must have at least `amount` tok
                                                                       * - `account` must have at least `amount` tok
    ens.
                                                                  ens.
599
                                                             599
       function _burn(address account, uint256 amoun
                                                                     function _burn(address account, uint256 amoun
600
                                                             600
                                                                  t) internal virtual {
    t) internal virtual {
601
           require(account != address(0), "ERC20: bur
                                                             601
                                                                         require(account != address(0), "ERC20: bur
    n from the zero address");
                                                                  n from the zero address");
602
                                                             602
603
            _beforeTokenTransfer(account, address(0),
                                                             603
                                                                          _beforeTokenTransfer(account, address(0),
     amount);
                                                                   amount);
604
                                                             604
                                                                          _balances[account] = _balances[account].su
605
            _balances[account] = _balances[account].su
                                                             605
    b(amount);
                                                                  b(amount);
606
            _totalSupply = _totalSupply.sub(amount);
                                                             606
                                                                          _totalSupply = _totalSupply.sub(amount);
            emit Transfer(account, address(0), amoun
                                                                          emit Transfer(account, address(0), amoun
    t);
                                                                  t);
608
                                                             608
        }
609
                                                             609
610
                                                             610
         * @dev Sets `amount` as the allowance of `spe
                                                                       ^{\star} @dev Sets `amount` as the allowance of `spe
                                                             611
    nder` over the `owner` s tokens.
                                                                  nder` over the `owner` s tokens.
612
                                                             612
         * This internal function is equivalent to `ap
                                                                       * This internal function is equivalent to `ap
    prove`, and can be used to
                                                                  prove`, and can be used to
         * e.g. set automatic allowances for certain s
                                                                       ^{\star} e.g. set automatic allowances for certain s
                                                             614
    ubsystems, etc.
                                                                  ubsystems, etc.
```

```
616
                                                                      * Emits an {Approval} event.
616
         * Emits an {Approval} event.
617
                                                             617
         * Requirements:
                                                                      * Requirements:
618
                                                             618
619
                                                             619
         * - `owner` cannot be the zero address.
                                                                      * - `owner` cannot be the zero address.
620
                                                             620
         * - `spender` cannot be the zero address.
                                                             621
                                                                      ^{\star} - `spender` cannot be the zero address.
622
                                                             622
623
        function approve(address owner, address spend
                                                             623
                                                                     function approve(address owner, address spend
    er, uint256 amount) internal virtual {
                                                                 er, uint256 amount) internal virtual {
           require(owner != address(0), "ERC20: appro
                                                                         require(owner != address(0), "ERC20: appro
624
                                                             624
    ve from the zero address");
                                                                 ve from the zero address");
           require(spender != address(0), "ERC20: app
                                                                         require(spender != address(0), "ERC20: app
                                                             625
    rove to the zero address");
                                                                 rove to the zero address");
626
                                                             626
627
            _allowances[owner][spender] = amount;
                                                             627
                                                                         _allowances[owner][spender] = amount;
            emit Approval(owner, spender, amount);
                                                             628
                                                                         emit Approval(owner, spender, amount);
628
629
        }
                                                             629
                                                                     }
630
                                                             630
631
                                                             631
        * @dev Sets {decimals} to a value other than
                                                                     * @dev Sets {decimals} to a value other than
632
                                                             632
     the default one of 18.
                                                                  the default one of 18.
633
                                                             633
        * WARNING: This function should only be calle
                                                             634
                                                                      * WARNING: This function should only be calle
634
    d from the constructor. Most
                                                                 d from the constructor. Most
       * applications that interact with token contr
                                                                     * applications that interact with token contr
635
                                                             635
    acts will not expect
                                                                 acts will not expect
       * {decimals} to ever change, and may work inc
                                                                     * {decimals} to ever change, and may work inc
    orrectly if it does.
                                                                 orrectly if it does.
637
        */
                                                             637
                                                                     */
638
                                                             638
639
                                                             639
      * @dev Hook that is called before any transfer
                                                                    * @dev Hook that is called before any transfer
640
                                                             640
     of tokens. This includes
                                                                  of tokens. This includes
                                                             641
      * minting and burning.
                                                                    * minting and burning.
641
642
                                                             642
      * Calling conditions:
                                                                    * Calling conditions:
643
                                                             643
       * - when `from` and `to` are both non-zero, `am
                                                                    * - when `from` and `to` are both non-zero, `am
                                                             645
    ount` of ``from``'s tokens
                                                                 ount` of ``from``'s tokens
646
       ^{\star} will be to transferred to 'to'.
                                                             646
                                                                    * will be to transferred to `to`.
       * - when `from` is zero, `amount` tokens will b
                                                                    * - when `from` is zero, `amount` tokens will b
    e minted for `to`.
                                                                 e minted for `to`.
      * - when `to` is zero, `amount` of ``from``'s t
                                                                    * - when `to` is zero, `amount` of ``from``'s t
    okens will be burned.
                                                                 okens will be burned.
      * - `from` and `to` are never both zero.
                                                                    * - `from` and `to` are never both zero.
649
                                                             649
650
                                                             650
       * To learn more about hooks, head to xref:ROOT:
                                                                    * To learn more about hooks, head to xref:ROOT:
651
                                                             651
    extending-contracts.adoc#using-hooks[Using Hooks].
                                                                 extending-contracts.adoc#using-hooks[Using Hooks].
652
                                                             652
     function _beforeTokenTransfer( address from_, ad
                                                                   function _beforeTokenTransfer( address from_, ad
    dress to_, uint256 amount_ ) internal virtual { }
                                                                 dress to_, uint256 amount_ ) internal virtual { }
654 }
                                                             654 }
655
656 library Counters {
                                                             656 library Counters {
657
       using LowGasSafeMath for uint256;
                                                             657
                                                                     using LowGasSafeMath for uint256;
658
                                                             658
659
       struct Counter {
                                                             659
                                                                     struct Counter {
           // This variable should never be directly
                                                                         // This variable should never be directly
     accessed by users of the library: interactions mu
                                                                  accessed by users of the library: interactions mu
    st be restricted to
                                                                 st be restricted to
           // the library's function. As of Solidity
                                                                         // the library's function. As of Solidity
661
                                                             661
     v0.5.2, this cannot be enforced, though there is
                                                                  v0.5.2,\ \mbox{this} cannot be enforced, though there is
     a proposal to add
                                                                  a proposal to add
           // this feature: see https://github.com/et
                                                                        // this feature: see https://github.com/et
    hereum/solidity/issues/4637
                                                                 hereum/solidity/issues/4637
663
           uint256 _value; // default: 0
                                                             663
                                                                        uint256 _value; // default: 0
664
        }
                                                             664
                                                                     }
```

615

615

```
rnal view returns (uint256) {
   rnal view returns (uint256) {
       return counter._value;
                                                                   return counter._value;
667
                                                           667
668
                                                           668
669
                                                           669
      function increment(Counter storage counter) in
                                                           670
                                                                  function increment(Counter storage counter) in
670
                                                               ternal {
     // The {SafeMath} overflow check can be sk
                                                                // The {SafeMath} overflow check can be sk
    ipped here, see the comment at the top
                                                                ipped here, see the comment at the top
     counter._value += 1;
                                                           672
                                                                   counter._value += 1;
672
673
                                                           673
675
       function decrement(Counter storage counter) in
                                                           675
                                                                   function decrement(Counter storage counter) in
                                                                ternal {
       counter._value = counter._value.sub(1);
                                                                       counter._value = counter._value.sub(1);
677
                                                           677
678 }
                                                           678 }
679
                                                            679
                                                           680 interface IERC2612Permit {
680 interface IERC2612Permit {
681 /**
                                                           681
       * @dev Sets `amount` as the allowance of `spe
                                                                   * @dev Sets `amount` as the allowance of `spe
                                                           682
    nder` over `owner`'s tokens,
                                                                nder` over `owner`'s tokens,
683
         * given `owner`'s signed approval.
                                                           683
                                                                     * given `owner`'s signed approval.
684
                                                           684
        * IMPORTANT: The same issues {IERC20-approve}
                                                                    * IMPORTANT: The same issues {IERC20-approve}
685
                                                           685
  has related to transaction
                                                               has related to transaction
        * ordering also apply here.
686
                                                           686
                                                                     * ordering also apply here.
687
                                                            687
        * Emits an {Approval} event.
                                                                     * Emits an {Approval} event.
688
                                                            688
        * Requirements:
690
                                                           690
                                                                     * Requirements:
                                                           691
691
        ^{\star} - 'owner' cannot be the zero address.
                                                                    * - `owner` cannot be the zero address.
692
                                                           692
         \mbox{\scriptsize \star} - 'spender' cannot be the zero address.
                                                                     ^{\star} - `spender` cannot be the zero address.
693
                                                           693
        ^{\star} - `deadline` must be a timestamp in the fut
                                                                     ^{\star} - 'deadline' must be a timestamp in the fut
      * - `v`, `r` and `s` must be a valid `secp256
                                                                     * - `v`, `r` and `s` must be a valid `secp256
    k1` signature from `owner`
                                                                k1` signature from `owner`
         * over the EIP712-formatted function argument
                                                                     * over the EIP712-formatted function argument
696
                                                           696
    S.
      * - the signature must use ``owner``'s curren
                                                                    * - the signature must use ``owner``'s curren
697
                                                           697
    t nonce (see {nonces}).
                                                                t nonce (see {nonces}).
698
                                                           698
        * For more information on the signature forma
                                                                     * For more information on the signature forma
    t, see the
                                                                t, see the
        * https://eips.ethereum.org/EIPS/eip-2612#spe
                                                                     * https://eips.ethereum.org/EIPS/eip-2612#spe
                                                            700
    cification[relevant EIP
                                                                cification[relevant EIP
                                                                     * section].
        * section].
701
                                                            701
702
                                                            702
       function permit(
                                                            703
                                                                    function permit(
703
          address owner,
                                                            704
                                                                       address owner,
705
           address spender,
                                                            705
                                                                       address spender,
                                                            706
706
           uint256 amount,
                                                                       uint256 amount,
           uint256 deadline,
                                                            707
                                                                       uint256 deadline,
707
                                                                       uint8 v,
           uint8 v,
708
                                                            708
709
           bytes32 r,
                                                            709
                                                                       bytes32 r,
          bytes32 s
                                                                       bytes32 s
710
                                                            710
711
       ) external;
                                                            711
                                                                    ) external;
712
                                                            712
713
                                                            713
714
       * @dev Returns the current ERC2612 nonce for
                                                           714
                                                                    * @dev Returns the current ERC2612 nonce for
                                                                 `owner`. This value must be
     `owner`. This value must be
        * included whenever a signature is generated
                                                           715
                                                                    * included whenever a signature is generated
     for {permit}.
                                                                 for {permit}.
                                                            716
       * Every successful call to {permit} increases
                                                                    * Every successful call to {permit} increases
    ``owner``'s nonce by one. This
                                                                ``owner``'s nonce by one. This
```

function current(Counter storage counter) inte

function current(Counter storage counter) inte

```
* prevents a signature from being used multip
                                                              718
                                                                       * prevents a signature from being used multip
    le times.
                                                                   le times.
719
                                                               719
720
        function nonces(address owner) external view r
                                                              720
                                                                       function nonces(address owner) external view r
    eturns (uint256);
                                                                   eturns (uint256);
721 }
                                                              721 }
723 abstract contract ERC20Permit is ERC20, IERC2612Pe
                                                               723 abstract contract ERC20Permit is ERC20, IERC2612Pe
724
        using Counters for Counters.Counter:
                                                              724
                                                                       using Counters for Counters.Counter:
        mapping(address => Counters.Counter) private _
                                                                       mapping(address => Counters.Counter) private _
    nonces;
                                                                   nonces;
727
                                                              727
        // keccak256("Permit(address owner,address spe
                                                                       // keccak256("Permit(address owner,address spe
    nder,uint256 value,uint256 nonce,uint256 deadlin
                                                                   nder,uint256 value,uint256 nonce,uint256 deadlin
729
        bytes32 public constant PERMIT_TYPEHASH = 0x6e
                                                              729
                                                                       bytes32 public constant PERMIT TYPEHASH = 0x6e
    71edae12b1b97f4d1f60370fef10105fa2faae0126114a169c
                                                                   71edae12b1b97f4d1f60370fef10105fa2faae0126114a169c
    64845d6126c9;
                                                                   64845d6126c9;
730
                                                               730
731
        bytes32 public immutable DOMAIN_SEPARATOR;
                                                               731
                                                                       bytes32 public immutable DOMAIN_SEPARATOR;
732
                                                               732
733
                                                               733
        constructor() {
                                                                       constructor() {
734
                                                               734
            uint256 chainID:
                                                                           uint256 chainID:
             assembly {
                                                                           assembly {
                 chainID := chainid()
                                                                               chainID := chainid()
738
                                                               738
             DOMAIN_SEPARATOR = keccak256(abi.encode(
                                                                           DOMAIN_SEPARATOR = keccak256(abi.encode(
740
                                                              740
                 keccak256("EIP712Domain(string name, st
                                                                               keccak256("EIP712Domain(string name, st
    ring version, uint256 chainId, address verifyingCont
                                                                   ring version, uint256 chainId, address verifyingCont
    ract)"),
                                                                   ract)"),
742
                                                                               keccak256(bytes(name())),
                 keccak256(bytes(name())),
                                                              742
743
                 keccak256(bytes("1")), // Version
                                                               743
                                                                               keccak256(bytes("1")), // Version
                 chainID.
                                                               744
                                                                               chainID,
744
                 address(this)
745
                                                               745
                                                                               address(this)
746
                                                               746
             ));
                                                                           ));
747
        }
                                                               747
                                                                       }
748
                                                               748
749
                                                               749
         * @dev See {IERC2612Permit-permit}.
                                                                        * @dev See {IERC2612Permit-permit}.
750
                                                               750
                                                               751
751
         */
                                                                        */
752
                                                               752
753
        function permit(
                                                               753
                                                                       function permit(
            address owner,
                                                              754
                                                                           address owner,
754
            address spender,
755
                                                              755
                                                                           address spender.
            uint256 amount,
                                                                           uint256 amount,
757
            uint256 deadline,
                                                              757
                                                                           uint256 deadline,
758
            uint8 v,
                                                              758
                                                                           uint8 v,
759
            bytes32 r,
                                                              759
                                                                           bytes32 r,
760
            bvtes32 s
                                                              760
                                                                           bvtes32 s
761
        ) public virtual override {
                                                               761
                                                                       ) public virtual override {
            require(block.timestamp <= deadline, "Perm</pre>
                                                                           require(block.timestamp <= deadline, "Perm</pre>
762
                                                               762
    it: expired deadline");
                                                                   it: expired deadline");
763
                                                               763
             bytes32 hashStruct =
                                                              764
                                                                           bytes32 hashStruct =
765
                 keccak256(abi.encode(PERMIT_TYPEHASH,
                                                               765
                                                                               keccak256(abi.encode(PERMIT_TYPEHASH,
     owner, spender, amount, _nonces[owner].current(),
                                                                    owner, spender, amount, _nonces[owner].current(),
    deadline));
766
                                                               766
             bytes32 _hash = keccak256(abi.encodePacked
                                                                           bytes32 _hash = keccak256(abi.encodePacked
767
                                                              767
    (uint16(0x1901), DOMAIN_SEPARATOR, hashStruct));
                                                                   (uint16(0x1901), DOMAIN_SEPARATOR, hashStruct));
768
                                                               768
             address signer = ecrecover(_hash, v, r,
                                                                           address signer = ecrecover(_hash, v, r,
769
                                                               769
     s);
                                                                    s);
770
             require(signer != address(0) && signer ==
                                                               770
                                                                           require(signer != address(0) && signer ==
     owner, "ERC20Permit: Invalid signature");
                                                                    owner, "ERC20Permit: Invalid signature");
771
                                                               771
```

```
773
            _approve(owner, spender, amount);
                                                             773
                                                                         _approve(owner, spender, amount);
774
                                                             774
        }
                                                                     }
                                                             775
776
                                                             776
777
        * @dev See {IERC2612Permit-nonces}.
                                                             777
                                                                      * @dev See {IERC2612Permit-nonces}.
778
                                                             778
        function nonces(address owner) public view ove
                                                                     function nonces(address owner) public view ove
    rride returns (uint256) {
                                                                 rride returns (uint256) {
780
           return _nonces[owner].current();
                                                             780
                                                                         return _nonces[owner].current();
781
                                                             781
        }
                                                                     }
782 }
                                                             782 }
783
                                                             783
784 contract OwnableData {
                                                             784 contract OwnableData {
       address public owner;
                                                                     address public owner;
786
        address public pendingOwner;
                                                             786
                                                                     address public pendingOwner;
787 }
                                                             787 }
788
                                                             788
789 contract Ownable is OwnableData {
                                                             789 contract Ownable is OwnableData {
                                                                     event OwnershipTransferred(address indexed pre
790
       event OwnershipTransferred(address indexed pre
                                                             790
    viousOwner, address indexed newOwner);
                                                                 viousOwner, address indexed newOwner);
791
                                                             791
        /// @notice `owner` defaults to msg.sender on
                                                                     /// @notice `owner` defaults to msg.sender on
792
                                                             792
     construction.
                                                                  construction.
       constructor() {
                                                             793
                                                                    constructor() {
793
                                                                        owner = msg.sender:
794
           owner = msg.sender;
                                                             794
           emit OwnershipTransferred(address(0), msg.
                                                                        emit OwnershipTransferred(address(0), msg.
795
                                                             795
    sender);
                                                                 sender);
796
                                                             796
797
                                                             797
        /// @notice Transfers ownership to `newOwner`.
                                                                     /// @notice Transfers ownership to `newOwner`.
    Either directly or claimable by the new pending ow
                                                                 Either directly or claimable by the new pending ow
       /// Can only be invoked by the current `owner
                                                                    /// Can only be invoked by the current `owner
799
                                                             799
800
        /// @param newOwner Address of the new owner.
                                                             800
                                                                     /// @param newOwner Address of the new owner.
        /// @param direct True if `newOwner` should be
                                                                     /// @param direct True if `newOwner` should be
    set immediately. False if `newOwner` needs to use
                                                                 set immediately. False if `newOwner` needs to use
     `claimOwnership`.
                                                                  `claimOwnership`.
        /// @param renounce Allows the `newOwner` to b
                                                                     /// @param renounce Allows the `newOwner` to b
802
                                                             802
    e `address(0)` if `direct` and `renounce` is True.
                                                                 e `address(0)` if `direct` and `renounce` is True.
    Has no effect otherwise.
                                                                 Has no effect otherwise.
       function transferOwnership(
                                                             803
                                                                    function transferOwnership(
803
          address newOwner,
                                                             804
                                                                        address newOwner,
805
           bool direct,
                                                             805
                                                                         bool direct,
            bool renounce
                                                                         bool renounce
806
                                                             806
        ) public onlyOwner {
                                                                     ) public onlyOwner {
807
                                                             807
           if (direct) {
                                                             808
                                                                         if (direct) {
808
809
                // Checks
                                                             809
                                                                             // Checks
                require(newOwner != address(0) || reno
                                                                             require(newOwner != address(0) || reno
    unce, "Ownable: zero address");
                                                                 unce, "Ownable: zero address");
811
                                                             811
                // Effects
                                                             812
                                                                             // Effects
812
                emit OwnershipTransferred(owner, newOw
                                                                             emit OwnershipTransferred(owner, newOw
                                                             813
    ner):
                                                                 ner):
814
                owner = newOwner;
                                                             814
                                                                             owner = newOwner;
                pendingOwner = address(0);
                                                             815
                                                                             pendingOwner = address(0);
815
816
            } else {
                                                             816
                                                                         } else {
                // Effects
                                                             817
                                                                             // Effects
                pendingOwner = newOwner;
                                                             818
                                                                             pendingOwner = newOwner;
818
                                                             819
819
            }
                                                                         }
820
                                                             820
        }
                                                                     }
821
        /// @notice Needs to be called by `pendingOwne
                                                                     /// @notice Needs to be called by `pendingOwne
    r` to claim ownership.
                                                                 r` to claim ownership.
        function claimOwnership() public {
                                                             823
                                                                     function claimOwnership() public {
824
            address _pendingOwner = pendingOwner;
                                                             824
                                                                         address _pendingOwner = pendingOwner;
825
                                                             825
            // Checks
                                                                         // Checks
826
                                                             826
```

\_nonces[owner].increment();

772

\_nonces[owner].increment();

```
require(msg.sender == _pendingOwner, "Owna
                                                              827
                                                                          require(msg.sender == _pendingOwner, "Owna
    ble: caller != pending owner");
                                                                  ble: caller != pending owner");
828
                                                              828
829
            // Effects
                                                              829
                                                                           // Effects
830
             emit OwnershipTransferred(owner, _pending0
                                                              830
                                                                           emit OwnershipTransferred(owner, _pending0
    wner);
            owner = _pendingOwner;
831
                                                              831
                                                                           owner = _pendingOwner;
832
            pendingOwner = address(0);
                                                              832
                                                                           pendingOwner = address(0);
833
                                                              833
        }
                                                              834
834
        /// @notice Only allows the `owner` to execute
                                                                       /// @notice Only allows the `owner` to execute
835
                                                              835
    the function.
                                                                   the function.
836
        modifier onlyOwner() {
                                                              836
                                                                      modifier onlyOwner() {
            require(msg.sender == owner, "Ownable: cal
                                                              837
                                                                           require(msg.sender == owner, "Ownable: cal
    ler is not the owner");
                                                                   ler is not the owner");
838
                                                              838
            _;
                                                                           _;
839
        }
                                                              839
                                                                      }
                                                              840 }
840 }
841
                                                              841
    contract MEMOries is ERC20Permit, Ownable {
                                                                   contract sMaia is ERC20Permit, Ownable {
842
                                                              842
843
                                                              843
844
        using LowGasSafeMath for uint256;
                                                              844
                                                                       using LowGasSafeMath for uint256;
845
                                                              845
846
        modifier onlyStakingContract() {
                                                              846
                                                                       modifier onlyStakingContract() {
847
            require( msg.sender == stakingContract, "0
                                                              847
                                                                           require( msg.sender == stakingContract, "0
    SC" );
                                                                  SC" );
848
                                                              848
849
                                                              849
850
                                                              850
851
        address public stakingContract;
                                                              851
                                                                       address public stakingContract;
852
        address public initializer;
                                                              852
                                                                       address public initializer;
853
                                                              853
        event LogSupply(uint256 indexed epoch, uint256
                                                                       event LogSupply(uint256 indexed epoch, uint256
854
                                                              854
    timestamp, uint256 totalSupply );
                                                                   timestamp, uint256 totalSupply );
855
        event LogRebase( uint256 indexed epoch, uint25
                                                              855
                                                                       event LogRebase( uint256 indexed epoch, uint25
    6 rebase, uint256 index );
                                                                   6 rebase, uint256 index );
        event LogStakingContractUpdated( address staki
                                                                       event LogStakingContractUpdated( address staki
                                                              856
    ngContract );
                                                                   ngContract );
857
        event LogSetIndex(uint256 indexed index );
                                                              857
                                                                       event LogSetIndex(uint256 indexed index );
858
                                                              858
        struct Rebase {
                                                                       struct Rebase {
859
                                                              859
860
            uint epoch;
                                                              860
                                                                           uint epoch;
            uint rebase; // 18 decimals
                                                                           uint rebase; // 18 decimals
861
                                                              861
            uint totalStakedBefore;
                                                                           uint totalStakedBefore;
862
                                                              862
                                                                           uint totalStakedAfter;
            uint totalStakedAfter;
                                                              863
864
            uint amountRebased;
                                                              864
                                                                           uint amountRebased;
            uint index;
                                                                           uint index;
865
                                                              865
            uint32 timeOccured:
                                                              866
                                                                           uint32 timeOccured:
866
867
                                                              867
                                                                       }
868
        Rebase[] public rebases;
                                                              868
                                                                       Rebase[] public rebases;
869
                                                              869
870
        uint public INDEX;
                                                              870
                                                                       uint public INDEX;
871
                                                              871
        uint256 private constant MAX_UINT256 = ~uint25
                                                                       uint256 private constant MAX_UINT256 = ~uint25
872
    6(0):
                                                                   6(0):
        uint256 private constant INITIAL FRAGMENTS SUP
                                                                      uint256 private constant INITIAL FRAGMENTS SUP
873
                                                              873
    PLY = 5000000 * 10**9;
                                                                  PLY = 5000000 * 10**9;
874
                                                              874
        // TOTAL_GONS is a multiple of INITIAL_FRAGMEN
                                                                       // TOTAL_GONS is a multiple of INITIAL_FRAGMEN
875
    TS_SUPPLY so that _gonsPerFragment is an integer.
                                                                  TS_SUPPLY so that _gonsPerFragment is an integer.
        // Use the highest value that fits in a uint25
                                                                      // Use the highest value that fits in a uint25
    6 for max granularity.
                                                                  6 for max granularity.
        uint256 private constant TOTAL GONS = MAX UINT
                                                              877
                                                                      uint256 private constant TOTAL GONS = MAX UINT
877
    256 - (MAX_UINT256 % INITIAL_FRAGMENTS_SUPPLY);
                                                                  256 - (MAX_UINT256 % INITIAL_FRAGMENTS_SUPPLY);
878
                                                              878
        // MAX_SUPPLY = maximum integer < (sqrt(4*TOTA</pre>
                                                                       // MAX_SUPPLY = maximum integer < (sqrt(4*TOTA
    L GONS + 1) - 1) / 2
                                                                   L GONS + 1) - 1) / 2
        uint256 private constant MAX_SUPPLY = ~uint128
                                                                      uint256 private constant MAX_SUPPLY = ~uint128
    (0); // (2^128) - 1
                                                                   (0); // (2^128) - 1
881
                                                              881
```

```
uint256 private _gonsPerFragment;
                                                                       uint256 private _gonsPerFragment;
882
883
        mapping(address => uint256) private gonBalanc
                                                              883
                                                                       mapping(address => uint256) private gonBalanc
    es;
                                                                   es;
884
                                                              884
885
        mapping ( address => mapping ( address => uint
                                                              885
                                                                       mapping ( address => mapping ( address => uint
    256 ) ) private _allowedValue;
                                                                   256 ) ) private _allowedValue;
                                                              886
886
        constructor() ERC20("MEMOries", "MEMO", 9) ERC
                                                                       constructor() ERC20("Staked Maia", "MAIA", 9)
887
                                                              887
    20Permit() {
                                                                    ERC20Permit() {
888
            initializer = msq.sender;
                                                              888
                                                                           initializer = msq.sender;
             _totalSupply = INITIAL_FRAGMENTS_SUPPLY;
                                                                           _totalSupply = INITIAL_FRAGMENTS_SUPPLY;
889
                                                              889
890
             _gonsPerFragment = TOTAL_GONS.div(_totalSu
                                                              890
                                                                           _gonsPerFragment = TOTAL_GONS.div(_totalSu
    pply);
                                                                   pply);
891
                                                              891
892
                                                              892
893
        function initialize( address stakingContract_
                                                              893
                                                                       function initialize( address stakingContract_
     ) external returns ( bool ) {
                                                                    ) external returns ( bool ) {
            require( msg.sender == initializer, "NA"
                                                                           require( msg.sender == initializer, "NA"
894
                                                              894
     );
                                                                    );
895
             require( stakingContract_ != address(0),
                                                              895
                                                                           require( stakingContract_ != address(0),
     "IA" );
                                                                    "IA" );
896
             stakingContract = stakingContract_;
                                                              896
                                                                           stakingContract = stakingContract_;
897
             _gonBalances[ stakingContract ] = TOTAL_GO
                                                              897
                                                                           _gonBalances[ stakingContract ] = TOTAL_GO
    NS:
                                                                   NS;
898
                                                              898
            emit Transfer( address(0x0), stakingContra
                                                              899
                                                                           emit Transfer( address(0x0), stakingContra
899
    ct, _totalSupply );
                                                                   ct, _totalSupply );
900
            emit LogStakingContractUpdated( stakingCon
                                                              900
                                                                           emit LogStakingContractUpdated( stakingCon
    tract );
                                                                   tract );
901
                                                              901
902
            initializer = address(0);
                                                              902
                                                                           initializer = address(0);
                                                              903
903
             return true:
                                                                           return true:
                                                              904
904
        }
905
                                                              905
906
        function setIndex( uint _INDEX ) external only
                                                              906
                                                                       function setIndex( uint _INDEX ) external only
    Owner() {
                                                                   Owner() {
907
            require( INDEX == 0, "INZ");
                                                              907
                                                                           require( INDEX == 0, "INZ");
908
            INDEX = gonsForBalance( _INDEX );
                                                              908
                                                                           INDEX = gonsForBalance( _INDEX );
            emit LogSetIndex(INDEX);
                                                                           emit LogSetIndex(INDEX);
909
                                                              909
                                                              910
910
        }
                                                                       }
911
                                                              911
912
                                                              912
913
            @notice increases MEMOries supply to incre
                                                              913
                                                                           @notice increases MEMOries supply to incre
    ase staking balances relative to profit_
                                                                   ase staking balances relative to profit_
914
            @param profit_ uint256
                                                              914
                                                                           @param profit_ uint256
915
            @return uint256
                                                              915
                                                                           @return uint256
916
                                                              916
        function rebase( uint256 profit_, uint epoch_
                                                                       function rebase( uint256 profit_, uint epoch_
917
                                                              917
     ) public onlyStakingContract() returns ( uint256
                                                                    ) public onlyStakingContract() returns ( uint256
     ) {
                                                                    ) {
            uint256 rebaseAmount;
                                                                           uint256 rebaseAmount;
918
                                                              918
            uint256 circulatingSupply_ = circulatingSu
                                                              919
                                                                           uint256 circulatingSupply_ = circulatingSu
    :()vlqq
                                                                   :()vlag
920
                                                              920
            if ( profit_ == 0 ) {
921
                                                              921
                                                                           if ( profit_ == 0 ) {
922
                 emit LogSupply( epoch_, block.timestam
                                                              922
                                                                               emit LogSupply( epoch_, block.timestam
    p, _totalSupply );
                                                                   p, _totalSupply );
                 emit LogRebase( epoch_, 0, index() );
                                                                               emit LogRebase( epoch_, 0, index() );
923
                                                              923
924
                 return _totalSupply;
                                                              924
                                                                               return _totalSupply;
925
            } else if ( circulatingSupply_ > 0 ){
                                                              925
                                                                           } else if ( circulatingSupply_ > 0 ){
                 rebaseAmount = profit_.mul( _totalSupp
                                                                               rebaseAmount = profit_.mul( _totalSupp
                                                              926
    ly ).div( circulatingSupply_ );
                                                                   ly ).div( circulatingSupply_ );
927
            } else {
                                                              927
                                                                           } else {
                 rebaseAmount = profit_;
                                                              928
                                                                               rebaseAmount = profit_;
928
                                                              929
929
930
                                                              930
            _totalSupply = _totalSupply.add( rebaseAmo
                                                                           _totalSupply = _totalSupply.add( rebaseAmo
    unt );
                                                                   unt );
932
                                                              932
```

```
_totalSupply = MAX_SUPPLY;
934
                 totalSupply = MAX SUPPLY;
                                                              934
935
            }
                                                              935
                                                              936
937
            _gonsPerFragment = TOTAL_GONS.div( _totalS
                                                              937
                                                                          _gonsPerFragment = TOTAL_GONS.div( _totalS
                                                              938
938
            _storeRebase( circulatingSupply_, profit_,
                                                              939
                                                                           _storeRebase( circulatingSupply_, profit_,
                                                                   epoch );
    epoch );
940
                                                              940
941
            return totalSupply;
                                                              941
                                                                           return totalSupply;
        }
942
                                                              942
                                                                       }
943
                                                              943
944
                                                              944
            @notice emits event with data about rebase
                                                                           @notice emits event with data about rebase
            @param previousCirculating_ uint
                                                                           @param previousCirculating_ uint
946
                                                              946
947
            @param profit_ uint
                                                              947
                                                                           @param profit_ uint
            @param epoch_ uint
                                                                           @param epoch_ uint
948
                                                              948
949
            @return bool
                                                              949
                                                                           @return bool
950
                                                              950
        function _storeRebase( uint previousCirculatin
                                                                       function _storeRebase( uint previousCirculatin
    g_, uint profit_, uint epoch_ ) internal returns (
                                                                   g_, uint profit_, uint epoch_ ) internal returns (
            uint rebasePercent = profit_.mul( 1e18 ).d
952
                                                              952
                                                                          uint rebasePercent = profit .mul( 1e18 ).d
    iv( previousCirculating_ );
                                                                   iv( previousCirculating_ );
953
                                                              953
954
            rebases.push( Rebase ( {
                                                              954
                                                                           rebases.push( Rebase ( {
955
                                                              955
                 epoch: epoch_,
                                                                               epoch: epoch_,
                 rebase: rebasePercent, // 18 decimals
                                                                               rebase: rebasePercent, // 18 decimals
956
                                                              956
                 totalStakedBefore: previousCirculating
                                                              957
                                                                               totalStakedBefore: previousCirculating
958
                totalStakedAfter: circulatingSupply(),
                                                              958
                                                                               totalStakedAfter: circulatingSupply(),
                 amountRebased: profit ,
                                                                               amountRebased: profit ,
959
                                                              959
960
                 index: index(),
                                                              960
                                                                               index: index(),
961
                 timeOccured: uint32(block.timestamp)
                                                              961
                                                                               timeOccured: uint32(block.timestamp)
            }));
                                                              962
                                                                           }));
            emit LogSupply( epoch_, block.timestamp, _
                                                              964
                                                                           emit LogSupply( epoch , block.timestamp,
    totalSupply ):
                                                                   totalSupply ):
            emit LogRebase( epoch_, rebasePercent, ind
                                                                           emit LogRebase( epoch_, rebasePercent, ind
965
                                                              965
    ex());
                                                                   ex());
966
                                                              966
967
            return true;
                                                              967
                                                                           return true;
968
                                                              968
969
                                                              969
        function balanceOf( address who ) public view
                                                                      function balanceOf( address who ) public view
     override returns ( uint256 ) {
                                                                   override returns ( uint256 ) {
            return _gonBalances[ who ].div( _gonsPerFr
                                                              971
                                                                           return _gonBalances[ who ].div( _gonsPerFr
971
    agment );
                                                                   agment );
972
                                                              972
973
                                                              973
        function gonsForBalance( uint amount ) public
                                                              974
                                                                       function gonsForBalance( uint amount ) public
     view returns ( uint ) {
                                                                    view returns ( uint ) {
            return amount.mul( _gonsPerFragment );
                                                                           return amount.mul( _gonsPerFragment );
975
                                                              975
976
                                                              976
977
                                                              977
978
        function balanceForGons( uint gons ) public vi
                                                              978
                                                                       function balanceForGons( uint gons ) public vi
    ew returns ( uint ) {
                                                                   ew returns ( uint ) {
979
            return gons.div( _gonsPerFragment );
                                                              979
                                                                           return gons.div( _gonsPerFragment );
980
981
                                                              981
982
        // Staking contract holds excess MEMOries
                                                              982
                                                                       // Staking contract holds excess MEMOries
        function circulatingSupply() public view retur
                                                                       function circulatingSupply() public view retur
983
                                                              983
    ns ( uint ) {
                                                                   ns ( uint ) {
984
            return _totalSupply.sub( balanceOf( stakin
                                                              984
                                                                           return _totalSupply.sub( balanceOf( stakin
    gContract ) );
                                                                   gContract ) );
985
                                                              985
        }
986
                                                              986
987
        function index() public view returns ( uint )
                                                              987
                                                                       function index() public view returns ( uint )
     {
                                                                    {
```

if ( \_totalSupply > MAX\_SUPPLY ) {

if ( \_totalSupply > MAX\_SUPPLY ) {

```
989
                                                               989
         }
 990
                                                               990
 991
         function transfer( address to, uint256 value )
                                                               991
                                                                       function transfer( address to, uint256 value )
     public override returns (bool) {
                                                                   public override returns (bool) {
             uint256 gonValue = value.mul( _gonsPerFrag
                                                                           uint256 gonValue = value.mul( _gonsPerFrag
992
                                                               992
     ment );
                                                                    ment );
993
             _gonBalances[ msg.sender ] = _gonBalances[
                                                               993
                                                                           _gonBalances[ msg.sender ] = _gonBalances[
     msg.sender ].sub( gonValue );
                                                                   msg.sender ].sub( gonValue );
             _gonBalances[ to ] = _gonBalances[ to ].ad
                                                                           _gonBalances[ to ] = _gonBalances[ to ].ad
994
                                                               994
     d( gonValue );
                                                                   d( gonValue );
995
             emit Transfer( msg.sender, to, value );
                                                               995
                                                                            emit Transfer( msg.sender, to, value );
                                                               996
996
             return true;
                                                                            return true;
 997
                                                               997
998
                                                               998
         function allowance( address owner_, address sp
                                                                       function allowance( address owner_, address sp
     ender ) public view override returns ( uint256 ) {
                                                                   ender ) public view override returns ( uint256 ) {
                                                                            return _allowedValue[ owner_ ][ spender ];
             return _allowedValue[ owner_ ][ spender ];
1000
1001
                                                              1001
1002
                                                              1002
1003
         function transferFrom( address from, address t
                                                              1003
                                                                        function transferFrom( address from, address t
     o, uint256 value ) public override returns ( bool
                                                                   o, uint256 value ) public override returns ( bool
1004
            _allowedValue[ from ][ msg.sender ] = _allo
                                                              1004
                                                                          _allowedValue[ from ][ msg.sender ] = _allo
     wedValue[ from ][ msg.sender ].sub( value );
                                                                   wedValue[ from ][ msg.sender ].sub( value );
            emit Approval( from, msg.sender, _allowedV
                                                                          emit Approval( from, msg.sender, _allowedV
     alue[ from ][ msg.sender ] );
                                                                    alue[ from ][ msg.sender ] );
1006
                                                              1006
1007
             uint256 gonValue = gonsForBalance( value
                                                              1007
                                                                            uint256 gonValue = gonsForBalance( value
             _gonBalances[ from ] = _gonBalances[from].
                                                              1008
                                                                            _gonBalances[ from ] = _gonBalances[from].
     sub( gonValue );
                                                                   sub( gonValue );
             _gonBalances[ to ] = _gonBalances[to].add(
                                                              1009
                                                                           _gonBalances[ to ] = _gonBalances[to].add(
     gonValue );
                                                                   gonValue );
1010
             emit Transfer( from, to, value );
                                                              1010
                                                                            emit Transfer( from, to, value );
                                                              1011
1012
             return true;
                                                              1012
                                                                            return true;
1013
                                                              1013
         }
                                                                       }
1014
                                                              1014
         function approve( address spender, uint256 val
                                                                       function approve( address spender, uint256 val
     ue ) public override returns (bool) {
                                                                   ue ) public override returns (bool) {
1016
              _allowedValue[ msg.sender ][ spender ] =
                                                              1016
                                                                             _allowedValue[ msg.sender ][ spender ] =
      value:
                                                                     value;
1017
              emit Approval( msg.sender, spender, value
                                                              1017
                                                                             emit Approval( msg.sender, spender, value
                                                                   );
     );
1018
                                                              1018
              return true;
                                                                             return true;
                                                              1019
1019
1020
                                                              1020
1021
         // What gets called in a permit
                                                              1021
                                                                        // What gets called in a permit
         function _approve( address owner, address spen
                                                              1022
                                                                       function _approve( address owner, address spen
1022
     der, uint256 value ) internal override virtual {
                                                                   der, uint256 value ) internal override virtual {
1023
             _allowedValue[owner][spender] = value;
                                                              1023
                                                                            _allowedValue[owner][spender] = value;
1024
             emit Approval( owner, spender, value );
                                                              1024
                                                                            emit Approval( owner, spender, value );
1025
                                                              1025
1026
                                                              1026
1027
         function increaseAllowance( address spender, u
                                                              1027
                                                                       function increaseAllowance( address spender, u
     int256 addedValue ) public override returns (bool)
                                                                   int256 addedValue ) public override returns (bool)
                                                                            _allowedValue[ msg.sender ][ spender ] = _
1028
             _allowedValue[ msg.sender ][ spender ] = _
                                                              1028
     allowedValue[ msg.sender ][ spender ].add( addedVa
                                                                   allowedValue[ msg.sender ][ spender ].add( addedVa
1029
             emit Approval( msg.sender, spender, allow
                                                              1029
                                                                            emit Approval( msg.sender, spender, _allow
     edValue[ msg.sender ][ spender ] );
                                                                   edValue[ msg.sender ][ spender ] );
                                                                           return true;
1030
             return true;
                                                              1030
1031
                                                              1031
1032
1033
         function decreaseAllowance( address spender, u
                                                              1033
                                                                       function decreaseAllowance( address spender, u
     int256 subtractedValue ) public override returns
                                                                   int256 subtractedValue ) public override returns
      (bool) {
                                                                     (bool) {
```

return balanceForGons( INDEX );

988

return balanceForGons( INDEX );

```
uint256 oldValue = _allowedValue[ msg.send
                                                       1034
                                                                   uint256 oldValue = _allowedValue[ msg.send
                                                         er ][ spender ];
    er ][ spender ];
                                                                  if (subtractedValue >= oldValue) {
          if (subtractedValue >= oldValue) {
1035
                                                       1035
               _allowedValue[ msg.sender ][ spender ]
1036
                                                       1036
                                                                       _allowedValue[ msg.sender ][ spender ]
    = 0;
                                                         = ⊙;
1037
            } else {
                                                        1037
                                                                    } else {
               _allowedValue[ msg.sender ][ spender ]
                                                                        _allowedValue[ msg.sender ][ spender ]
    = oldValue.sub( subtractedValue );
                                                         = oldValue.sub( subtractedValue );
1039
           }
                                                        1039
                                                                    }
1040
           emit Approval( msg.sender, spender, _allow
                                                        1040
                                                                    emit Approval( msg.sender, spender, _allow
                                                        edValue[ msg.sender ][ spender ] );
    edValue[ msg.sender ][ spender ] );
1041
           return true;
                                                        1041
                                                                    return true;
1042
                                                        1042
1043 }
                                                        1043 }
```

>