Project Crowbar

Manual trading wallet app specifications

v0.0.5a

1. The concept of the app is a wallet app with built-in simplified trading terminal, complexity and feature set of which can grow, based on contest outcomes.
2. The app should be serverless client to interface with data logging smart contract deployed on Ethereum network
3. Gas price and gas amount should be configurable on a Settings screen
4. There should be authentication as in MyEtherWallet - simple private key decryption with a pass.
5. Optional, but very desired would be auth with a hardware device like Ledger Nano
6. It has to be able to interact with Kyber Network, Bancor and/or Radar Relay via API
7. There should be two operations - buy and sell with corresponding buttons
8. Operations should be bounded to some captcha-like solvers to ensure human-only interaction.
   The problem with this requirement is that app should be serverles - therefore using regular captcha solutions doesn’t make much sense, in a same way as using 2FA from Google doesn’t make much sense in MyEtherWallet. The approach to this problem could be solved in two ways:
   a. By lessening restrictions on a contest preconditions. If we consider division between manual and automated traders to be informal, then there is no need for strict segregation. Of course hypothetical attacker can develop such a software that will mimic interaction with contract in a same way as manual trading app does. But to affect test results this informal segregation has to be violated in a vast majority of cases. And the effect would be similar as described in white paper section **3.3 Possible attack vectors** so outcomes and protection would be similar as well.
   b. By ensuring human-only interaction with manual app. This will require centralized server in some way. The app still would interact with blockchain directly, but in

order for transactions to be eligible for payout, they will have to contain specific nonce attached to data field of transaction, same as one showed on a server. The nonce can be generated from process running Google 2FA on an offline device. The device would be seeded randomly and the seed would be be kept secretly until contest end. The 2FA nonce could be captured by a camera and the resulting image can be transformed to ensure human only recognition in order to exclude most software solvers to some predictable limit. However, in order to avoid mistakes in recognition by human users - validation of nonce can be introduced on device. The 2FA seed than has to be known to server, just held secret until end of the contest. The requirement to pass captcha to make transaction could be very inconvenient for traders, but as in case of growing number of requests for 2FA on MyEtherWallet - users are ok with such measures when it concerns security. The capture requirement in the case of trading app may seem a bit artificial, but still it contributes to validity and quality of statistical data and prevents some possible(at least theoretically) manipulations.

9. The app has to have Amount field
10. The app has to have Volume field
11. Calculations/conversions between amount and volume field should be automatic, based on conversion ratio (price) coming from bancor protocol.
12. Optional suggested price/24h volume etc indicator could be shown by obtaining price from some API endpoint for example at
    a. CryptoCompare
    https://min-api.cryptocompare.com/data/price?fsym=IML&tsyms=BTC,USD,ETH
    https://min-api.cryptocompare.com/data/price?fsym=SNM&tsyms=BTC,USD,ETH
    b. CoinMarketCap.com
    https://api.coinmarketcap.com/v1/ticker/<coin_id>/
    https://api.coinmarketcap.com/v1/ticker/bitcoin/
    https://api.coinmarketcap.com/v1/ticker/ethereum/
13. App should be crossplatform, optionally it has to leverage .NET ecosystem by using Mono to cover Linux-like OS types, Xamarin.Forms to cover mobile platforms for Android, iOS, UWP (also desktop via Windows 10). Interacting with Ethereum should be performed then via Nethereum wrapper. Rich charting can be achieved with Syncfusion portable charting controls.