Directions

1. The process of our scheme

Step 1: Alice deploys the smart contract and initiates the transaction

First, the seller Alice sets some parameters of the smart contract, for example the address of the big data. After that Alice deploys the smart contract on the blockchain by click the bottom "Deploy".

Also the address of the smart contract can be seen so that people who are interested in the transaction can check the amount of the total money in the smart contract.

Fig.1 shows where the bottom is and the specific address of the smart contract.

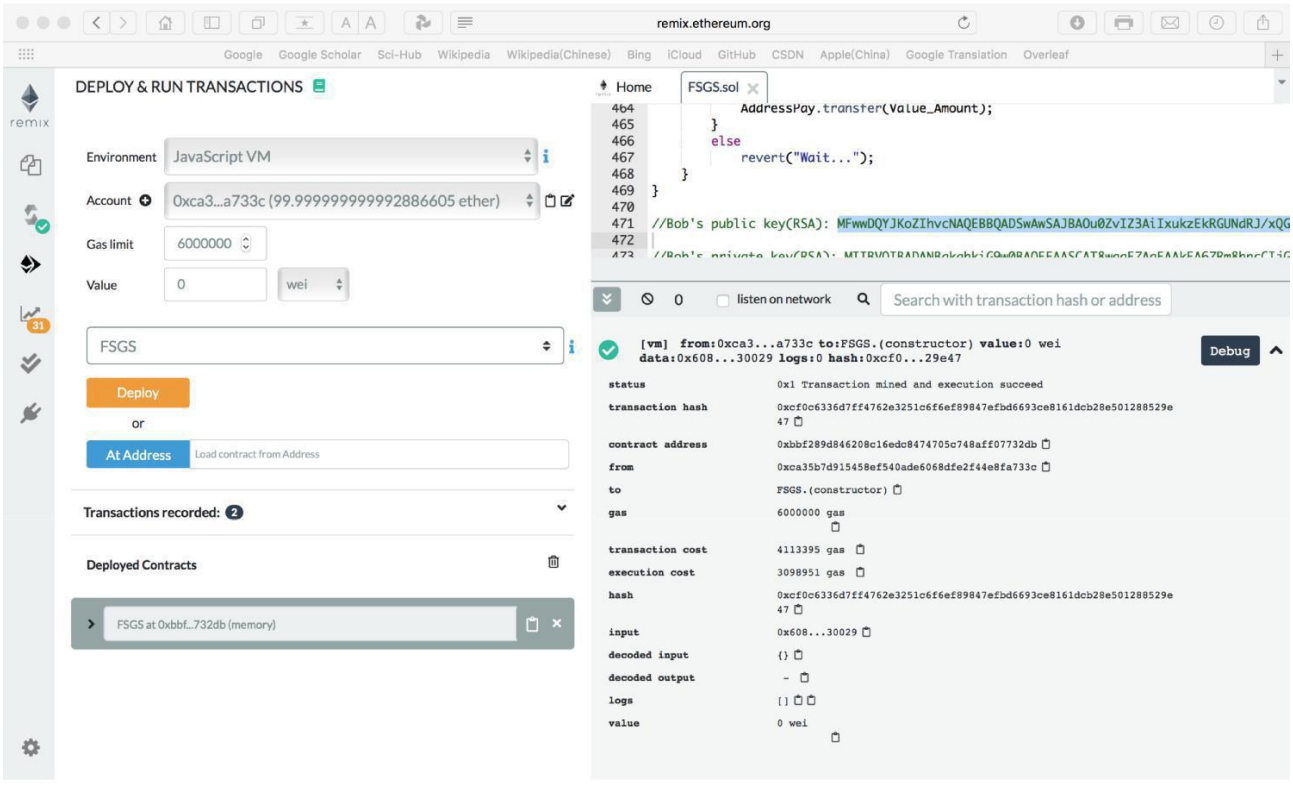

Fig.1. *The bottom and the address of smart contract*

Then, Alice sets the amount of money for the transaction, and the amount of deposit she should pay will generate automatically according to the codes (Here deposit = 2 * amount of money), shown as Fig.2.

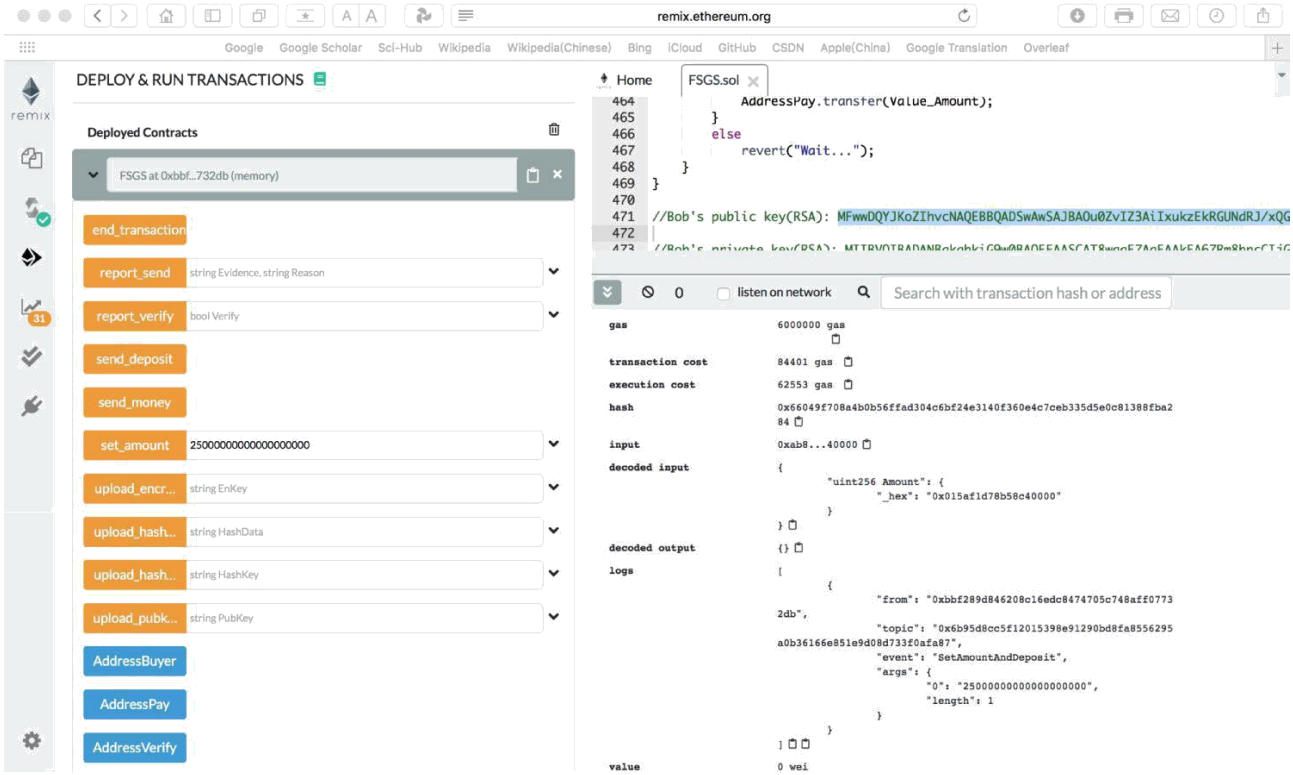

Fig.2. *Alice sets the amount of money and deposit for the transaction*

After setting the amount, Alice uploads the hash value of the data stored in the address she claims. And Alice uploads the key to the smart contract, where the key is used to encrypted the data, shown as Fig.3.

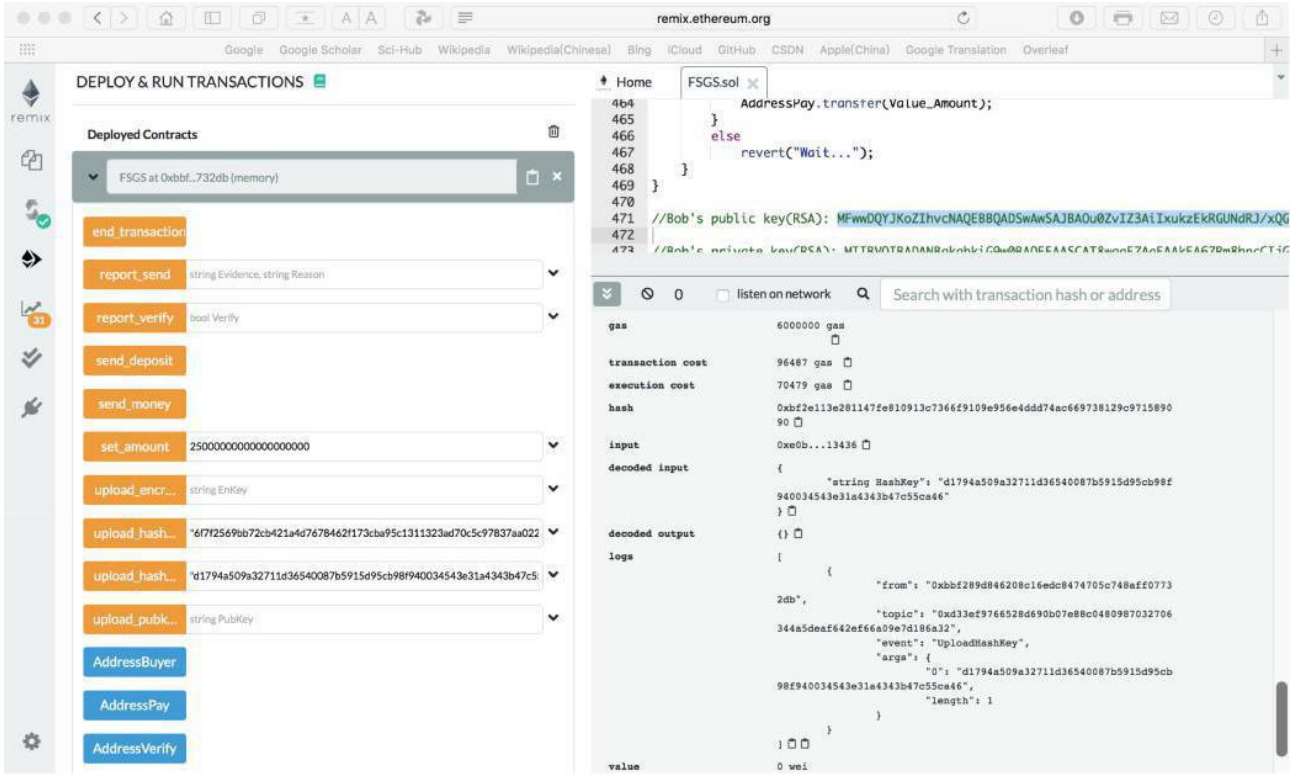

Fig.3. *Alice uploads the hash value of the data and the key to the smart contract*

The last operation of the step 1 is that Alice pays the deposit to the smart contract(All accounts have 100 ether at the beginning), and people can check the deposit using function "get_balance"(Input the address of the smart contract), shown as Fig.4 and Fig.5.

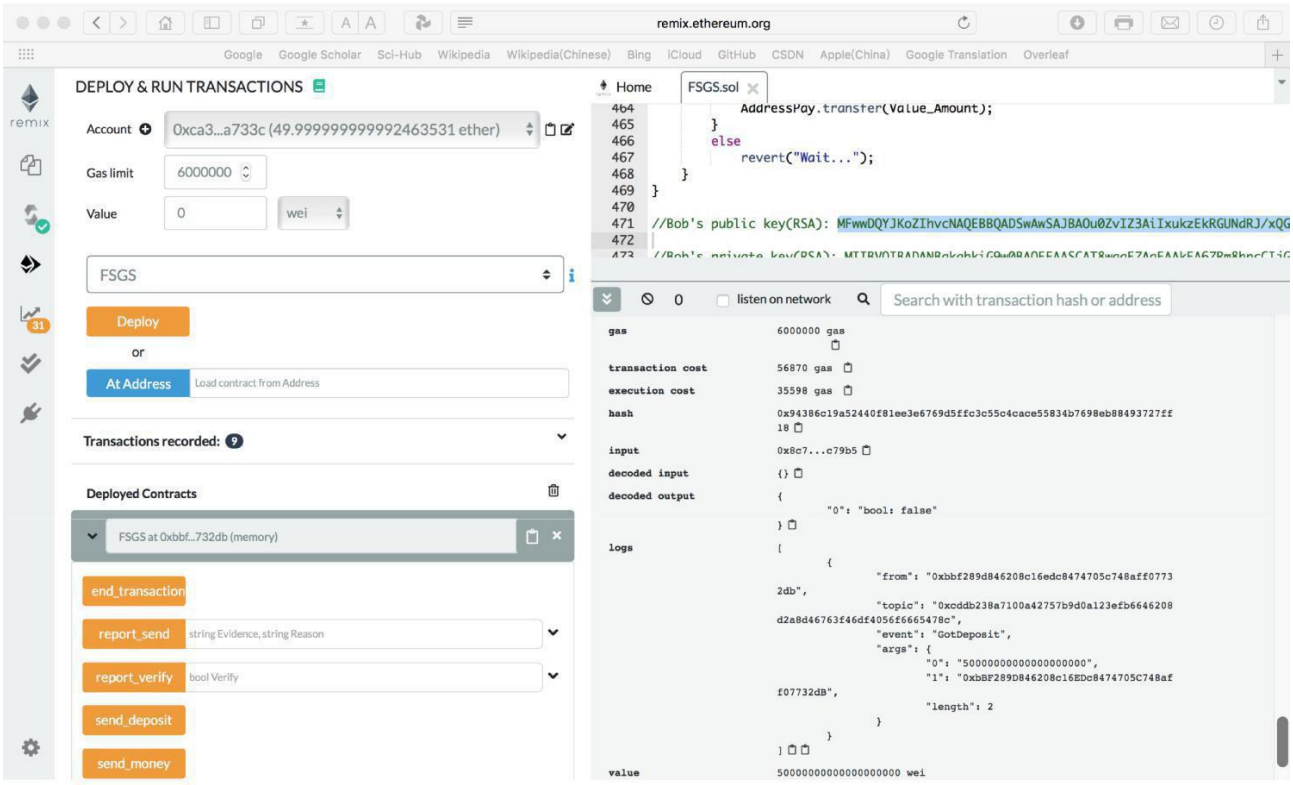

Fig.4. *Alice pays the deposit to the smart contract*

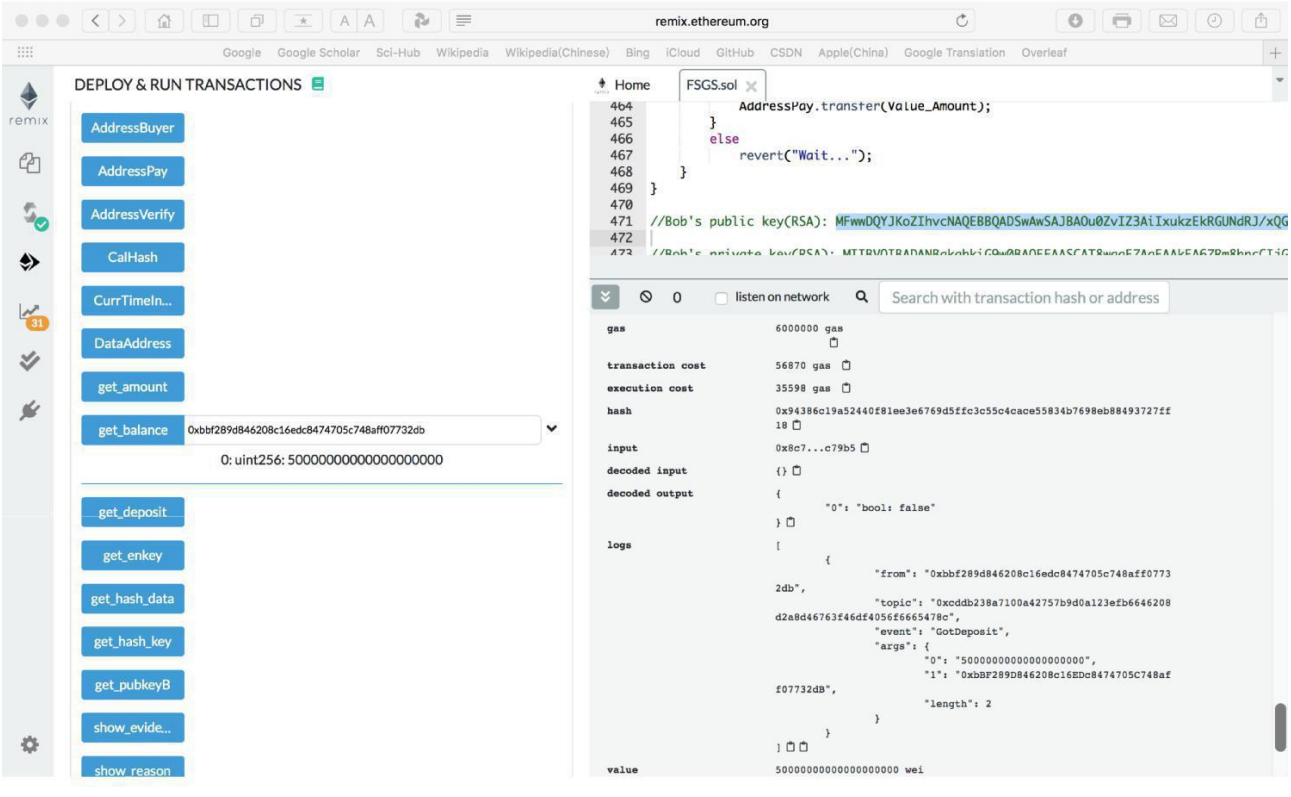

Fig.5. *Show the total amount of money in the smart contract*

Step 2: Bob pays for the data and uploads the public key

After Alice pays the deposit, buyers can check the hash value of the data and choose whether to buy it. Assume that one of buyers is Bob.

If Bob finds of the data downloads from the address whose hash value is the same as Alice claims and he wants to buy the data, then he pays as much as the amount Alice sets in the smart contract, and then uploads public key to the smart contract, shown as Fig.6 and Fig.7.

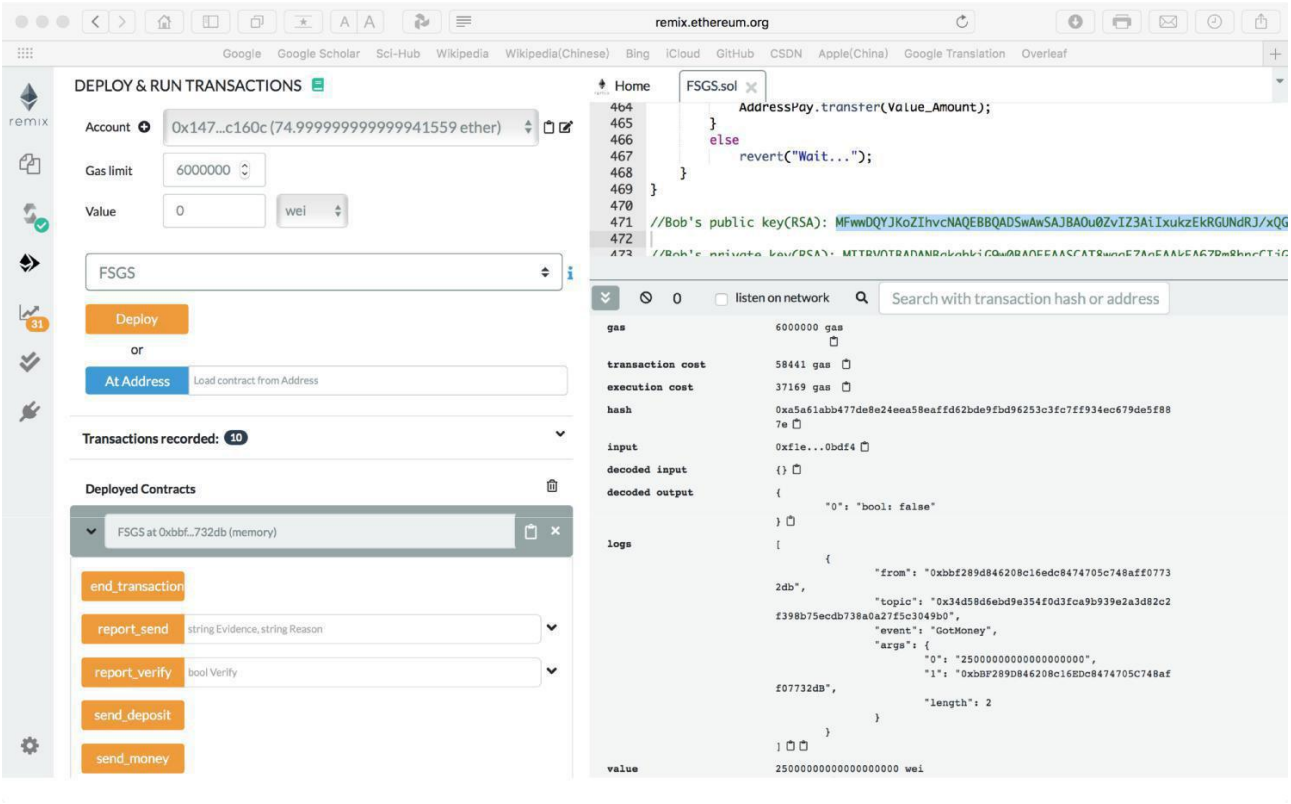

Fig.6. *Bob pays*

And after Bob pays, we can check the total money stored in the smart contract which is the amount of money sends by Bob adds the amount of the deposit sends by Alice, shown as Fig.8.

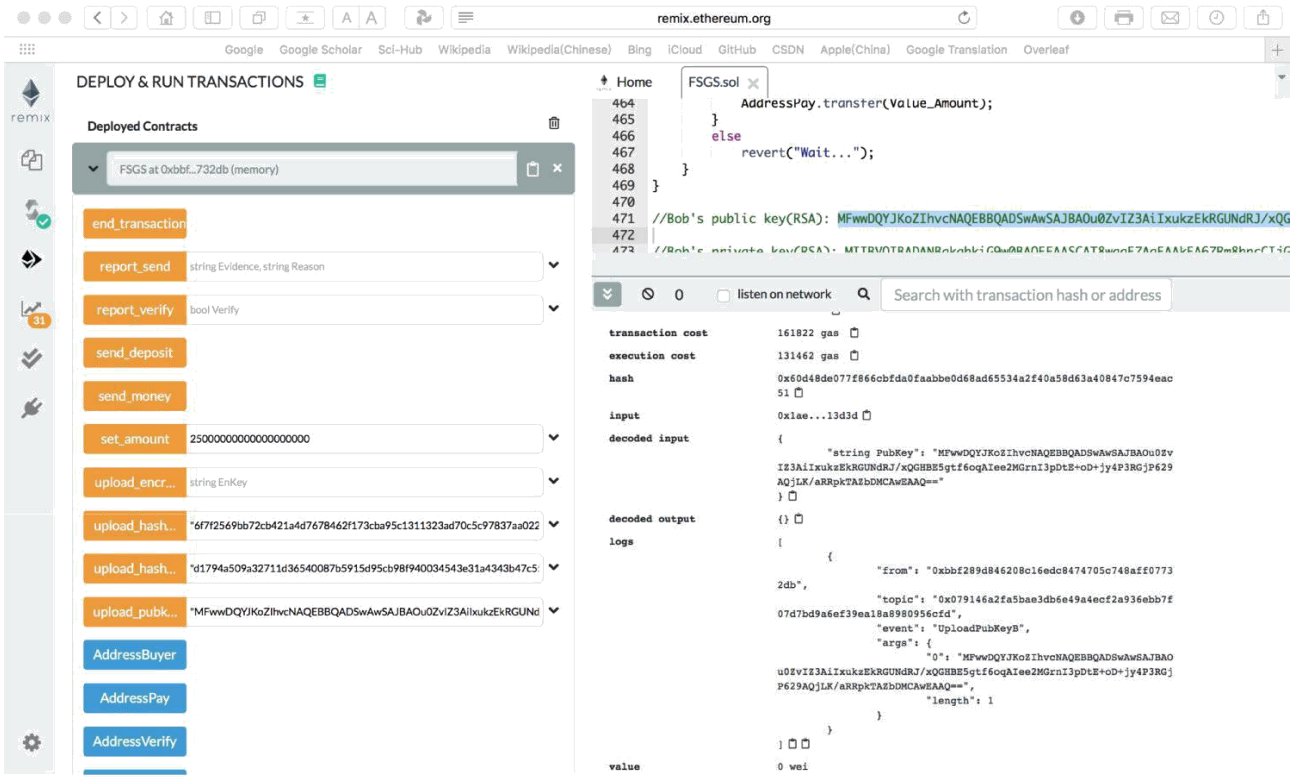

Fig.7. *Bob uploads the public key*

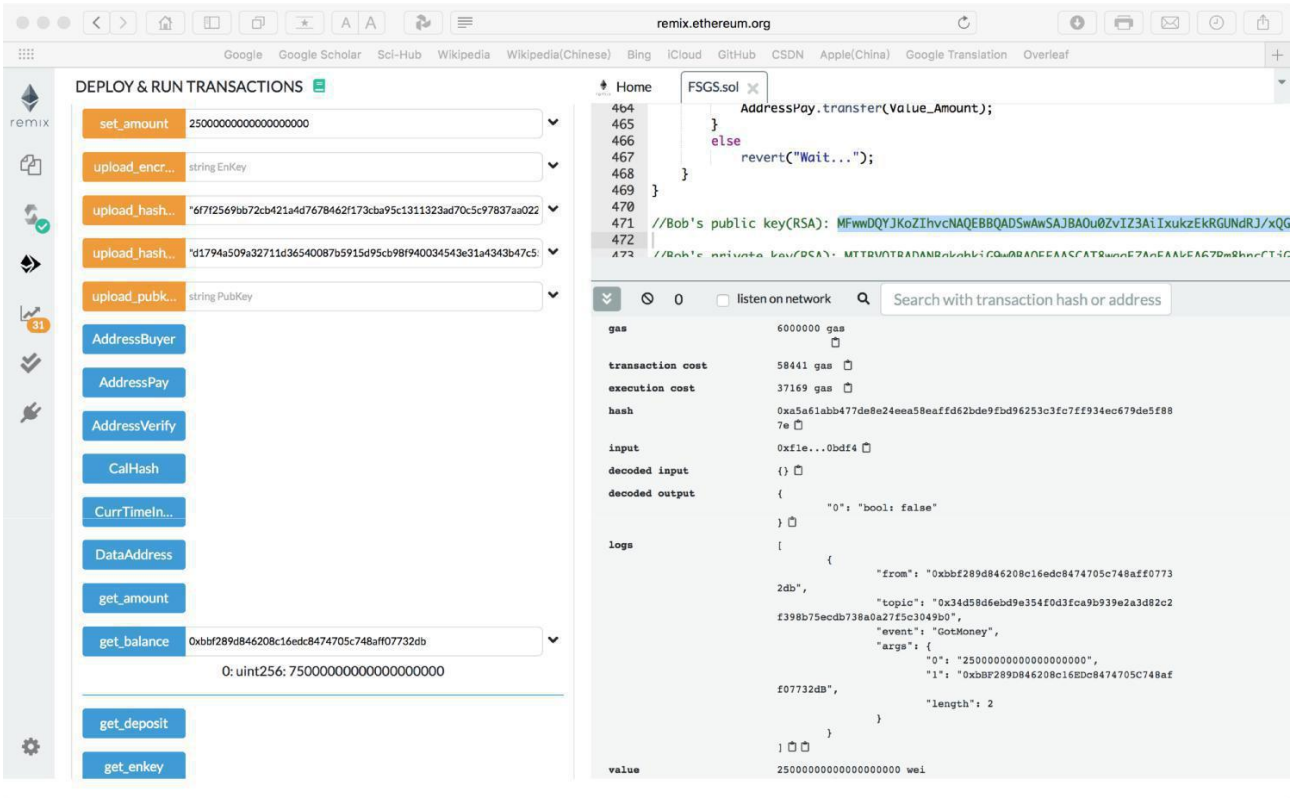

Fig.8. *Total amount of money in the smart contract*

Step 3: Alice uploads the encrypted key

When Alice finds the smart contract receives the money and Bob's public key, Alice encrypts the key using Bob's public key and uploads the generated encrypted key to the smart contract, shown as Fig.9.

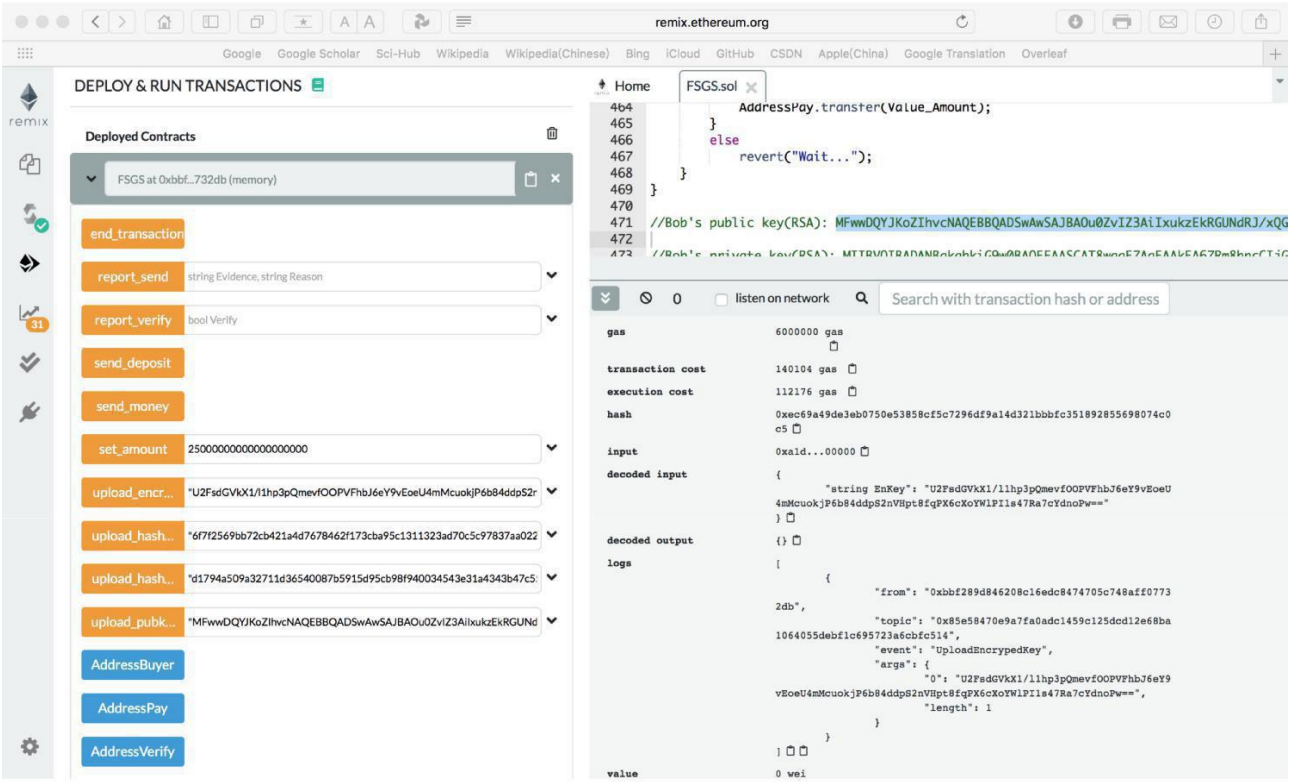

Fig.9. *Alice uploads the encrypted key to the smart contract*

Step 4: The result of the transaction

If Bob does not find any problem of the data, then he clicks the bottom "end_transaction", and Alice will receive the money and the deposit, the transaction is successful, shown as Fig.10.

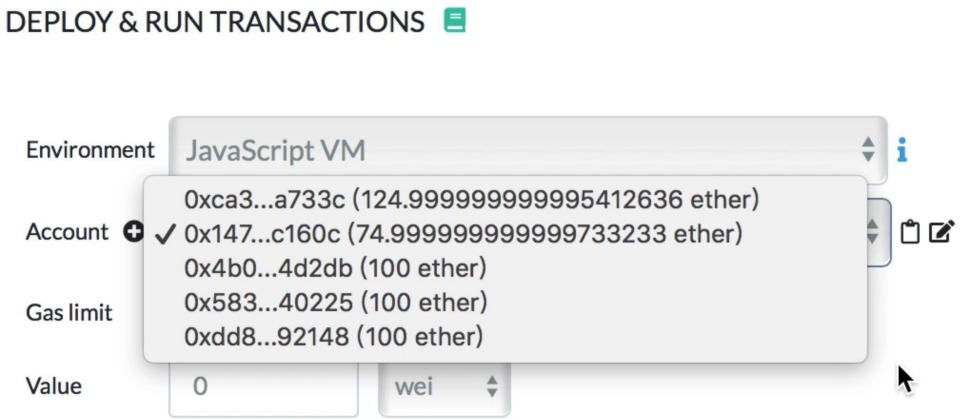

Fig.10. *Transaction is successful*

But if Bob find any problem about the data he receives, he can send a report to the smart contract. The report Bob sends should include the key he received as the evidence and the type of the problem, shown as Fig.11.

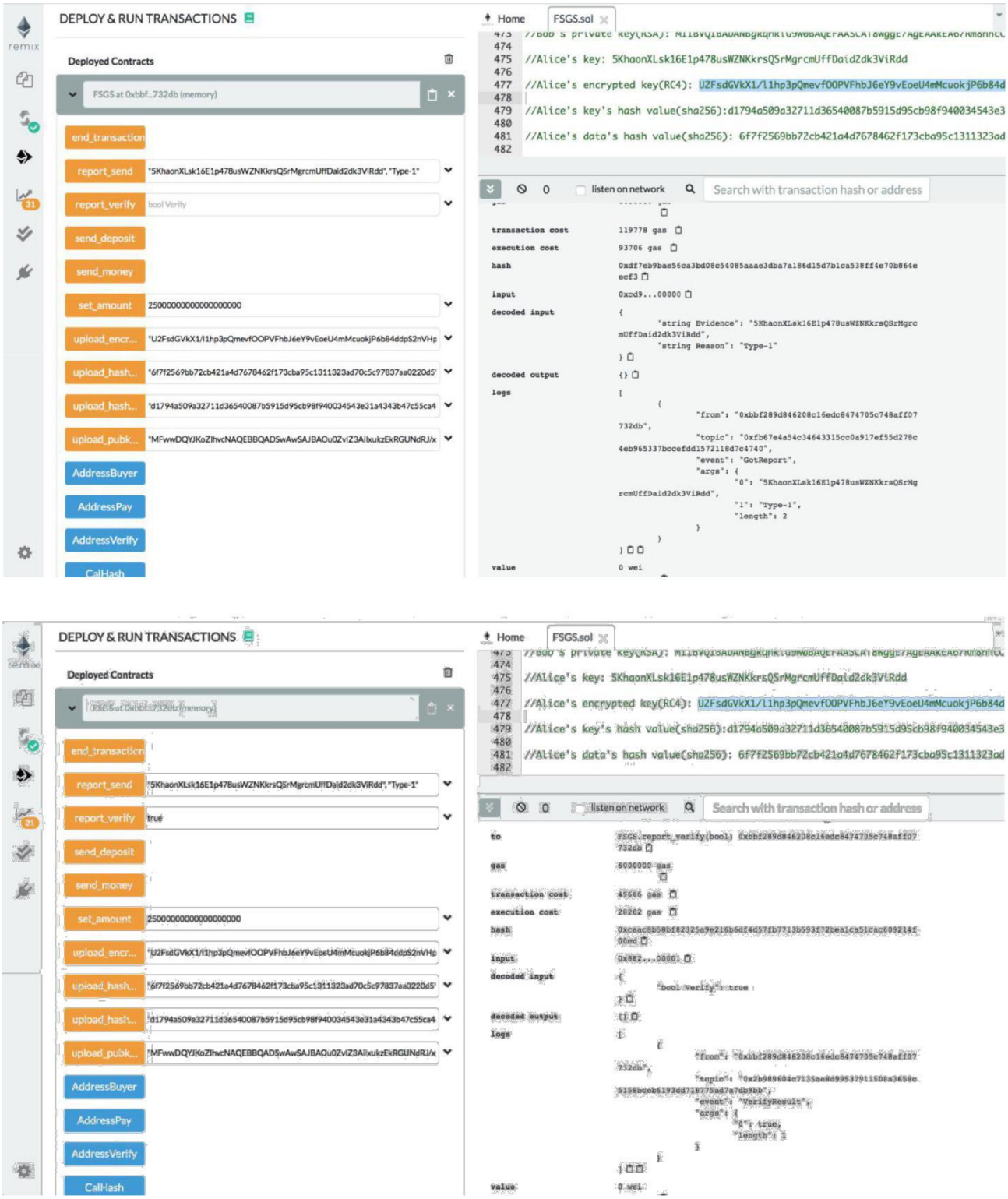

Fig.11. *Bob sends the report to the smart contract*

The third helps verifying whether the report is right, the third party will use the key to check the data Alice uploads and then sends the result of the report, finally the third party press the bottom “end_transaction” to end the transaction and send the money to the right one. If Bob’s report is wrong, Alice will receive all the money in the smart contract, which the result is the same as Fig.10. On the contrary, if Alice cheats Bob, Bob will receive all the money in the smart contract, shown as Fig.12.

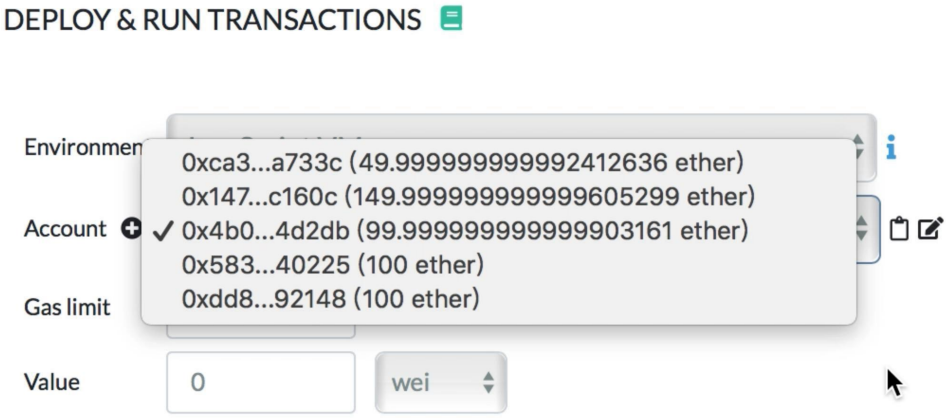

Fig.12. *The transaction result of Alice cheats Bob*

2. Show parameters both parties and the third party need to know

The Fig.13 shows the information of addresses, the web to calculate hash value and the web where the data is, the timestamp and the amount of money and deposit. As for the address, it includes addresses of the seller, buyer and the third party which helps to verify the report.

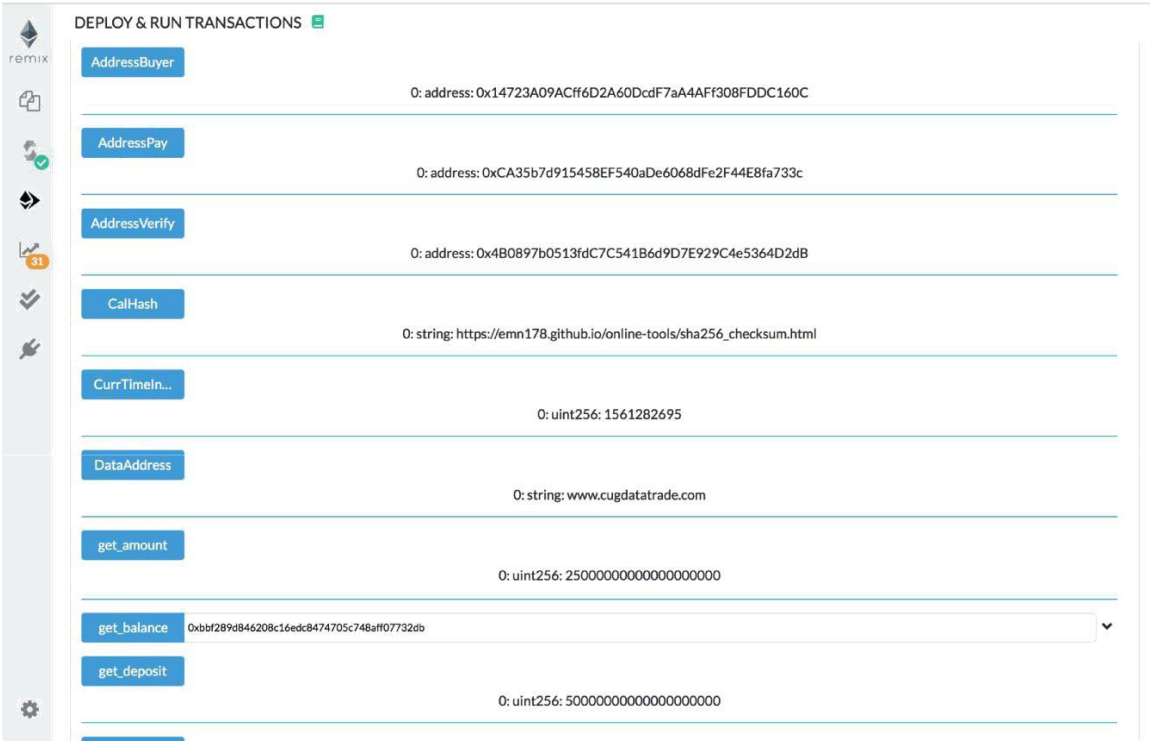

Fig.13. *Addressed, web, timestamp and amount of money and deposit*

The Fig.14 displays the information of keys, hash values and report. The “show_reason” tells users the types of different problems and their numbers.

The “show_evidence_reason” shows the key Alice sent to Bob and the type of the specific problem.

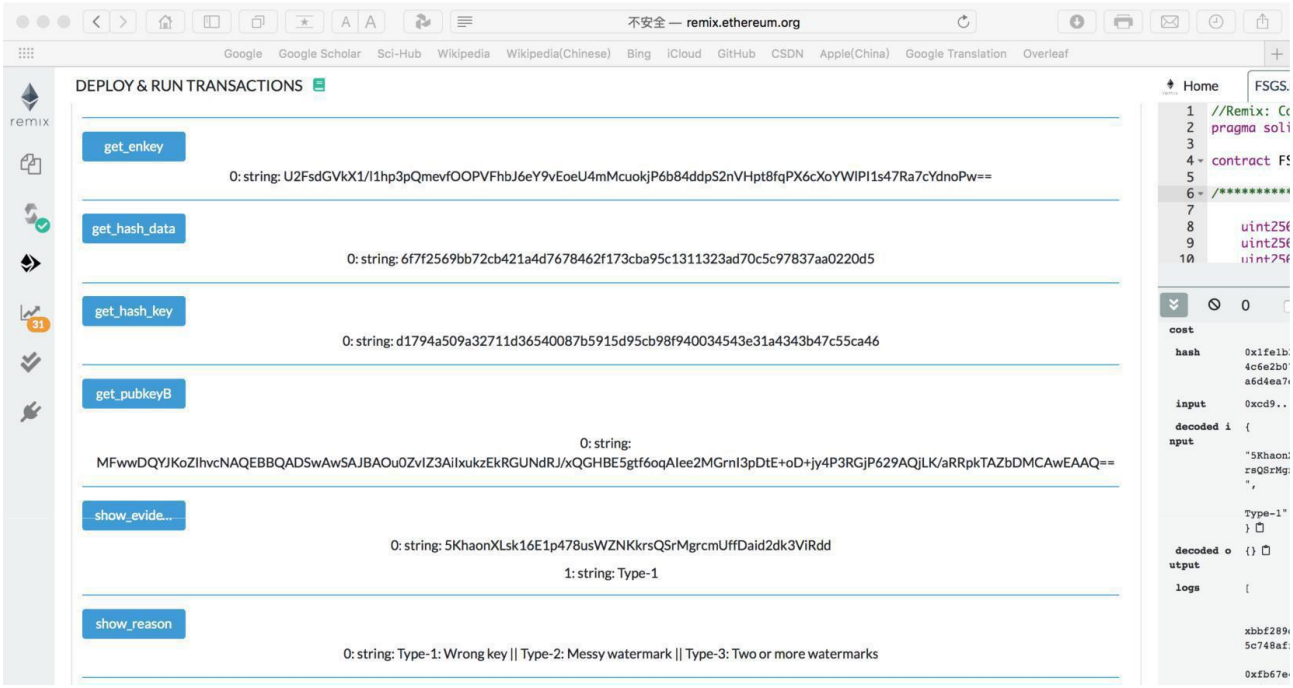

Fig.14. *Keys, hash values and report*

The Fig.15 shows the time when the first, second and third step. Both parties in the transaction can do their step on time according to the time shows below and the time now.

The time now can be showed by pressing the bottom “CurrTimeInSecond” in Fig.13.

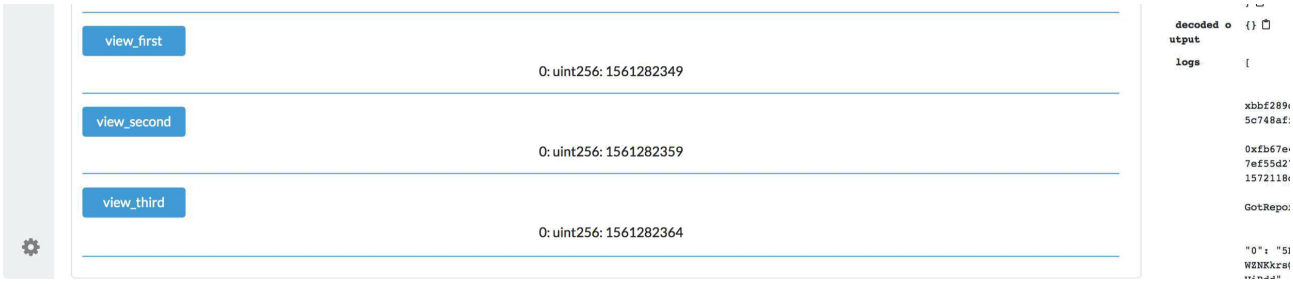

Fig.15. *The time each step finished*

3. Deal with the wrong operations

3.1 Wrong amount of money or deposit

If Alice sends wrong amount of the deposit or Bob sends the wrong amount of the money, the transaction will not continue until the right amount is sent. For example, if Alice sends wrong amount of deposit, it shows “The value of the deposit is wrong”, and Alice should send the right to continue the transaction, which is shown as Fig.16.

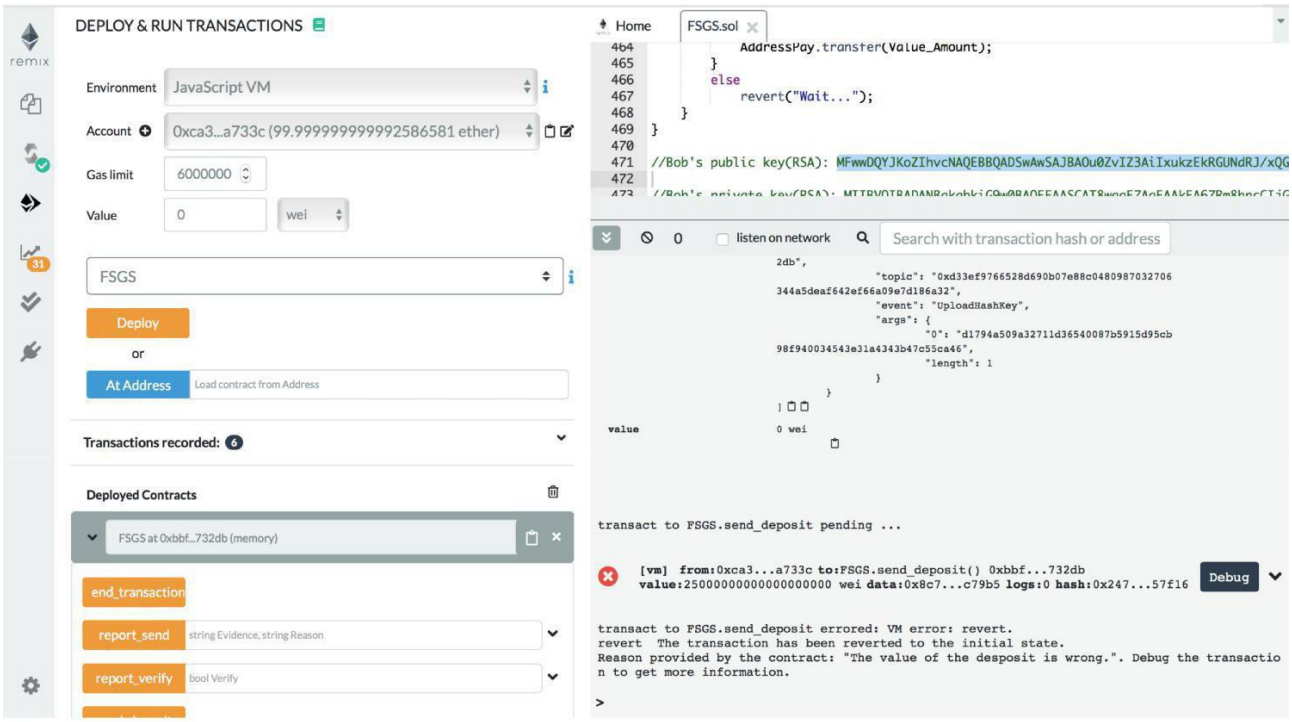

Fig.16. *Wrong amount of deposit*

3.2 The order is wrong

In our scheme, every participant should obey the order of transaction, if the order is wrong, the participant should finish the step before first. For example, Bob can pay after Alice sends the deposit, if Alice has not sent but Bob tries to pay, it shows “Seller should send deposit first”, as shown in Fig.17.

3.3 The time is run out

If Alice sends the deposit but in transaction time, there is no one accept transaction, Alice can press the bottom “end_transaction”, and the smart contract will send back the deposit to Alice, as shown in Fig.18. Also, if Alice sends the deposit and Bob sends the money, but the transaction ends in step 2 because the transaction time is run out, both parties can press the

bottom “end_transaction” and then, Alice will receive the deposit and Bob will receive the money.

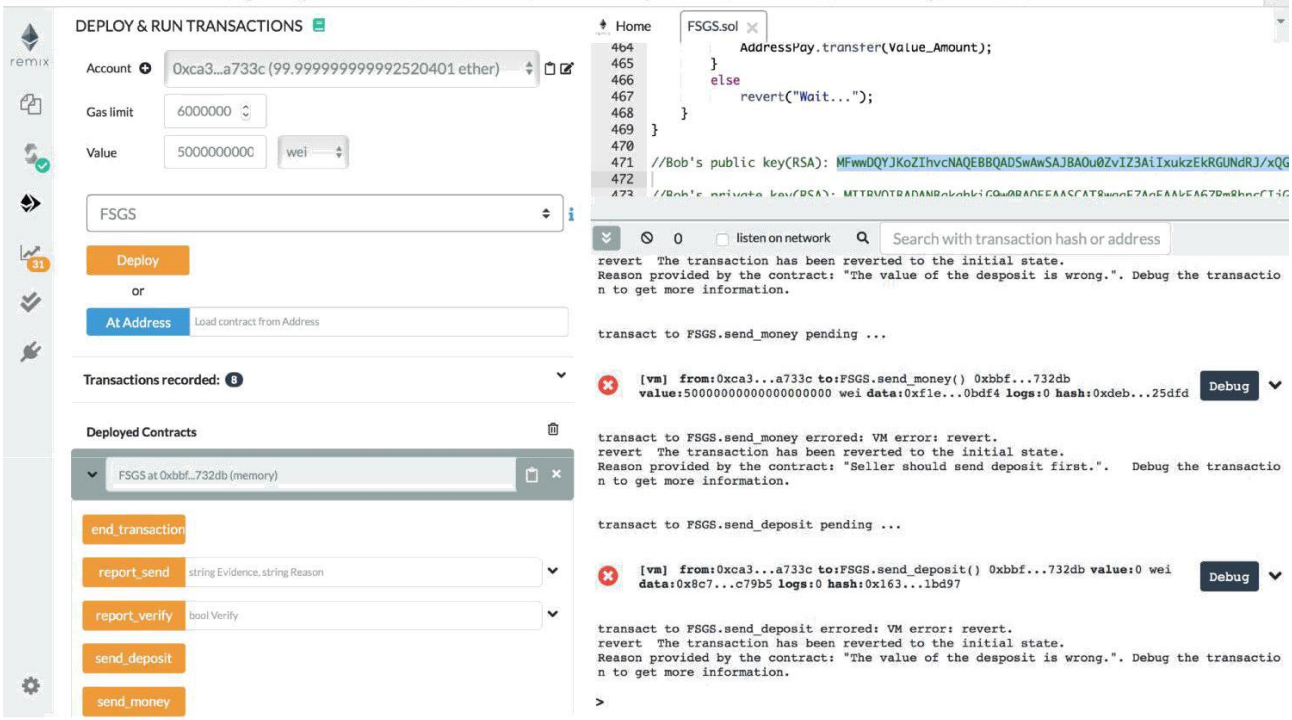

Fig.17. *Wrong order*

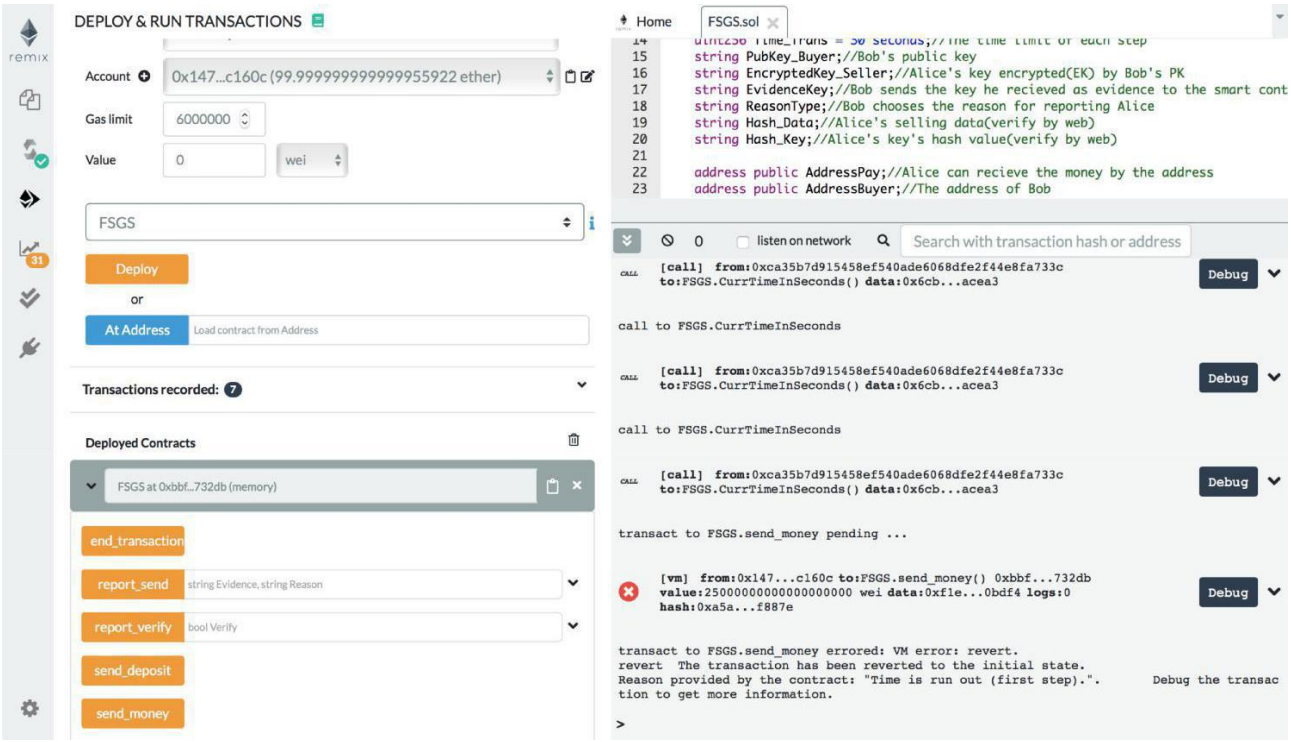

Fig.18. *Time is run out*