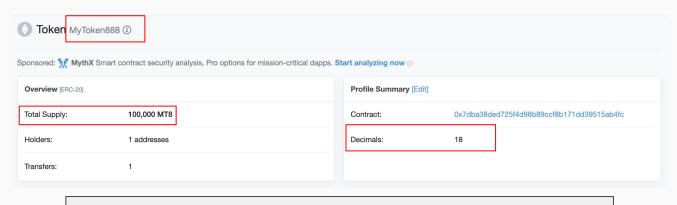
# **Token Contrac Review**

이진호

• 토큰 기본정보를 저장하기위한 상태변수



```
string public name;
string public symbol;
uint8 public decimals;

mapping (address => uint256) private _balances;
mapping (address => mapping (address => uint256)) private _allowed;
uint256 private _totalSupply;
```

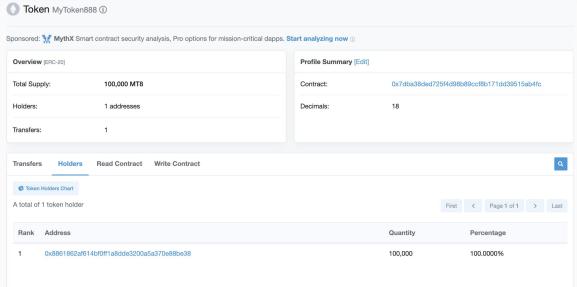
#### \_balance

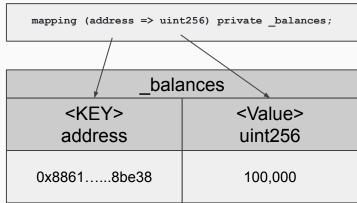
- 각 주소별로 토큰 잔액정보를 저장하기 위한 테이블
- o Private 옵션을 통해 외부에서 상태변수를 직접 볼 수 없도록 함

```
string public name;
string public symbol;
uint8 public decimals;

mapping (address => uint256) private _balances;
mapping (address => mapping (address => uint256)) private _allowed;

uint256 private _totalSupply;
```





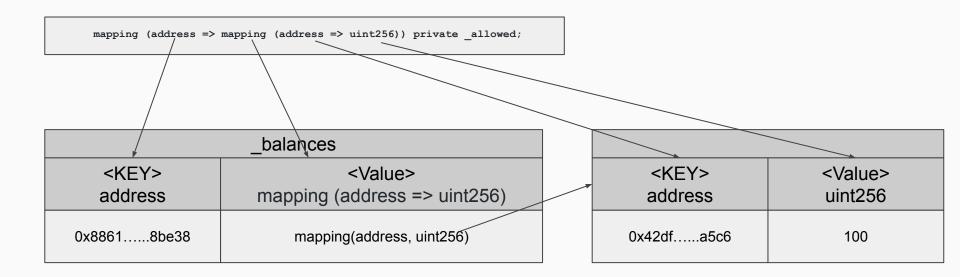
#### \_allowed

- 각 주소별로 제 3자에게 토큰사용을 허락한 정보
- o mapping 안의 Value가 또다른 mapping 테이블
- o Private 옵션을 통해 외부에서 상태변수를 직접 볼 수 없도록 함

```
string public name;
string public symbol;
uint8 public decimals;

mapping (address => uint256) private _balances;
mapping (address => mapping (address => uint256)) private _allowed;

uint256 private _totalSupply;
```



#### **Event**

#### Event

- 트랜잭션 수행결과에 따라, 남기기 위한 로그 데이터
- o emit 이라는 명령어를 통해 트랜잭션 이력에 이벤트를 발생
- 노드에서는 트랜잭션에서 이벤트 발생시, 이를 감지하여, 다른 프로세스 진행이 가능
   ex) 입,출금 이벤트에 따른 거래소 지갑 DB 업데이트

```
event Transfer(address indexed _from, address indexed _to, uint256 _value);
event Approval(address indexed _owner, address indexed _spender, uint256 _value);
```

#### **Event**

#### • 생성자

- 컨트랙트 배포에 따른 기본 값 설정
- o \_mint 함수 호출을 통한 토큰 수량 생성

```
constructor() public{
    name = "MyToken888";
    symbol="MT8";
    decimals = 18;
    _mint(msg.sender,100000 * (10**18));
}
```

#### **Constant Function**

#### Constant Function

- 토큰의 상태값 조회를 위한 Read-Only Function
- Private 상태변수의 값 조회를 위한 getter

```
function totalSupply() public view returns (uint256) {
   return _totalSupply;
}

function balanceOf(address owner) public view returns (uint256) {
   return _balances[owner];
}

function allowance( address owner, address spender ) public view returns (uint256)

{
   return _allowed[owner][spender];
}
```

#### **Constant Function**

#### Constant Function

- 토큰의 상태값 조회를 위한 Read-Only Function
- Private 상태변수의 값 조회를 위한 getter

```
function totalSupply() public view returns (uint256) {
   return _totalSupply;
}

function balanceOf(address owner) public view returns (uint256) {
   return _balances[owner];
}

function allowance( address owner, address spender ) public view returns (uint256)

{
   return _allowed[owner][spender];
}
```

- 토큰전송 기능
- \_transfer에서 실제 작업을 처리

```
function transfer(address to, uint256 value) public returns (bool) {
   _transfer(msg.sender, to, value);
   return true;
}
```

#### \_transfer

- internal Function으로 외부에서 직접호출 불가
- transfer / transferFrom을 통해서만 전송 가능
- 토큰 전송 작업 전에 유효성 검사 실시
- 작업 종료 후에 이벤트 발생

```
function _transfer(address from, address to, uint256 value) internal {
    require(value <= _balances[from]);
    require(to != address(0));

    _balances[from] = _balances[from].sub(value);
    _balances[to] = _balances[to].add(value);
    emit Transfer(from, to, value);
}</pre>
```

#### \_transfer

- o internal Function으로 외부에서 직접호출 불가
- transfer / transferFrom을 통해서만 전송 가능
- 토큰 전송 작업 전에 유효성 검사 실시
- 작업 종료 후에 이벤트 발생

```
function _transfer(address from, address to, uint256 value) internal {
    require(value <= _balances[from]);
    require(to != address(0));

    _balances[from] = _balances[from].sub(value);
    _balances[to] = _balances[to].add(value);
    emit Transfer(from, to, value);
}</pre>
```

```
from: 0x8861.....8be38
    : 0x42df.....a5c6
value: 100
function transfer(address from, address to, uint256 value) internal {
  require(value <= balances[from]);</pre>
  require(to != address(0));
   _balances[from] = _balances[from].sub(value);
   _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances		
<key> address</key>		
0x88618be38	100,000	

```
from: 0x8861.....8be38
    : 0x42df.....a5c6
value: 100
function transfer(address from, address to, uint256 value) internal {
  require(value <= _balances[from]);</pre>
  require(to != address(0));
  _balances[from] = _balances[from].sub(value);
  _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances		
<key> <value> address uint256</value></key>		
0x88618be38	100,000	

```
from : 0x8861.....8be38
    : 0x42df.....a5c6
value: 100
function transfer(address from, address to, uint256 value) internal {
  require(value <= _balances[from]);</pre>
  require(to != address(0));
  balances[from] = balances[from].sub(value);
   _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances	
<key> address</key>	<value> uint256</value>
0x88618be38	100,000

```
from : 0x8861.....8be38
    : 0x42df.....a5c6
value: 100
function transfer(address from, address to, uint256 value) internal {
  require(value <= _balances[from]);</pre>
  require(to != address(0));
  balances[from] = balances[from].sub(value);
   _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances	
<key> <value> address uint256</value></key>	
0x88618be38	99,900

```
from: 0x8861.....8be38
     : 0x42df.....a5c6
value: 100
function _transfer(address from, address to, uint256 value) internal {
  require(value <= _balances[from]);</pre>
  require(to != address(0));
  _balances[from] = _balances[from].sub(value);
  _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances		
<key> address</key>	<value> uint256</value>	
0x88618be38	99,900	
0	0	

```
from: 0x8861.....8be38
     : 0x42df.....a5c6
value: 100
function _transfer(address from, address to, uint256 value) internal {
  require(value <= _balances[from]);</pre>
  require(to != address(0));
   _balances[from] = _balances[from].sub(value);
  _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances		
<key> address</key>	<value> uint256</value>	
0x88618be38	99,900	
0x42dfa5c6	0	

```
from: 0x8861.....8be38
   : 0x42df.....a5c6
value: 100
function _transfer(address from, address to, uint256 value) internal {
  require(value <= _balances[from]);</pre>
  require(to != address(0));
  _balances[from] = _balances[from].sub(value);
  _balances[to] = _balances[to].add(value);
  emit Transfer(from, to, value);
```

_balances		
<key> address</key>	<value> uint256</value>	
0x88618be38	99,900	
0x42dfa5c6	100	

#### approve

- o spender를 지정하여, 자신의 토큰을 사용할 수 있게 허가
- o spender는 transferFrom을 통해 허가된 범위 안에서 토큰을 사용할 수 있음

```
function approve(address spender, uint256 value) public returns (bool) {
   require(spender != address(0));

   _allowed[msg.sender][spender] = value;
   emit Approval(msg.sender, spender, value);
   return true;
}
```

```
msg.sender : 0x8861.....8be38
spender
         : 0x42df....a5c6
value : 100
function approve(address spender, uint256 value) public returns (bool) {
  require(spender != address(0));
   allowed[msg.sender][spender] = value;
  emit Approval(msg.sender, spender, value);
  return true;
```

_allowed		
<key></key>	<value></value>	
address	mapping	

```
msg.sender : 0x8861.....8be38
spender
        : 0x42df....a5c6
value : 100
function approve(address spender, uint256 value) public returns (bool) {
  require(spender != address(0));
  allowed[msg.sender][spender] = value;
  emit Approval(msg.sender, spender, value);
  return true;
```

_allowed	
<key> address</key>	<value> mapping</value>
0	0

```
msg.sender : 0x8861.....8be38
spender
         : 0x42df.....a5c6
value : 100
function approve(address spender, uint256 value) public returns (bool) {
  require(spender != address(0));
  allowed[msg.sender][spender] = value;
  emit Approval(msg.sender, spender, value);
  return true;
```

_allowed		
<key> address</key>	<value> mapping</value>	
0x88618be38	0	

```
msg.sender : 0x8861.....8be38
spender
         : 0x42df.....a5c6
value : 100
function approve(address spender, uint256 value) public returns (bool) {
  require(spender != address(0));
  allowed[msg.sender][spender] = value;
  emit Approval(msg.sender, spender, value);
  return true;
```

_allo	owed	
<key> address</key>		lue> ping
	<key> address</key>	<value> uint256</value>
0x88618be38	0	0
		·

```
msg.sender : 0x8861.....8be38
         : 0x42df.....a5c6
spender
value : 100
function approve(address spender, uint256 value) public returns (bool) {
  require(spender != address(0));
   allowed[msg.sender][spender] = value;
  emit Approval(msg.sender, spender, value);
  return true;
```

_allowed		
<key> address</key>	<value> mapping</value>	
	<key> address</key>	<value> uint256</value>
	auuless	uiiit230
0x88618be38	0x42df.a5c6	100

```
msg.sender : 0x8861.....8be38
spender
        : 0x42df....a5c6
value : 100
function approve(address spender, uint256 value) public returns (bool) {
  require(spender != address(0));
   allowed[msg.sender][spender] = value;
  emit Approval(msg.sender, spender, value);
  return true;
```

_allowed		
<key> address</key>		lue> ping
	<key> address</key>	<value> uint256</value>
0x88618be38	0x42df.a5c6	100

```
msg.sender: 0x42df.....a5c6
         : 0x8861.....8be38
from
         : 0x33ff.....81ga
to
        : 10
value
function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
  require(value <= _allowed[from][msg.sender]);</pre>
  _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   transfer(from, to, value);
  return true;
```

_allowed		
<key> address</key>		lue> ping
	<key> address</key>	<value> uint256</value>
0x88618be38	0x42df.a5c6	100

```
msg.sender: 0x42df.....a5c6
           : 0x8861....8be38
from
         : 0x33ff.....81ga
to
value
         : 10
function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
  require(value <= allowed[from][msg.sender]);</pre>
  _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   transfer(from, to, value);
  return true;
```

_allowed		
<key> address</key>		lue> ping
	<key> address</key>	<value> uint256</value>
0x88618be38	0x42df.a5c6	100

```
msg.sender: 0x42df.....a5c6
           : 0x8861.....8be38
from
         : 0x33ff.....81ga
to
value
        : 10
function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
  require(value <= _allowed[from][msg.sender]);</pre>
  _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   transfer(from, to, value);
  return true;
```

_allowed		
<key> address</key>	<va map</va 	lue> ping
0x88618be38	<key> address</key>	<value> uint256</value>
	0x42df.a5c6	90

```
msg.sender : 0x42df.....a5c6
from : 0x8861.....8be38
to : 0x33ff.....81ga
value : 10

function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
   require(value <= _allowed[from][msg.sender]);
   _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   _transfer(from, to, value);
   return true;
}</pre>
```

_allowed		
<key></key>	<va< th=""><th>lue&gt;</th></va<>	lue>
address	map	ping
0x88618be38	<key></key>	<value></value>
	address	uint256
	0x42df.a5c6	90

_balances	
<key> address</key>	<value> uint256</value>
0x88618be38	99,900
0x42dfa5c6	100

```
msg.sender : 0x42df.....a5c6
from : 0x8861.....8be38
to : 0x33ff.....81ga
value : 10

function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
   require(value <= _allowed[from][msg.sender]);
   _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   _transfer(from, to, value);
   return true;
}</pre>
```

_allowed		
<key></key>	<va< th=""><th>lue&gt;</th></va<>	lue>
address	map	ping
0x88618be38	<key> address</key>	<value> uint256</value>
	0x42df.a5c6	90

_balances	
<key> address</key>	<value> uint256</value>
0x88618be38	99,900
0x42dfa5c6	100

```
msg.sender : 0x42df.....a5c6
from : 0x8861.....8be38
to : 0x33ff.....81ga
value : 10

function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
  require(value <= _allowed[from][msg.sender]);
  _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
  _transfer(from, to, value);
  return true;
}</pre>
```

_allowed		
<key></key>	<va< th=""><th>lue&gt;</th></va<>	lue>
address	map	ping
0x88618be38	<key> address</key>	<value> uint256</value>
	0x42df.a5c6	90

_balances	
<key> address</key>	<value> uint256</value>
0x88618be38	99,890
0x42dfa5c6	100

```
msg.sender : 0x42df.....a5c6
from : 0x8861.....8be38
to : 0x33ff.....81ga
value : 10

function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
  require(value <= _allowed[from][msg.sender]);
  _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
  _transfer(from, to, value);
  return true;
}</pre>
```

_allowed		
<key></key>	<va< th=""><th>lue&gt;</th></va<>	lue>
address	map	ping
0x88618be38	<key> address</key>	<value> uint256</value>
	0x42df.a5c6	90

_balances		
<key> address</key>	<value> uint256</value>	
0x88618be38	99,890	
0x42dfa5c6	100	
0	0	

```
msg.sender : 0x42df.....a5c6
from : 0x8861.....8be38
to : 0x33ff.....81ga
value : 10

function transferFrom( address from, address to, uint256 value ) public returns (bool) {
   require(value <= _allowed[from][msg.sender]);
   _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   _transfer(from, to, value);
   return true;
}</pre>
```

_allowed			
<key></key>	<value></value>		
address	mapping		
0x88618be38	<key> address</key>	<value> uint256</value>	
	0x42df.a5c6	90	

_balances		
<key> address</key>	<value> uint256</value>	
0x88618be38	99,890	
0x42dfa5c6	100	
0x33ff81ga	10	

```
msg.sender : 0x42df.....a5c6
from : 0x8861.....8be38
to : 0x33ff.....81ga
value : 10

function transferFrom( address from, address to, uint256 value ) public
returns (bool) {
   require(value <= _allowed[from][msg.sender]);
   _allowed[from][msg.sender] = _allowed[from][msg.sender].sub(value);
   _transfer(from, to, value);
   return true;
}</pre>
```

_allowed			
<key></key>	<value></value>		
address	mapping		
0x88618be38	<key> address</key>	<value> uint256</value>	
	0x42df.a5c6	90	

_balances		
<key> address</key>	<value> uint256</value>	
0x88618be38	99,890	
0x42dfa5c6	100	
0x33ff81ga	10	