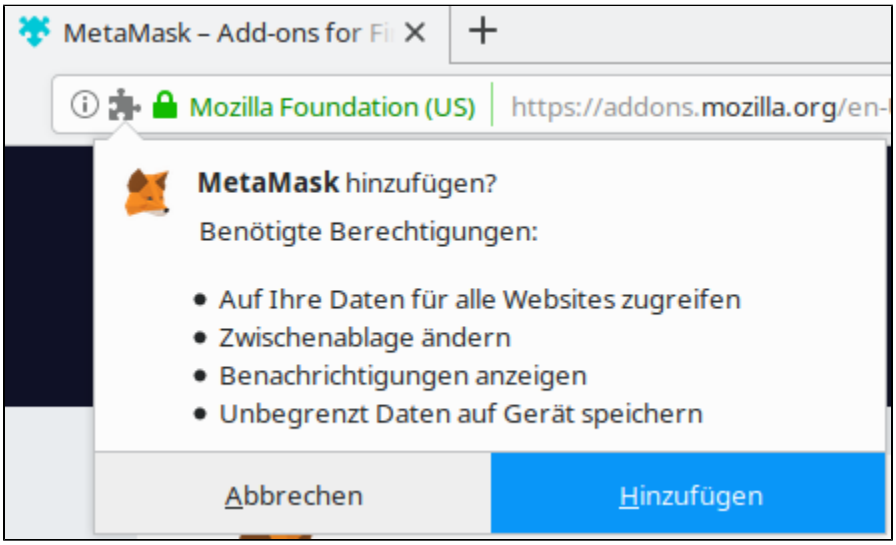
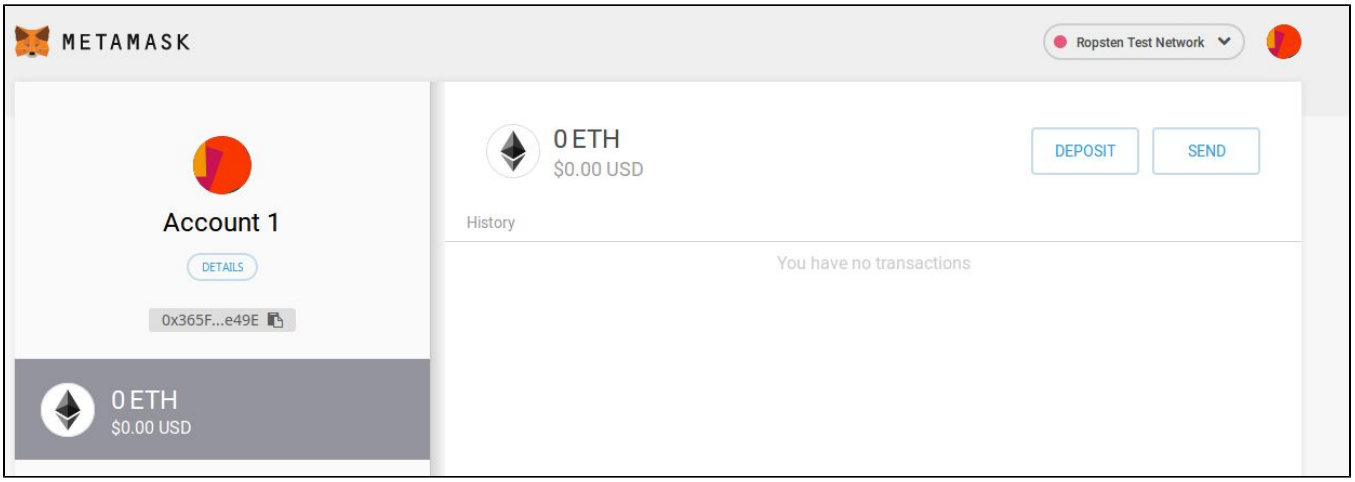
Praxissession 2a - Ethereum Grundlagen

MetaMask

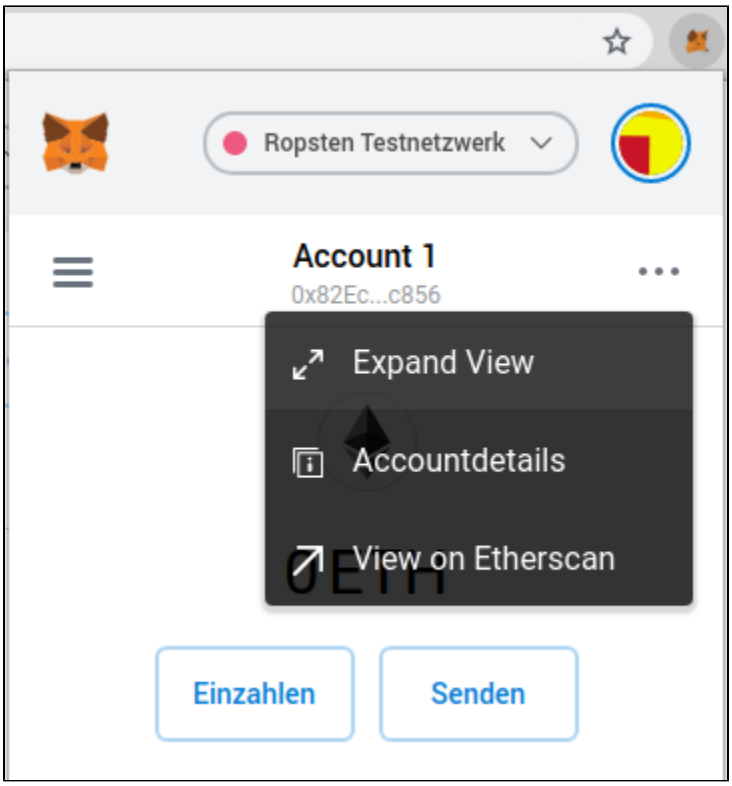
- Öffnen Sie den Firefox Browser und rufen Sie die Seite https://metamask.io auf und klicken Sie auf "GET FIREFOX ADDON".
- Klicken Sie auf "Add to Firefox".
- Bestätigen Sie die Berechtigungen, die von MetaMask benötigt werden, indem Sie auf "Hinzufügen" klicken.



- Es erscheint ein Begrüßungsbildschirm. Klicken Sie auf **Get Started**.
- Wählen Sie "**Create a Wallet**" aus.
- Entscheiden Sie, ob Sie bei der Verbesserung von MetaMask Daten übermitteln möchten **(No Thanks).**
- Vergeben Sie ein **Passwort** (und merken Sie sich dieses!).
- Kopieren Sie die **Secret Backup Phrase** in einen Editor (z. B. jEdit) und speichern Sie diese **(Weiter).**
- Geben Sie die Backup Phrase zur Bestätigung ein.
- Zum Verbinden von MetaMask mit Ropsten klicken Sie nun in MetaMask oben rechts auf "Ethereum Main Network" und wählen Sie aus dem DropDown-Menü "**Ropsten Test Network**".
- Nun sollte oben rechts "Ropsten Test Network" stehen.



- Meta Mask wird geöffnet, indem Sie auf den Fuchs oben rechts im Browser klicken.
- Für die große Ansicht der Wallet klicken Sie im MetaMask PopUp auf die drei Punkte und dann auf "**Expand View"**



Adresse teilen

- Teilen Sie dem Dozenten Ihre Adresse über die **Collabedit-Webseite** mit, die Ihnen genannt wird.

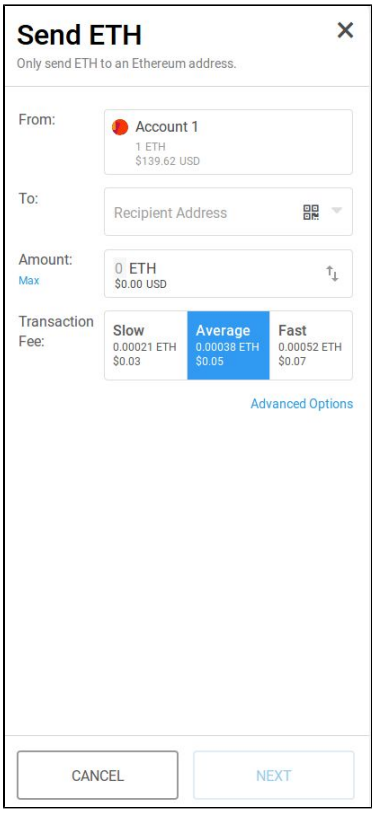
Organisieren Sie sich Ropsten Test Ether

- Um an Test Ether zu gelangen können Sie die folgenden beiden Faucets versuchen.
- https://faucet.ropsten.be/
    - Wenn Sie in MetaMask angemeldet sind, können Sie einfach auf "**Send me test Ether**" klicken.
- https://faucet.metamask.io/
    - Wenn Sie in MetaMask angemeldet sind, müssen Sie nur 1 Mal auf den Button "request 1 ether from faucet" klicken.
- **Sollten beide Faucets nicht funktionieren wird der Dozent ihnen Test Ether überweisen.**

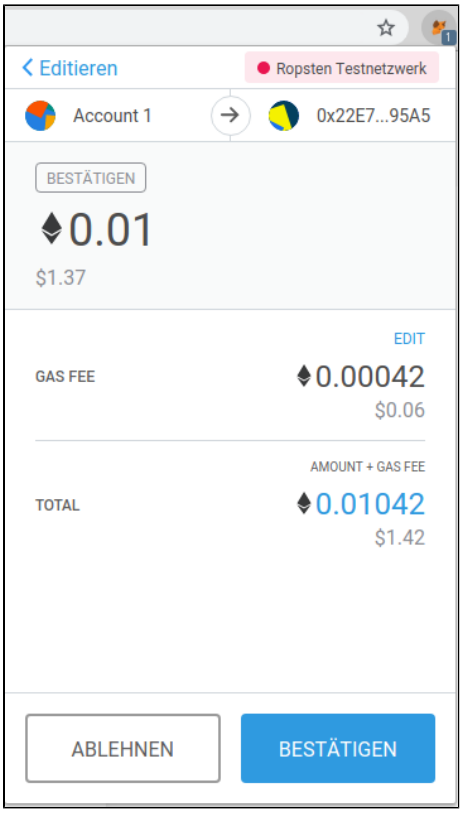
Ether senden

- Der Dozent wird Ihnen nun eine Adresse nennen, an die Sie einen Bruchteil ihrer Test-Ether zurück überweisen sollen.
- Sie können natürlich auch einem Ihrer Kommilitonen ein paar Test-Ether zukommen lassen.
- Klicken Sie dazu in MetaMask auf **"Send"** und fügen Sie den Empfängeradresse ein.

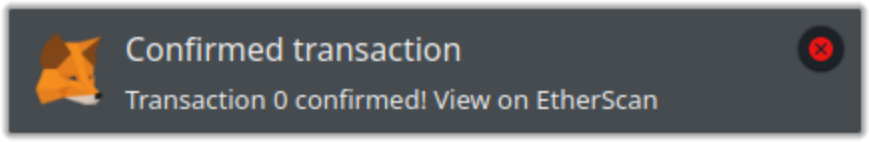
- Geben Sie einen kleinen Betrag ein (z.B. 0,001) und klicken Sie auf "Weiter".



- Bestätigen Sie die Transaktion, indem Sie im folgenden Fenster auf "Bestätigen" klicken.



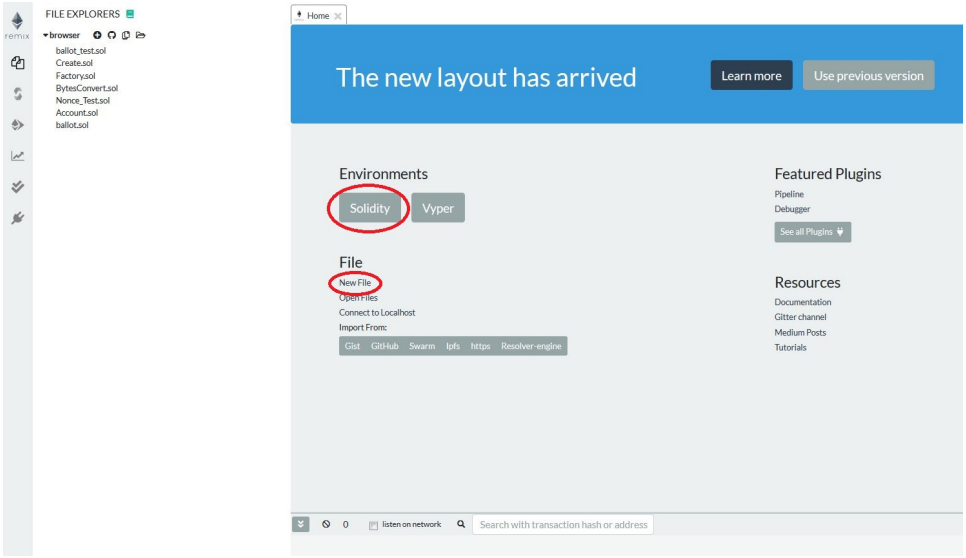
- Sobald die Transaktion gemined wurde, sollte oben rechts ein Pop Up erscheinen.



Im Folgenden sollen Sie einige Smart Contracts programmieren und benutzen. Dazu verwenden wir die Remix IDE. Damit können Sie Smart Contracts für die Ethereum Blockkette in der Programmiersprache "Solidity" erstellen und deployen. Die Remix IDE finden Sie unter http://remix.ethereum.org.

Remix IDE

- Öffnen Sie die Seite http://remix.ethereum.org im Firefox Browser.
- Wählen Sie als Sprache **Solidity** aus und klicken Sie auf **"New File**". Siehe Screenshot.
- Geben Sie anschließend einen Dateinamen ein. z.B. HelloWorld.

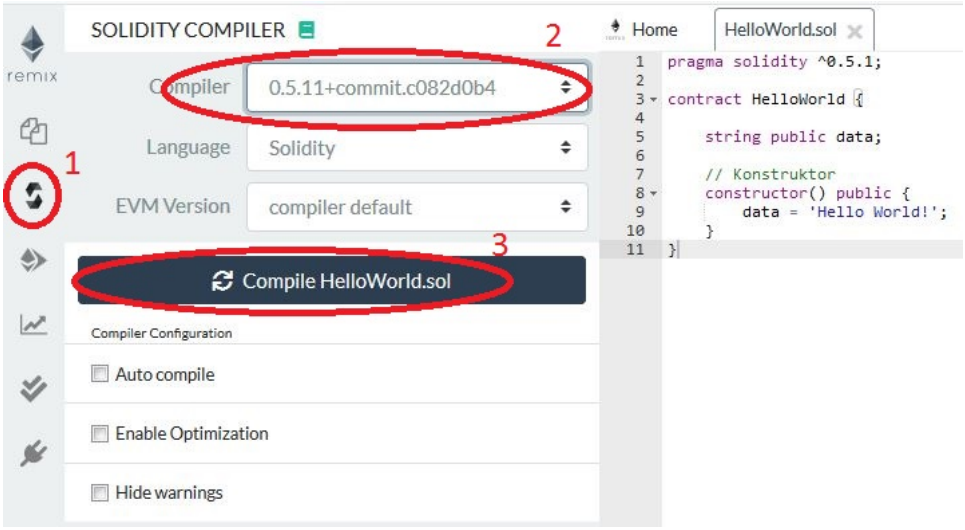


- Die schmale linke Spalte der IDE beinhaltet Zugriff auf den Compiler, den Dateiexplorer und das Deployment.
- Die mittlere Spalte zeigt die jeweiligen Elemente des Compilers, Dateiexplorers und für das Deployment.
- Die rechte Spalte enthält das Editorfenster. Der untere Bereich dient als eine Art "Logausgabe" für durchgeführte Transaktionen.
- Fügen Sie nun den folgenden **Quellcode in das Editorfenster** ein.

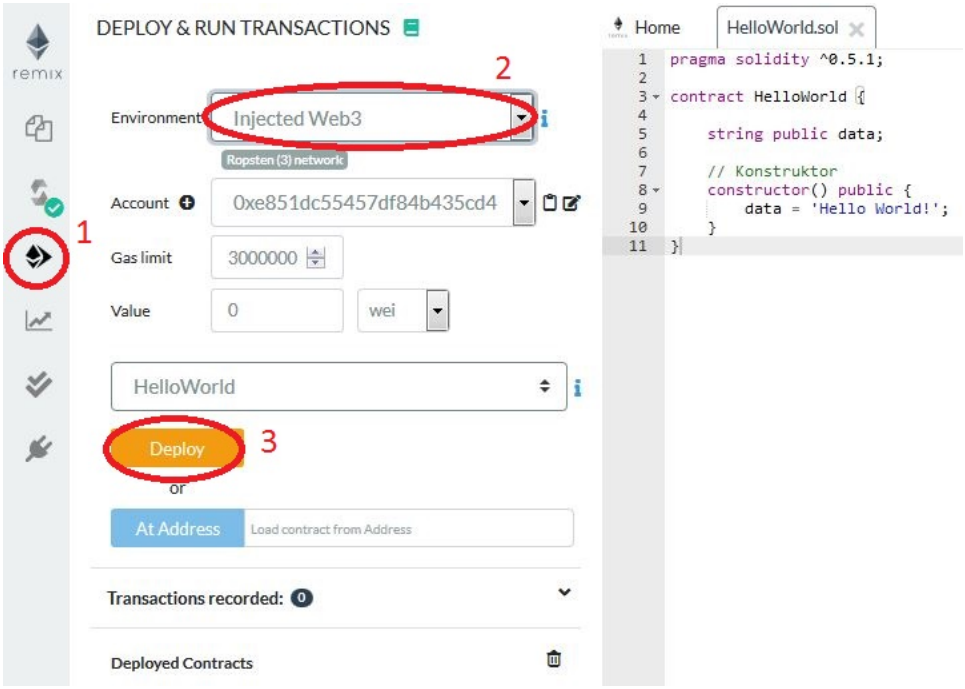
```
pragma solidity ^0.5.11;

contract HelloWorld {

    string public data;

    // Konstruktor
    constructor() public {
        data = 'Hello World!';
    }
}
```

- Wählen Sie in der linken Spalte **Solidity Compiler**. (Siehe Screenshot)
- Wählen Sie den **richtigen Compiler aus: 0.5.11+commit.c082d0b4**

- Zum Kompilieren des Contracts klicken Sie in der mittleren Spalte der Remix IDE auf **"Compile HelloWorld.sol"**.

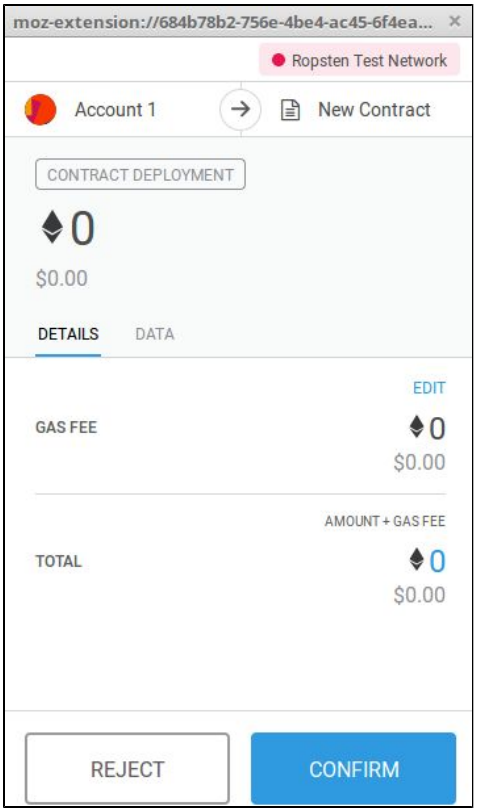


- Wenn beim Kompilieren keine Fehler aufgetreten sind, können wir den Contract deployen - also direkt in die Blockkette schreiben.
- Dazu müssen Sie zunächst in der linken Spalte in den Reiter **Deploy & Run transactions** wechseln. (Siehe Nr.1 auf Screenshot)
- Dort können Sie unter **"Environment"** verschiedenen Deploymentmethoden wählen. Wenn Sie das MetaMask Addon erfolgreich installiert haben, sollte unter Environment **"Injected Web3**" zu lesen sein und wenn Sie in Meta Mask noch angemeldet sind, sollte unter "Account" ihr MetaMask Account zu sehen sein. Wenn das nicht der Fall ist, melden Sie sich wieder am MetaMask Addon an. (Siehe Nr. 2 auf Screenshot)
- Klicken Sie dann auf den orangen **Button Deploy**. (Darüber können Sie den entsprechenden Contract auswählen.) (Siehe Nr. 3 auf Screenshot)

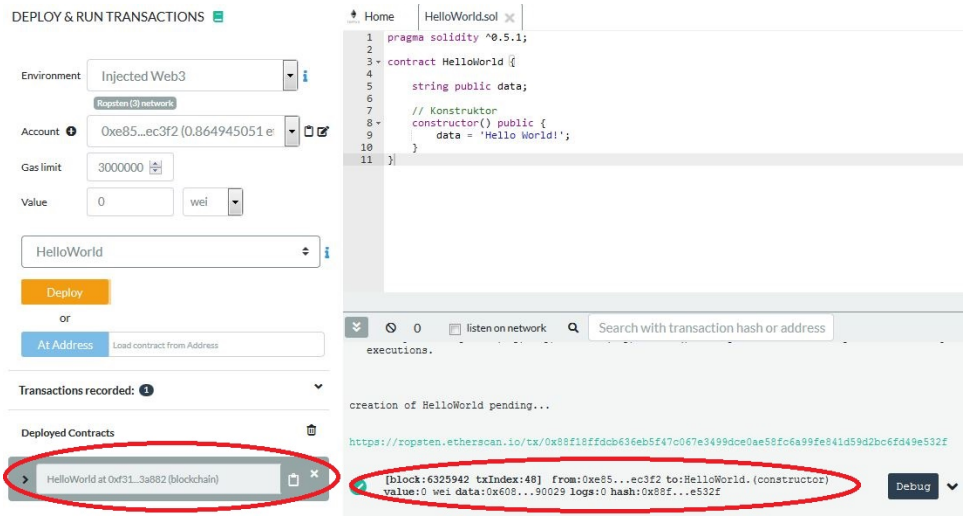


- Es erscheint nun ein MetaMask Popup zum Bestätigen der Transaktion. Bestätigen Sie die Transaktion indem Sie auf "**CONFIRM**" klicken

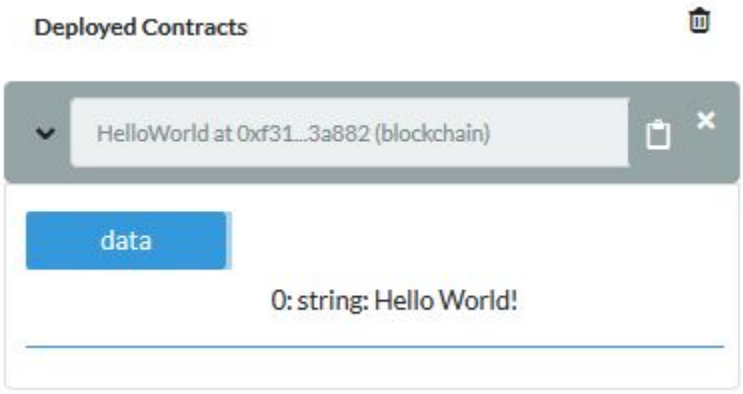
> Es kann in seltenen Fällen sein, dass Sie im Transaktionspopup noch die Transaktionsgebühr einstellen müssen. Dies ist der Fall, wenn bei GAS FEE der Wert 0 steht.
>
> - Klicken Sie dazu auf "**EDIT**" im Feld GAS FEE
> - Stellen Sie dort bei Estimated Processing Time "**Fast**" ein.
> - Klicken Sie auf "**Save**" und anschließend auf "**CONFIRM**".



- Sobald der Vertrag gemined wurde, erscheint unten im Konsolenfenster die Information über den Block. Außerdem erscheint in der mittleren Spalte der IDE ein kleines Interface, um mit dem Vertrag zu interagieren.
- **Dies kann eine Weile dauern, je nach Auslastung des Netzwerkes.**



- Lassen Sie sich den Wert "data" des Smart Contracts anzeigen, indem Sie unter "Deployed Contracts" den **"HelloWorld" Contract ausklappen** und anschließend auf **"data" klicken**.



Smart Contracts

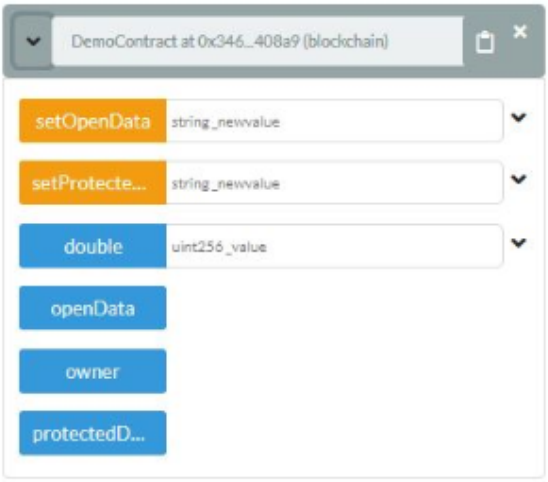
- Erstellen Sie in der Remix IDE einen neuen Smart Contract, nennen Sie ihn "DemoContract.sol" und fügen Sie den folgenden Quellcode ein.

```
pragma solidity ^0.5.11;
contract DemoContract {

    address public owner;
    string public protectedData;
    string public openData;

    modifier onlyOwner()
    {
        require(msg.sender == owner);
        _;
    }

    constructor () public
    {
        owner = msg.sender;
    }

    function setOpenData(string memory _newvalue) public
    {
        openData = _newvalue;
    }

    function setProtectedData(string memory _newvalue) onlyOwner public
    {
        protectedData = _newvalue;
    }

    function double (uint _value) public pure returns (uint)
    {
        return _value*2;
    }
}
```

- **Komplieren** Sie den Contract.
- Wenn das Kompilieren ohne Fehler funktioniert hat, können Sie den Smart Contract analog dem vorherigen Beispiel **deployen**.
- Sobald im Konsolenfenster zu sehen ist, dass der zweite Contract deployed wurde, wollen wir mit ihm interagieren.
- Dazu klappen wir den "DemoContract" in der mittleren Spalte der Remix IDE unter "Deployed Contracts" aus. Es sollten 6 Methoden zu sehen sein.

> - Beachten Sie, dass die blauen Methoden so genannte "constant" Funktionen bzw. "view" / "pure" sind. Diese verändern der Zustand der Blockkette nicht und können einfach so ausgeführt werden, ohne eine Transaktion erstellen zu müssen.
> - Die roten Methoden hingegen verändern den Zustand der Blockkette und müssen entsprechend über Transaktionen (die Gebühren kosten) ausgeführt werden. Aus diesem Grund müssen Sie auch in MetaMask das Ausführen dieser Methoden bestätigen.

- Testen Sie zunächst die vier **constant** (blau) Funktionen und verstehen Sie die Ausgabe.



- Testen Sie nun die State-verändernde Funktion "**setOpenData**". Beachten Sie, dass die jeweiligen Resultate erst zu sehen sind, wenn die Transaktion mit MetaMask bestätigt und anschließend gemined wurde.

- Um die Wirksamkeit der Methode "setProtectedData" testen zu können, benötigen Sie einen weiteren Account mit Test Ether.
- Da dies mit MetaMask und der Remix IDE etwas umständlich ist, verwenden wir für diesen Test eine Art "Test Blockkette" die virtuell im Speicher des Browser läuft, die so genannte "**JavascriptVM**".
- Wählen Sie die "JavascriptVM" aus und **deployen Sie den Contract erneut**. Da sie nun in einer "virtuellen Blockkette" arbeiten, müssen Sie keine Transaktionen mehr bestätigen und darauf warten, dass sie gemined werden.
- Rufen Sie nun die Methode "**setProtectedData**" einmal mit dem Account auf, der den Contract erstellt hat, und einmal mit einem anderen Account den Sie oben unter "Account" auswählen können.