FS Club

Covid-19 Contact Tracing:
A Solution?
A Privacy & GDPR Nightmare?
A Technical Bridge Too Far?

28 May 2020

Maury Shenk
in conversation with
Professor Michael Mainelli

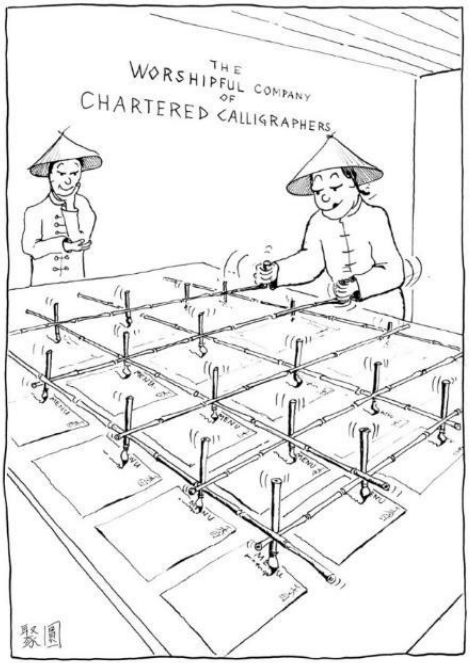
With Thanks To Our Sponsors

FS Club

Agenda

FS Club

- Permission frameworks
- What is contact tracing and why might it matter?
- Efficacy concerns
- Who's done what? Who's doing what?
- Privacy & GDPR concerns
- Outlook



"Get a detailed grip on the big picture."
Chao Kli Ning

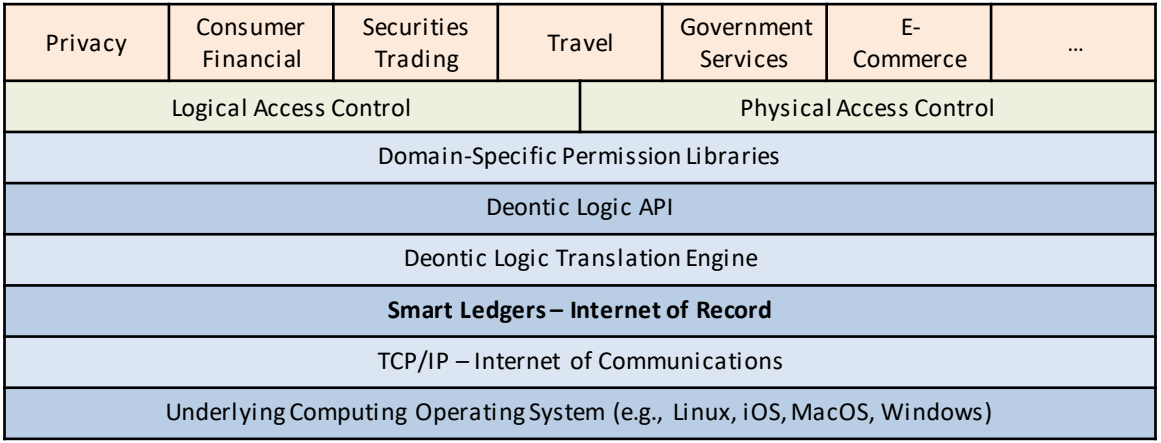
Why We Need Permissions Frameworks

FS Club

- Permission (or not) to use digital / online resources is at the core of our information economy
- But there are major holes in existing frameworks
  - No widely-accepted standards
  - Major cybersecurity issues as more devices come online (e.g. IoT)
  - Difficulty of implementing concepts of "may" and "should" (or not) on Boolean devices
- Need to move beyond access control

Structure Of A New Permission Architecture

FS Club



Choosing A Permissions Framework

FS Club

- Criteria
  - Precision – ability to accurately convey permissions
  - Breadth – ability to convey any permission
  - Applicability – comprehensibility and practicality for real-world markets
- Candidates
  - Access control
    - Standard for computer systems
    - Comes in many flavors – e.g. access control list, role-based, attribute-based
  - Differential privacy – conveying information while avoiding disclosure of personal information
  - Deontic logic – formal logic of “may” and “ought”

Deontic Logic in Practice (for Identity)

FS Club

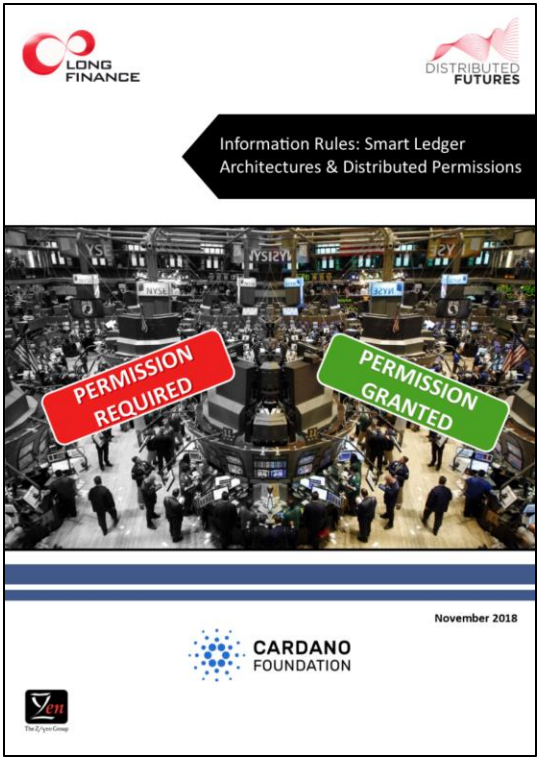
What a Human Hears	High-Level Proposition	Propositional Variables	Deontic Proposition
You are an authorised user of this computer system	Person X may access resource R	AR_X = X accesses resource R	$P(AR_X)$
If you are in the finance department, you may access the accounting system	If person X belongs to group G, she may access resource R	AR_X = X accesses resource R G = group G	$If\ X \in G \rightarrow P(AR_X)$
Would Mr. Jones please go to the ticketing desk	If recipient of message is person X, she should take action A	U = recipient of message A_X = X takes action A	$If\ U = X \rightarrow O(A_U)$ $If\ U = X \rightarrow O(A_X)$
Sorry, no admittance for under 18s	If person X is under age K, she may not access resource R	K_X = age of X AR_X = X accesses resource R	$If\ K_X < 18$ $\rightarrow \neg P(AR_X)$
No ID, no entry	If person X cannot prove she is over age K, she may not access resource R	K_X = age of X ID_X = identification documents in X's possession AR_X = X accesses resource R	$If\ (K_X > 18) \neg\vdash ID_X$ $\rightarrow \neg P(AR_X)$

Why and How Smart Ledgers?

FS Club

- Advantages over centralised solutions
  - Inherently distributed
  - Open architectures are common / understood
- Technical challenges
  - Functions to manage technical complexity – requires advanced, 'third generation' architecture
  - Implementing deontic logic on a Boolean computer
- Legal challenges
  - Differ by jurisdiction (e.g. Europe, US, China, India)
  - Tensions between GDPR and Smart Ledgers (e.g. erasure, repeated processing) are surmountable

Report



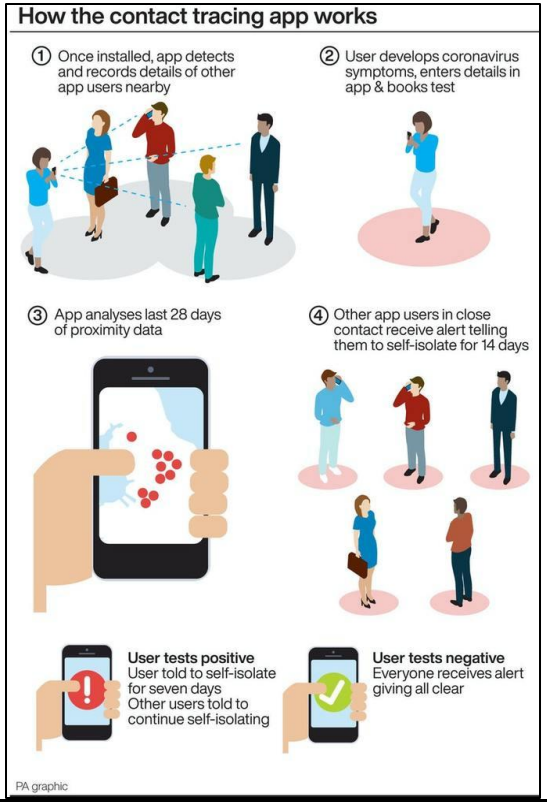
Read the report here.

Covid-19 Contact Tracing

FS Club

Contact Tracing & Smartphone Apps

FS Club



Documentation Apps

FS Club

Cov-ID

The Personal Digital Passport
In this era of Bio-security challenges

CATENAE INNOVATION

The Challenges

- Accelerating exponential growth of infections
- Risk of virus spreaders at events is significant
- Subsequent waves of infections likely
- Verification of an individual's Covid-19 status
- Disruption to business continuity
- Financial impact of shutdowns are considerable
- Increasing negative social and psychological impacts
- Need to fulfil duty of care to communities
- Difficulties with all scientific modelling

The Solution – Cov-ID

Bio-security that addresses the Corona virus threat

- The Covid-19 status verification App
- Fully-scalable cloud-based platform
- Core technology with demonstrable provenance
- GDPR compliant
- Designed to mitigate risk
- Provides verifiable Covid-19 status within defined environments where people congregate:
  - Multiple gatherings
  - Educational establishments
  - Business & workplaces

Features

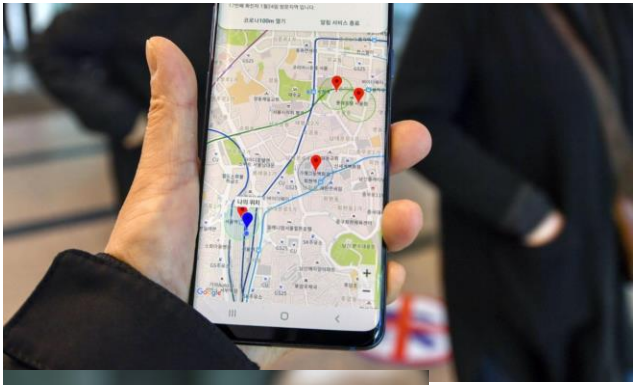
- Completely secure
- Personal information is encrypted, held in a digital wallet
- Participants control the use of their data
- Generic usage across all smart phones
- Easy to use App provides visual verification
- API into existing IT systems
- All transactions recorded to Distributed Ledger Technology

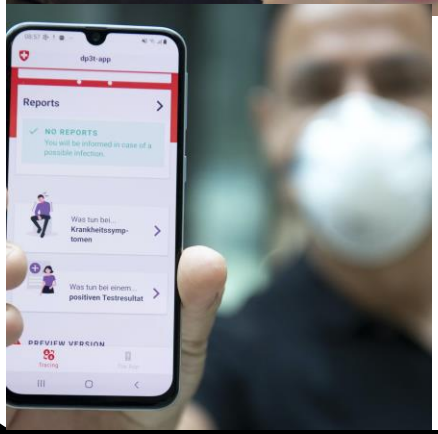
How it works

https://www.chainzy.com/case-studies/cov-id-project/

Tracing The World

FS Club





Singapore - TraceTogether

FS Club

What is TraceTogether and how does it work?

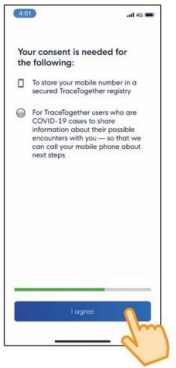
TraceTogether is a contact-tracing smartphone app that enables the Ministry of Health (MOH) to quickly track people who have been exposed to confirmed coronavirus cases.

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

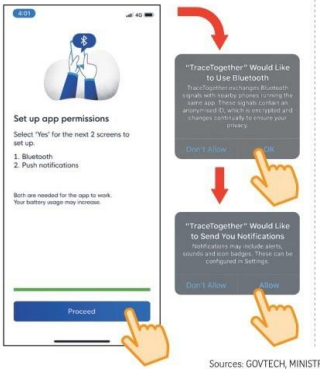
SCAN TO DOWNLOAD

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.

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



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



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.

Sources: GOVTECH, MINISTRY OF HEALTH PHOTOS: GOVTECH STRAITS TIMES GRAPHICS

A World Of Many Protocols

FS Club

Name	Architecture	Author/promoter	Licence
Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project	Central log processing, Ephemeral IDs	Fraunhofer Institute for Telecommunications, Robert Koch Institute, Technical University of Berlin, TU Dresden, University of Erfurt, Vodafone Germany, French Institute for Research in Computer Science and Automation (Inria)	multiple protocols, closed source, private specifications
Google / Apple privacy-preserving tracing project	Client log processing, Ephemeral IDs	Google, Apple Inc.	public specification
Decentralized Privacy-Preserving Proximity Tracing (DP-3T)	Client log processing, Ephemeral IDs	EPFL, ETHZ, KU Leuven, TU Delft, University College London, CISPA, University of Oxford, University of Torino / ISI Foundation	publicly-developed Apache 2.0 reference implementation
BlueTrace / OpenTrace	Central log processing, Ephemeral IDs	Singapore Government Digital Services	public specification, GPL 3 code
TCN Coalition / TCN Protocol	Client log processing,Unique IDs	CovidWatch, CoEpi, ITO, Commons Project, Zcash Foundation, Openmined	public developed specification, MIT License code
Whisper Tracing Protocol (Coalition App)	Client log processing, Ephemeral IDs	Nodle, Berkeley, California, TCN Coalition, French Institute for Research in Computer Science and Automation (Inria)	GPL 3
Privacy Automated Contact Tracing (East Coast PACT)	Client log processing, Ephemeral IDs	Massachusetts Institute of Technology, ACLU, Brown University, Weizmann Institute, Thinking Cybersecurity, Boston University	MIT License
Privacy-Sensitive Protocols & Mechanisms for Mobile Contact Tracing (West Coast)	Client log processing, Ephemeral IDs	University of Washington, University of Pennsylvania, Microsoft	
NHS contact tracing protocol	Central log processing, Ephemeral IDs	NHS Digital	private specification

Consortia Gloria

FS Club

Decentralized Privacy-Preserving Proximity Tracing (DP^3T)

École Polytechnique Fédérale de Lausanne, ETH Zurich, KU Leuven, Delft University of Technology, University College London, Helmholtz Centre for Information Security, University of Torino

- https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing
- https://github.com/DP-3T
- https://github.com/DP-3T/documents

Pan-European Privacy-Preserving Proximity Tracing (PEPP-3T)

Fraunhofer Institute for Telecommunications, Robert Koch Institute, Technical University of Berlin, TU Dresden, University of Erfurt, Vodafone Germany, French Institute for Research in Computer Science and Automation (Inria)

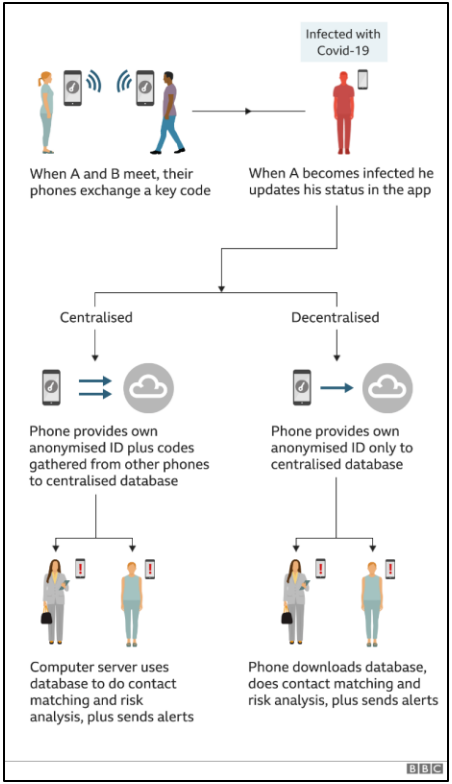
- https://en.wikipedia.org/wiki/Pan-European_Privacy-Preserving_Proximity_Tracing
- https://www.pepp-pt.org/
- https://github.com/pepp-pt
- https://github.com/pepp-pt/pepp-pt-documentation

Google/Apple Privacy-Preserving Contact Tracing Project

- https://en.wikipedia.org/wiki/Google_/_Apple_contact_tracing_project
- https://ico.org.uk/media/2617653/apple-google-api-opinion-final-april-2020.pdf
- https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology
- https://blog.google/documents/74/Android_Exposure_Notification_API_documentation_v1.3.pdf

Gapple & Aaggle

UK Contact Tracing



Privacy & GDPR Concerns

FS Club

- Raises basic principles of data protection law
  - Data protection by design and default
  - Processing for limited purposes and minimisation
  - Basis for processing – consent? public interest?
- European Data Protection Board recommendations (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf)
  - Must be voluntary
  - Favour national over third-party apps
  - No general sharing of location data
  - When identifying individual as infected:
    - Only after proper health assessment
    - Pseudonymous identifier
  - Centralised or decentralised solutions are acceptable
- Should the law bend to the exigencies of Covid-19?
  - Is this affected by concerns about efficacy of contact-tracing apps?

Efficacy Concerns

FS Club

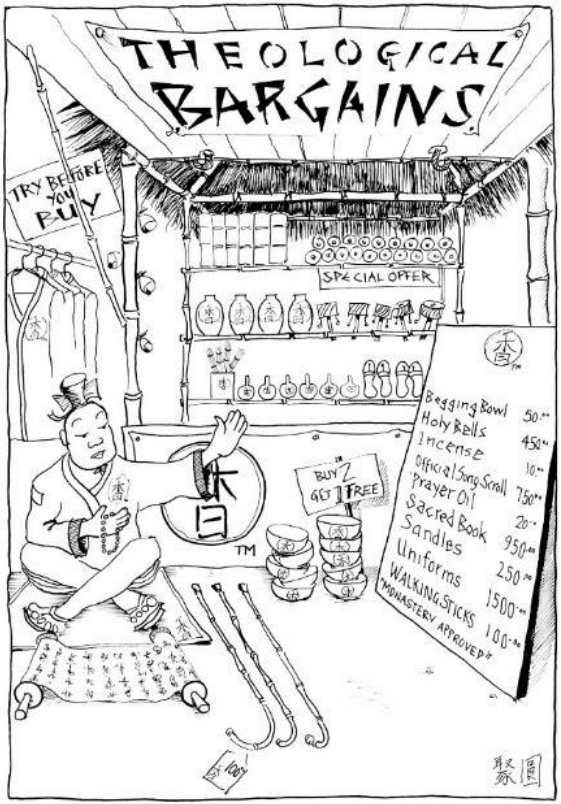
- False positives
  - Distance setting
  - Walls and partitions
  - Accuracy of GPS and Bluetooth
- False negatives
  - People without app (Singapore 20% takeup)
  - Accuracy of GPS and Bluetooth
  - Transmission versus contact, e.g. time, other circumstances
- Use
  - Really clear?
  - Really sure you want two weeks of quarantine
- Performance
  - Background working of Bluetooth
  - Battery

https://www.schneier.com/crypto-gram/archives/2020/0515.html#cg12

Questions, Comments, Answers(?)

FS Club

Outlook



With Thanks To Our Sponsors

FS Club