I was shocked to learn that several dozen Ethereum people tested positive (or were refused testing despite being symptomatic) for COVID-19 in early/mid March – closely followed a Google spreadsheet that showed Ethereum community members with COVID-19 symptoms with a few other bits:

1. who had what symptoms [name, Twitter handle]
2. what locations people may have been infected
3. whether the person was hospitalized
4. whether the person recovered

This was a form of distributed contact tracing

powered not by dapps and crypto but by public tweets and public Google Docs, but it showed a ton of personal information … so, sadly, the spreadsheet was taken down for privacy reasons (I think …). I hope all of the people (and probably hundreds of people likely infected by the people on the sheet) have recovered and will exit from self-quarantine in the next couple of weeks.

Well, all of us are aware of China's massive success in cutting down the reported cases through horrifying authoritarian measures. The goal is to reduce transmission of disease by bringing R0=0 or at least under 1, but in China it was done in part through by smartphone applications with zero privacy (e.g. you can't get on public transportation without your app showing "GREEN" because its tied to national databases doing ML on everything associated with your digital identity). Singapore recently released a mobile app TraceTogether that uses Bluetooth Low Energy (BLE) in a less authoritarian way, but still relies on a central database, and so many engineering efforts are going to follow Singapores lead in a more privacy conscious way. An excellent summary to catch up on these effort is Cho et al (2020)'s Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs.

Well, I have spent the last few weeks working withCoEpi to engineer open source iOS app/Android app/server implementations of a "CEN protocol" (CEN=Contact Event Number, where CEN is what your phone broadcasts to others and receives from others in a Bluetooth neighborhood) to get at pretty good privacy-preserving distributed contact tracing, using elementary crypto primitives familiar to all of us.

CoEpi apps works like this, following a CEN protocol (now called TCN), in storyboard form:

1. Alex got COVID-19 at EthCC on March 5th, but he didn't know that at the time.
2. Vitalik got within sneezing distance of Alex on March 5th at EthCC, but Sourabh did not.
3. Alex and Vitalik's CoEpi apps are sharing CENs, but never with a server.
4. Alex finds out he has COVID-19 on March 12th and send his report to a CEN node (along with some information X), to altruistically share with all the people who know his CEN
5. Vitalik and Sourabh download potential infectors from a CEN node.
6. Vitalik finds a match on X, and might deduce that it was at THIS lat-long-time, and probably Alex, but ideally Vitalik shouldn't know if possible.
7. Sourabh does not find a match, and nor does any government, any CEN node.

In all cases the user is under control of their altruistic report, but the goal is to not have snoopers, your contacts or the government learn much about you. The end result is reduction of disease transmission through altruistic reporting while preserving privacy, and not privacy of medical information more generally, which can be done with other means.

I encourage all of you to apply your crypto engineering skills to this pressing problem. Now that Apple and Google have joined in, we need to hold Big Tech/Big Govt in check, while still allowing life saving activity to occur.