

/r/ethereum

COMMENTS

16

Is the entire source code of any smart contract always publicly visible?

self.ethereum

Submitted 2 months ago by chescos

7 comments share report

all 7 comments

sorted by: top (suggested)?

Want to add to the discussion?

Post a comment!

SIGN UP[-] **saddit42** 10 points 2 months ago

The byte code. It's probably possible to reverse engineer though.

permalink embed report

[-] **bagofEth** 3 points 2 months ago

To elaborate, every full node in the network needs to maintain a copy of the latest state (which includes smart contract bytecode). Its definitely possible to reverse engineer most of the contract just by looking at opcodes, but this would be very time consuming and difficult.

Block explorers like etherscan.io allow you to view the bytecode of smart contracts and also translate the bytcodes into opcodes. Check out this one for example:

<https://etherscan.io/address/0x4c09bd6dbe308c1e49bb0a408d10c9d1ea303197#code>

permalink embed parent report

[-] **alsomahler** 3 points 2 months ago

Technically not really necessary. You can decide to **only** share the contract with the parties involved. But if you want people to sign a contract, they need to at least see the contents.

Think of it as a paper contract. Would you sign something that you couldn't read?

The distribution and payment of ether is a public contract (currently hardcoded in every full client, but in the future is also planned to become an EVM contract)

Submit a new link

This post was submitted on 19 Aug 2017

16 points (88% upvoted)shortlink: <https://redd.it/6urviz>

username

password

☐ remember me [reset password](#)

LOGIN

ethereum

143,670 readers, 1,058 here

Subscribe

Welcome to [r/Ethereum](#), the front page of the Web 3.

Rules

- No inappropriate behavior. This includes, but is not limited to: personal attacks, threats of violence, slurs of any kind, posting people's private information.
- **Keep price discussion and market talk, memes & exchanges to subreddits such as [/r/ethtrader](#)**
- Keep plain ICO advertisements to subreddits such as [r/ethinvestor](#).
- Keep mining discussion to subreddits such as [r/EtherMining](#).
- No duplicate threads.
- No spamming or drive by posting.
- No misleading titles.
- No creating multiple accounts to get around Reddit rules.
- English language only. Please provide accurate translations where

... so if you want to make a contract that interacts with it, it automatically also has to become public.

Anything that doesn't use ether, doesn't have to be public... only among those who sign. But if you want to decentralise the enforcement of double spending by the hashing power of the network, then you'll need to make it public again.

(For simplicity I'm counting "byte code" as source code)

[permalink](#) [embed](#) [report](#)

[–] **ItsAConspiracy** 1 point 2 months ago

Not necessarily, but if you want other people to use the contract, you pretty much have to publish verified source on etherscan.

[permalink](#) [embed](#) [report](#)

[–] **interition** 2 points 2 months ago

I have not tried it but evm bytecode can be reverse engineered into solidity with porosity
<https://github.com/comaeio/porosity> .

I would guess that what you will not get is the idea behind the code that would be hinted at through the variable, function names etc. because that would be lost in translation

[permalink](#) [embed](#) [report](#)

[–] **infernal_toast** 1 point 2 months ago

There are probably ways to obfuscate the code and make it harder to reverse engineer the bytecode ?

[permalink](#) [embed](#) [report](#)

[–] **[deleted]** -4 points 2 months ago

Yes.

[permalink](#) [embed](#) [report](#)

appropriate.


- Posts and comments must be made from an account at least 10 days old with a minimum of 20 comment karma. Exceptions may be made on a discretionary basis.
- Public moderation logs [can be found here](#).
- For a complete list of rules and an Ethereum getting started guide, [click here](#).

Resources

- [Website & Blog](#)
- [White Paper & Yellow Paper](#)
- [Devcon 3](#) (Cancún, 2017)
 - [Devcon 3 Chat on Riot](#)
 - [Devcon 3 Social Events](#)
- [Documentation & Stack Exchange](#)
- [Learn Solidity](#)
- [Source Code on Github](#)
- [Bounty program](#)
- [Chat on Gitter](#)
- [Network Status & Gas Price Market](#)
- [List of DApps](#)
- [Meetups](#)
- [Twitter](#), [Facebook](#), [Google+](#)

MODERATORS

[message the moderators](#)

[vbuterin](#) Just some guy
[thehighfiveghost](#) Melonport
[nickjohnson](#) Ethereum - Nick Johnson
[heliumcraft](#) Embark Framework - Iuri Matias
[insomniasexx](#) 
[5chdn](#) Flair
[avsa](#) Ethereum - Alex van de Sande
[etherpropeller](#)
[rzurrer](#)
[publicmodlogs](#)

...and 1 more »

< > discussions in [r/ethereum](#) X

387 · 42 comments



Real estate title transfer on-chain.
The property keys were finally exchanged at Devcon3!

CSS Theme via [/r/Naut](#)

about

- [blog](#)
- [about](#)
- [source code](#)
- [advertise](#)
- [careers](#)

help

- [site rules](#)
- [help center](#)
- [wiki](#)
- [reddiquette](#)
- [mod guidelines](#)
- [contact us](#)

apps & tools

- [Reddit for iPhone](#)
- [Reddit for Android](#)
- [mobile website](#)
- [buttons](#)

<3

- [reddit gold](#)
- [redditgifts](#)

Use of this site constitutes acceptance of our [User Agreement](#) and [Privacy Policy](#). © 2017 reddit inc. All rights reserved.
REDDIT and the ALIEN Logo are registered trademarks of reddit inc.