Smart Contract Bug 1

Security Bug

Contract

```
contract Example {

    address public owner;
    string private mySecret;

    constructor {
        owner = msg.sender;
    }

    function setSecret(string _secret) public {
        require(msg.sender == owner);
        mySecret = _secret;
    }

    function getSecret() public returns (string) {
        require(msg.sender == owner);
        return mySecret;
    }
}
```

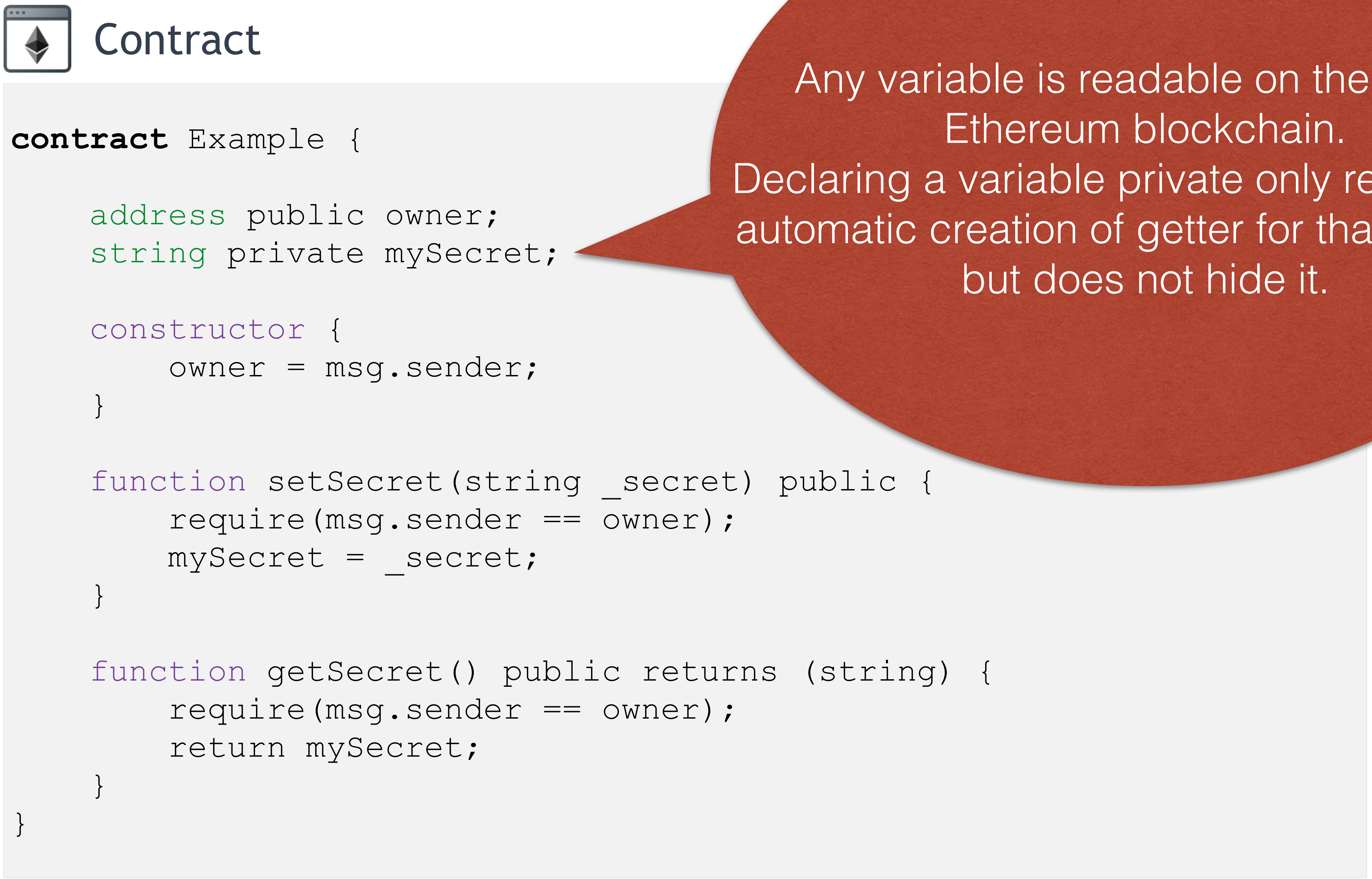
Security Bug

Contract

```
contract Example {

    address public owner;
    string private mySecret;

    constructor {
        owner = msg.sender;
    }

    function setSecret(string _secret) public {
        require(msg.sender == owner);
        mySecret = _secret;
    }

    function getSecret() public returns (string) {
        require(msg.sender == owner);
        return mySecret;
    }
}
```

Hint: who would be able to read *mySecret* ?

Security Bug



Contract

```
contract Example {

    address public owner;
    string private mySecret;

    constructor {
        owner = msg.sender;
    }

    function setSecret(string _secret) public {
        require(msg.sender == owner);
        mySecret = _secret;
    }

    function getSecret() public returns (string) {
        require(msg.sender == owner);
        return mySecret;
    }
}
```

Any variable is readable on the public Ethereum blockchain.
Declaring a variable private only restricts the automatic creation of getter for that variable, but does not hide it.

Hint: who would be able to read *mySecret* ?