Pandemics and Blockchains

Interreg
North Sea Region
BLING
European Regional Development Fund

EUROPEAN UNION

Danny Dreves
BCLD member
Tech enthusiast

DRENTHE
LAB
BLOCK
CHAIN

Current pandemic, COVID-19 (*coronavirus disease 2019*)

- Relative low mortality rate (3-6%) compared to other pandemics, but much more contagious
- Stays active on surfaces
- Cured: no health problems for 24 hours. This means: no fever, no nose cold and no cough.
- Infected people without symptoms can spread the virus (indications, no proof yet)
- Incubation period , max 14 days

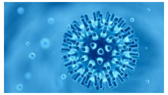
Approach in the Netherlands:

- Building (group) immunity
- Manage stress on Healthcare

Solution: Targeted lock-down

- Social distancing, avoid contact with people, at lease 1,5 m distance
- Close all public places except businesses where the 1,5 m rule can be applied

Fight the spread with Apps



- 1 Self-Assesment and remote care
  - Diagnostics
  - Smart Sensors
- 2 Track physical contact (proximity)
  - Based on creating and maintaining group immunity without massive and inclusive physical testing
  - Call for participation to companies and organisations by the Dutch Govn.
  - 750 callers, during appathon weekend 17-18 april a selection of 5 is being put to the test (public available)
  - In addition to GGD (Public Health Service) work-process.
  - Disclosed source, only to experts
  - Privacy-first
- 3 Support transition strategy (3rd wave of apps)

Taiwan
Electronic Fence

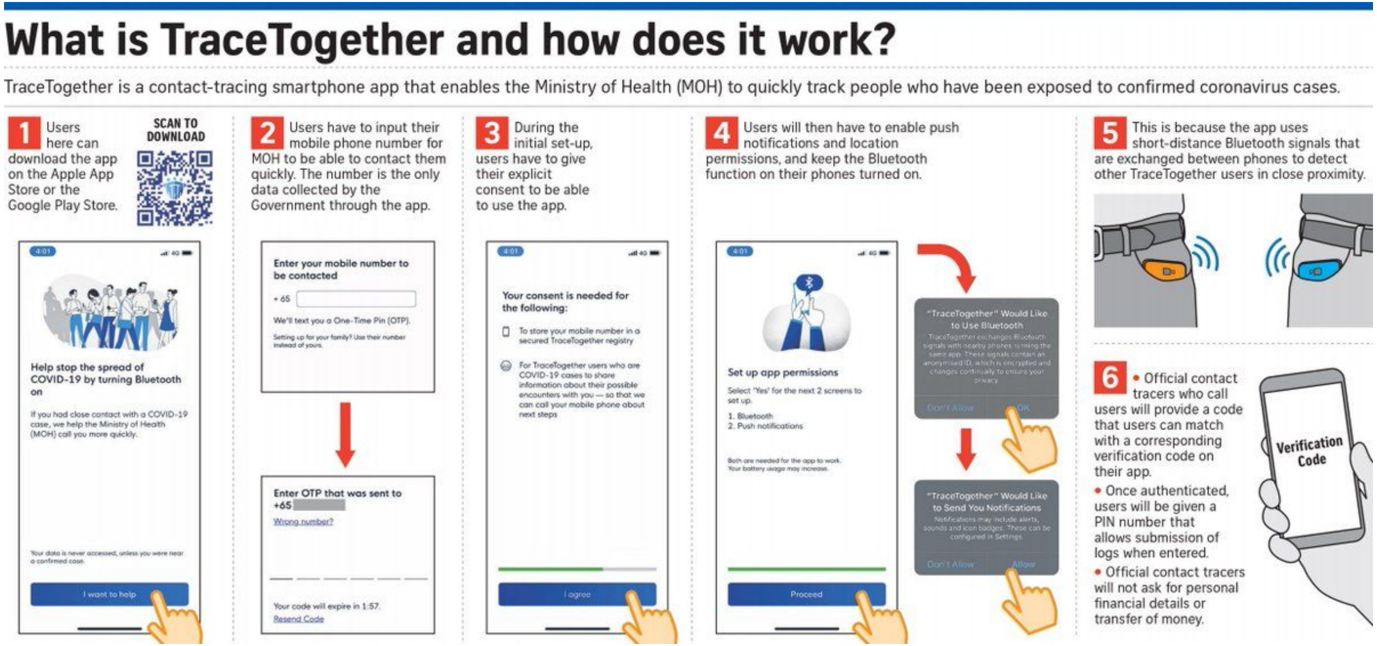
> “The goal is to stop people from running around and spreading the infection,”

The “electronic fence” uses mobile phone data to notify police if the cell phones of any people under mandatory quarantine leave their home areas.

If caught, quarantine dodgers are subject to a 1,000,000 NTD fine, which equates to around $33,000 USD

Canada is also thinking about Telco supported track & trace

Singapore
TraceTogether



What is TraceTogether and how does it work?

TraceTogether is a contact-tracing smartphone app that enables the Ministry of Health (MOH) to quickly track people who have been exposed to confirmed coronavirus cases.

1 Users here can download the app on the Apple App Store or the Google Play Store.

SCAN TO DOWNLOAD

4:01

Help stop the spread of COVID-19 by turning Bluetooth on

If you had close contact with a COVID-19 case, we help the Ministry of Health (MOH) call you more quickly.

Your data is never accessed, unless you were near a confirmed case.

I want to help

2 Users have to input their mobile phone number for MOH to be able to contact them quickly. The number is the only data collected by the Government through the app.

Enter your mobile number to be contacted

+ 65

We'll text you a One-Time Pin (OTP).

Setting up for your family? Use their number instead of yours.

Enter OTP that was sent to +65 [redacted]

Wrong number?

Your code will expire in 1:57.

Resend Code

3 During the initial set-up, users have to give their explicit consent to be able to use the app.

4:01

Your consent is needed for the following:

To store your mobile number in a secured TraceTogether registry

For TraceTogether users who are COVID-19 cases to share information about their possible encounters with you — so that we can call your mobile phone about next steps

I agree

4 Users will then have to enable push notifications and location permissions, and keep the Bluetooth function on their phones turned on.

4:01

Set up app permissions

Select 'Yes' for the next 2 screens to set up.

1. Bluetooth
2. Push notifications

Both are needed for the app to work. Your battery usage may increase.

Proceed

"TraceTogether" Would Like to Use Bluetooth

TraceTogether exchanges Bluetooth signals with nearby phones running the same app. These signals contain an anonymised ID, which is encrypted and changes continually to ensure your privacy.

Don't Allow | OK

"TraceTogether" Would Like to Send You Notifications

Notifications may include alerts, sounds and icon badges. These can be configured in Settings.

Don't Allow | Allow

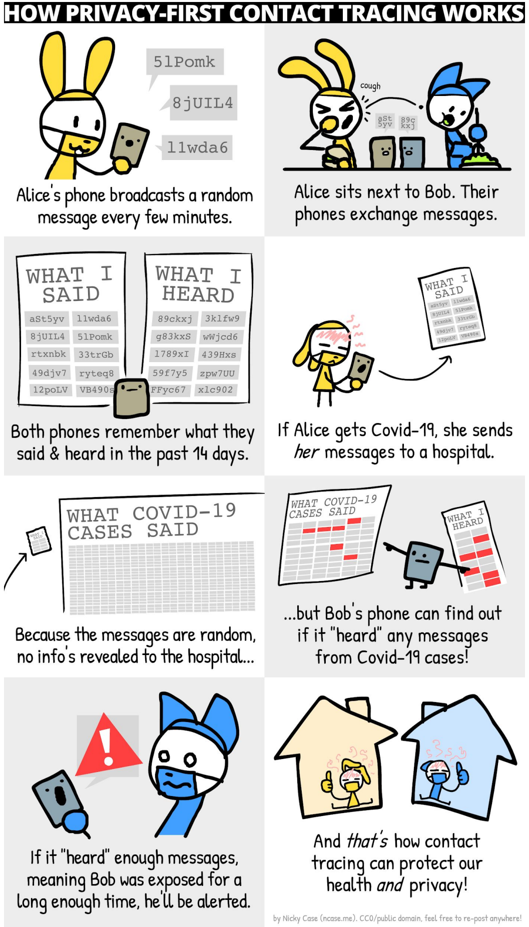
5 This is because the app uses short-distance Bluetooth signals that are exchanged between phones to detect other TraceTogether users in close proximity.

6
- Official contact tracers who call users will provide a code that users can match with a corresponding verification code on their app.
- Once authenticated, users will be given a PIN number that allows submission of logs when entered.
- Official contact tracers will not ask for personal financial details or transfer of money.

Interreg North Sea Region BLING
European Regional Development Fund
EUROPEAN UNION

DRENTHE LAB BLOCKCHAIN

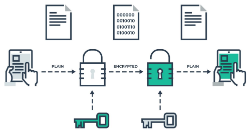
DP3T
Track physical contact


HOW PRIVACY-FIRST CONTACT TRACING WORKS
51Pomk
8jUIL4
l1wda6
Alice's phone broadcasts a random message every few minutes.
cough
aSt5yv
89ckxj
Alice sits next to Bob. Their phones exchange messages.
WHAT I SAID
aSt5yv l1wda6 8jUIL4 51Pomk rtxnbk 33trGb 49djv7 ryteq8 12poLV VB490s
WHAT I HEARD
89ckxj 3k1fw9 g83kxS wWjcd6 1789xI 439Hxs 59f7y5 zpw7UU FFyc67 x1c902
Both phones remember what they said & heard in the past 14 days.
WHAT I SAID
If Alice gets Covid-19, she sends her messages to a hospital.
WHAT COVID-19 CASES SAID
Because the messages are random, no info's revealed to the hospital...
WHAT COVID-19 CASES SAID
WHAT I HEARD
...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!
If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.
And that's how contact tracing can protect our health and privacy!
by Nicky Case (ncase.me). CC0/public domain, feel free to re-post anywhere!

Decentralized
Privacy-Preserving
Proximity Tracing
(protocol), from
https://www.pepp-pt.org/

Risks:
Replay attack
False alert injection
False report
Backend impersonation (MitM attack)
A New Tool for Tracking People (with all unwanted side effects)
Deanonymizing Known Reported Users
Paparazzi attack
Nerd attack
Mitigation ? strong but very complex TPM infrastructure
Disclosing Private Encounters

Homomorphic Encryption



Homomorphic encryption can be used for privacy-preserving outsourced storage and computation. This allows data to be encrypted and out-sourced to commercial cloud environments for processing, all while encrypted

Shafi Goldwasser (https://dualitytech.com/)

“So the government might say to a telecoms firm like Vodafone: ‘We have a list of 100 Covid patients, we know who they are. You [Vodafone] will never know who they are. And you will give me back all the locations that these people have been in, in the last say two weeks.”

“The next part is, the government says ‘Listen, give me anyone else at these locations at the time [the patient was there]’, and again you provide me with only the right answer without me having to see the location data of all the population. “The government only sees who matches up, and Vodafone doesn't see anything. Because you don’t want the government to see everyone’s location data, and you don’t want to tell Vodafone who is sick. Every side sees only what it has to see. Nothing more than that.”

Interreg North Sea Region BLING European Regional Development Fund
EUROPEAN UNION
DRENTHE LAB BLOCKCHAIN

Risks ? Blockchain to the rescue!

Blockchainlab Drenthe:

Blockchain technology (DLT) is useful voor systems with participants how do not know each other, they have to trust each other, and there is a (strong) incentive to cheat.

Blockchain to the rescue!

One promise of BC (DLT) tech : Disintermediation, cut out the middle man

Why ?

- Let the system be the governing body and do the governance
- Let parties (e.g. persons) be self-sovereign (in control) of their data
- No manipulation or abuse of data through the use of smart contracts

Blockchain to the rescue!

How ?

- Instead of letting the hospital make the heatmap of proximity, let's have a smart contract using Homomorphic Encryption do the risk assessment and publish the artifacts about infection, in a way that if you are at risk, you don't know from who (Zero Knowledge Proof)
- Through self-sovereign identity systems onboarding on the system can be done safely, without making clear who was where at what time.
- Offboarding (you decide to leave the network) is facilitated by just throwing away your keys.

Interreg North Sea Region BLING European Regional Development Fund EUROPEAN UNION

3rd Wave Apps

- Register test-results (clearance for travel) in a Zero Knowledge Proof way. To Enter for instance an Hospital, you only have to proof that you have a recent negative COVID-19 test-result. (This is actually a nice Blockchain use-case)

  https://dutchblockchaincoalition.org/nieuws/blockchain-ssi-voor-privacy-vriendelijke-corona-verklaringen

- Supply Chain Management (digitalisation and certification of assets like tests or medical supplies)

DRENTHE LAB BLOCKCHAIN

Thank you!

- Stay in, check https://www.rijksoverheid.nl/actueel/nieuws/2020/04/15/ministerie-van-vws-organiseert-digitaal-evenement-voor-beoordeling-corona-apps for details about the upcoming appathon .
- check and try to spot the usage of Homomorphic Encryption and/or Blockchain https://en.wikipedia.org/wiki/COVID-19_apps

DRENTHE LAB BLOCKCHAIN

reference

- https://www.rivm.nl/en/novel-coronavirus-covid-19/current-information-about-novel-coronavirus-covid-19
- https://github.com/DP-3T/documents
- https://eprint.iacr.org/2020/399.pdf
- https://qnewtech.com/author/lina-smith/
- https://dualitytech.com/wp-content/uploads/2020/04/The-Telegraph-The-tech-that-can-track-a-pandemic-without-sacrificing-privacy.pdf

Interreg
North Sea Region
BLING
European Regional Development Fund
EUROPEAN UNION

DRENTHE LAB BLOCKCHAIN