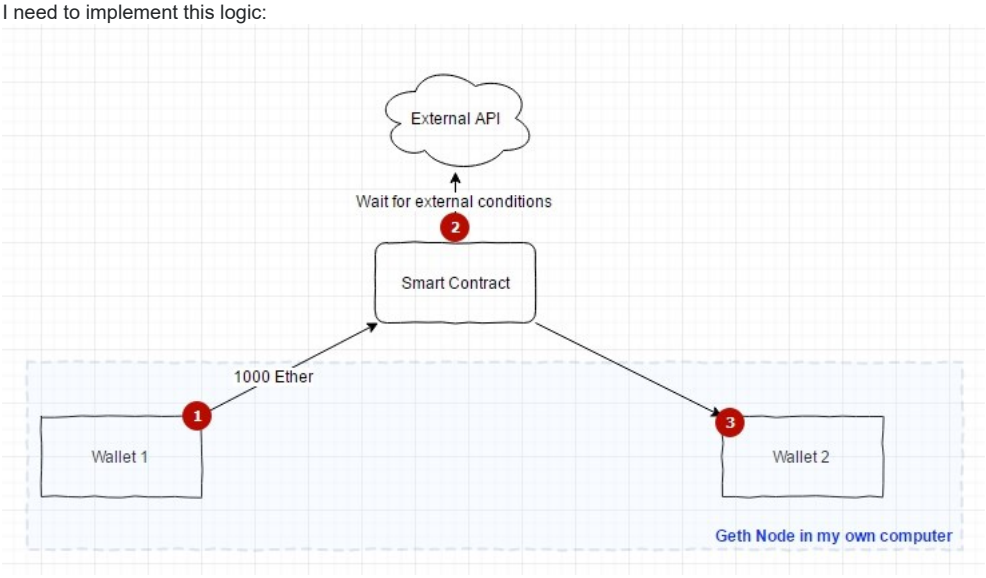
Does this architecture violate a Dapp-philosophy?

Sorry for my English, again...
First I wanted to place this post on Etherium Reddit. If it needs to be there, just close this question...

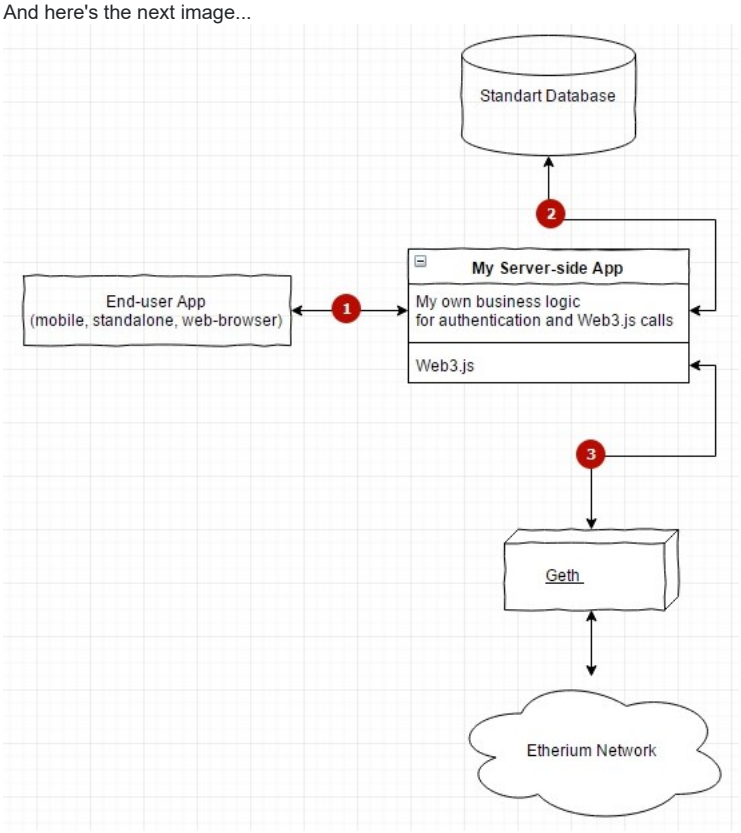
I need to implement this logic:



1. From *Wallet 1* user sends *Smart Contract* 1000 Ether by calling a function in *Smart Contract*.
2. *Smart Contract* holds 1000 Ether until some external event occurs. *Smart Contract* checks this by polling information from *external API*. If this event does not occur after two days *Smart Contract* reverts Ether.
3. *Smart Contract* sends 1000 Ether to Wallet 2 (if the external condition of the previous step does occur).

But I need do this for users who can`t have blockchain ("Etherium Wallet" app e.g.) on own computers.

And here's the next image...



1. Standart authentication - Login/Pass, OAuth, not important...
2. We identified the user credentials and associate it with a particular Wallet Account (0x123...).
3. Now we send commands to Geth using the Wallet Account of the previous paragraph.
4. Finally, end-user has a limited set of possibilities by using the UI in the end-user app.

Is it okay to do this server-side layer, and do some authentication?

dapp-development design-patterns architecture

edited Jan 24 at 12:58

Rob Hitchens
11.2k 1 11 42

asked Jan 24 at 11:44

Artem
172 1 10

1 I corrected some syntax to help you out. Please check I haven't distorted your intentions in the process. – Rob Hitchens Jan 24 at 13:04

Why does this application need a blockchain? – Edmund Edgar Jan 24 at 13:26

@Edmund Edgar, I am a programmer in the Bank, We want to start use blockchain, but our clients and top managers doesn`t ready to future :) So we do DAPP, but we also do "traditional" interface for this DAPP. If this app will be a success, we want to develop fully decentralized service. – Artem Jan 24 at 13:37

2 It looks like it'll work. If there's only one server writing to it then having the blockchain there isn't very useful, but I understand your situation. This kind of thing makes a bit more sense in a consortium situation, where you'd have multiple companies each with their own database controlling access to their own users, but the companies are connected to each other through the blockchain. – Edmund Edgar Jan 24 at 13:46

I agree with @EdmundEdgar but I'd also add that if the end users are not actually storing their own keys, it may make more sense for the server to just have one key, and have total administrative control from just that one key. It would be no less secure, and the server would only need to manage and protect one key. – Tjaden Hess ♦ Jan 25 at 18:15