Privacy of smart contract? How can one implement “private” smart contract on Ethereum? [duplicate]

This question already has an answer here:
Private Info on Ethereum *2 answers*

Based on my current reading, I understand smart contract as a code visible and runnable on the whole blockchain. The smart contract code could be published by author, and everyone can verify the code against the opcode in the contract address.

But how if someone wants to have privacy over their smart contract? How if they want to hide their detail implementation(to avoid hacker attack etc) while they want everyone to access and use their contract at the same time.

How to achieve private smart contract then?

privacy

asked Oct 3 '16 at 6:00
Lin
46 2

marked as duplicate by eth ♦ Mar 29 at 10:06

This question has been asked before and already has an answer. If those answers do not fully address your question, please ask a new question.

2 Answers

There are multiple projects and techniques for making transactions as "private" as possible. To name a few: Hawk Project, zk-SNARKS, Coinjoin and Ring Signatures. These are different in their approach and the problem they solve.

There is an excellent blogpost by Vitalkik Buterin regarding blockchain & smart contract privacy, where these are explained in more detail:
https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

answered Oct 4 '16 at 11:14
Jacob Eberhardt
181 6

Hackers can't manipulate your code. They can only execute it like all other people. Smart contracts are hacker resistant. If you leave a hole in your system so anyone can enter and execute the code they see via that hole. The_Dao wasn't exactly an hack, it was an exploit, the code was written in the wrong way.

Anyone can see your compiled code on the blockchain, but in order to understand how it works they need a human readable code usually. If you don't publish the "human-version" they will only see the compiled code. At the moment, there is no tool allowing you to get the human code starting from the compiled one.

If you code is VERY easy (?!?) so maybe one can understand something from the compiled version. I could never recognize a code written by me if you show me the compiled version.

check this one

https://etherscan.io/address/0x2f593f1809876bf76d0992e0527a19d56b44754c

there is a TAB: contract code

click and see the link VERIFY AND PUBLISH, if you know the original "human" code you can publish it, the system will compile it and compare it to the compiled code existing online, if they match it is accepted and shown, and people can audit the compiled one reading the human version.

This is how it works. If I use a dapp, I can easy find in js the contract address. You can't hide a contract. You could fill the contract with lot of rubbish code, so the compiled version will be more complex, if you want to feel more comfortable. But so far I never met anyone very comfortable with reading the compiled code.

You can make a test, write a code, and offer a bounty to see if anyone can read it.

answered Oct 3 '16 at 11:33
Max
31 3

Thanks Max! Do you know any smart contract that is quite commonly used but the author didn't publish the original readable code? My concern is, in order to convice people my code is save and trustable, I need to publish readable code. But by doing that, I'm opening for any hackers to make use of any mistakes I made in the smart contract. I'm not sure if my understanding is correct. Looking forward to hear from you :) – Lin Oct 5 '16 at 9:42

All people use paypal and they don't know the code.. But this is a different community. You must simply write the right code with no errors and no bugs.. – Max Oct 12 '16 at 21:27