BIS

BIS Bulletin

No 17

On health and privacy: technology to combat the pandemic

Carlos Cantú, Gong Cheng, Sebastian Doerr, Jon Frost and Leonardo Gambacorta

19 May 2020

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. The authors are grateful to Giulio Cornelli and Taejin Park for excellent analysis and research assistance, to Rodrigo Moreno for graphical input and to Louisa Wagner for administrative support.

The editor of the BIS Bulletin series is Hyun Song Shin.

This publication is available on the BIS website (www.bis.org).

ISSN: 2708-0420 (online)
ISBN: 978-92-9197-385-8 (online)

Carlos Cantú carlos.cantu@bis.org
Gong Cheng gong.cheng@bis.org
Sebastian Doerr sebastian.doerr@bis.org
Jon Frost jon.frost@bis.org
Leonardo Gambacorta leonardo.gambacorta@bis.org

On health and privacy: technology to combat the pandemic

Key takeaways

- *Technology has been harnessed in the fight against the Covid-19 pandemic, eg to administer remote medical consultations, analyse aggregate movements and track paths of contact.*
- *Successful applications are predicated on broad public support. They must address concerns about data privacy, and the potential for misuse of data by governments and companies.*
- *Transparent public policies and clear governance frameworks can help to build trust. One possible approach is to differentiate data use during a pandemic and in normal times.*

Governments, technology firms and citizen groups are using new technology such as mobile applications (apps) to treat patients and contain the spread of Covid-19. While these applications hold substantial promise, users are concerned about their privacy. This Bulletin gives an overview of new technological applications, the different forms of control over data and the related privacy issues. It draws some lessons from the use of personal data in finance (BIS (2019)) to inform discussions on the use of health data and policies to address public concerns going forward.

Technological applications: a taxonomy

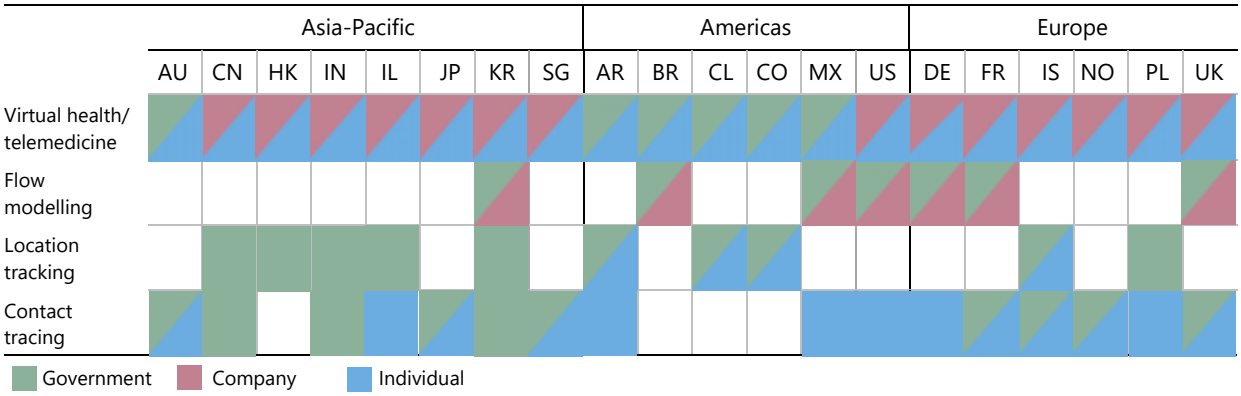
Four major types of new technological applications are widely used to fight the Covid-19 pandemic. (i) Telemedicine provides remote medical consultation for diagnosis, care or other non-emergency medical needs via mobile apps or websites. While telemedicine existed in the past, eg by phone, its use has expanded during the pandemic, and sometimes involves new intermediaries. (ii) Flow modelling assesses aggregate movements of people, eg how many people pass through an area and how quickly (*The Economist* (2020)). It often uses anonymous and aggregated geolocation data from mobile phones. (iii) Location tracking uses individuals' location to ensure that people follow quarantine rules. It is thus focused on a selected group of individuals, eg people returning from high-risk zones or those in previous contact with infected people. (iv) Contact tracing applications track the points of contact between infected people and others, and alert app users about potential contagion.

Table 1 illustrates which countries are implementing which technologies. Telemedicine became much more common during the pandemic, due to reduced mobility and new medical needs.[1] Several countries use flow modelling to support the work of health authorities. Heat maps show if people are abiding by social distancing measures and help predict how the virus will spread. Location tracking and contact tracing were first widely introduced in Asia, particularly in countries with advanced digital infrastructures and those which had early exposure to Covid-19, such as China, Singapore and Korea

[1] In China, telemedicine is mostly a service offered by private technology firms with the support of the public sector, including hospitals. It thus involves new private sector intermediaries in data collection and processing. In Japan, Germany and France, telemedicine is provided by expert groups, such as physicians, within a clearly defined legal framework for data and privacy protection. In Latin America, governments have taken charge of the development of virtual health apps.

(Chandran (2020)).[2] Many countries in the Americas and Europe introduced these applications in March, April or May.[3]

Overview of selected technological applications: who controls personal data? Table 1



Colours denote which entities have control over personal data. Where governments and companies both access personal data, or access by governments or companies is conditional on individual consent, the cell displays both colours. Colours within cells are arranged in the same order as in the legend. Hyperlinks in the table give information on specific applications. The online appendix gives a full list of applications; some are pending or have been discontinued (see Table 2 in the online appendix).

Sources: BIS; public data sources.

Evidence on the effectiveness of the different applications is still limited. Contact tracing promises to help isolate initial cases, reduce new infections and control the pandemic (Servick (2020), Huang et al (2020)). Yet the effectiveness of tracing apps depends on the number of users (Ferretti et al (2020)). Studies suggest that, for a contact tracing app to be effective, at least 60% of the population must use it (Hinch et al (2020), *Stanford News* (2020). To control outbreaks within three months, 80% of contacts need to be traced and isolated (Hellewell et al (2020)). Countries with a high rate of smartphone use have an advantage in this regard, but most applications have so far failed to achieve sufficient adoption.

Many applications collect, process and store personal data. In Table 1, green cells denote government control over personal data, red cells company control and blue cells individual control. Mixed colours denote shared control. Often, governments initiated the design and introduction of location tracking and contact tracing apps. In several cases, this gives them control over personal data submitted by app users, at least for a defined period of time. In other cases, private companies are collecting personal data (eg from mobile phone users). For most flow modelling applications, companies control individual data and share aggregate data with governments. In a decentralised contact tracing model (see below), data are controlled by individuals and shared with governments only with user consent.

New technological applications raise concerns about data privacy. Telemedicine apps transmit confidential medical information through new channels. Flow modelling apps often report only aggregated data to the authorities, but companies can still retain individual data. Location tracking apps often require users to report data to a health authority, as mandated by law for quarantine enforcement. In some countries, governments link locational data to people's identity.

Depending on their design, contact tracing apps can be more or less invasive. Apps can follow two models (Graph 1). In a centralised model, public authorities have access to geolocation records and

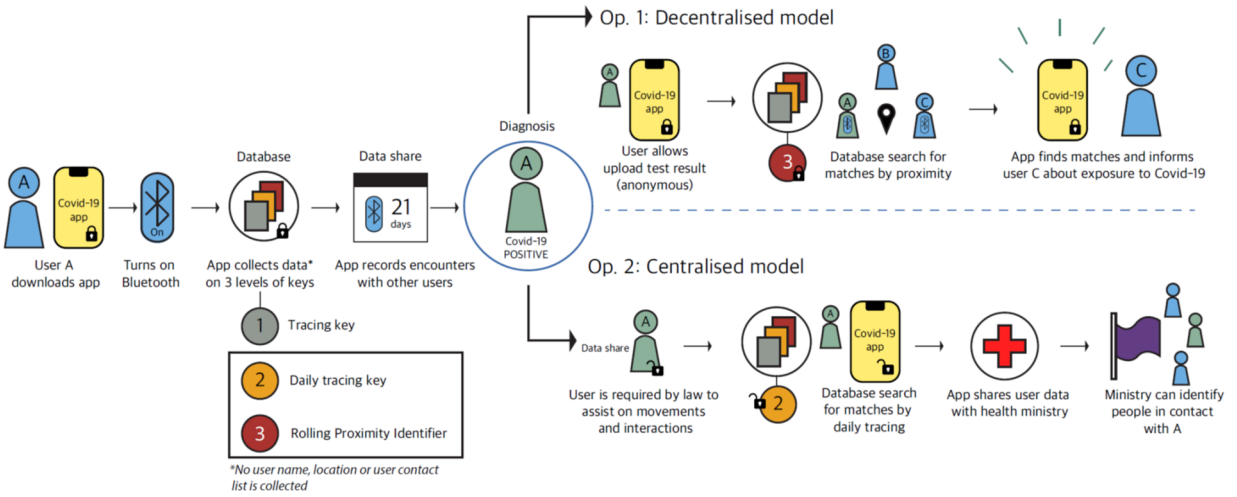
[2] Ant Financial introduced a mobile health code in mid-February in the city of its headquarters, Hangzhou. It added this health code directly to its widely used Alipay Wallet. The health code is generated when Alipay users report data on their past movement, places visited and a coronavirus diagnosis. Data are shared with the government. See Xinhua Net (2020).

[3] An earlier case of contact tracing is the FluPhone application in Cambridge, developed in 2011 to combat influenza. See Yoneki (2011). More recently, Apple and Google have announced cooperation on a Bluetooth-based contact tracing app (Apple and Google (2020)).

can contact potentially infected people directly. While this may be effective in helping to identify and isolate contacts, there may be higher risks of breaches or misuse of centrally held data. In a decentralised model, data remain on users' phones. Apps use Bluetooth to establish when individuals are close to each other and store the encrypted information locally. If a user tests positive for Covid-19, the app uploads the status to a server and other users can check whether they have been in contact with the infected person. In decentralised models, authorities cannot uncover users' identities.

Where sensitive data are collected and combined, there is the potential for data to be used for other purposes, or leaked. For example, geolocation data could reveal details of individuals' movements, habits and social contacts.[4] Even users of Bluetooth-based applications need to regularly update their phones' operating systems to patch vulnerabilities and avoid data breaches (Bay et al (2020)).

Two models for contact tracing technology — Graph 1



Source: BIS.

Societal preferences on data privacy

Successful applications need strong public support. Contact tracing apps may be particularly effective in fighting the spread of the pandemic if adopted widely. Yet wide adoption requires that apps, and legal rules for their use, reflect societal preferences on the trade-off between preserving individual privacy and sharing data to achieve the provision of public goods. While individuals may already share geolocation data with their phone or app providers, they may not want their personal data to be used for purposes that they were not previously aware of. Moreover, if users do not trust the government or companies to respect their right to privacy, they will not consent to sharing sensitive information during the pandemic.

Individuals' trust in different actors to store and analyse health data varies quite dramatically. Graph 2 (left-hand panel) plots the share of survey respondents that trust different counterparties to handle their DNA and health information (Middleton and Milne (2019)). Across all regions, around 70% of respondents are willing to share their data with their doctors and 32% trust non-profit researchers to handle their health information with due diligence. Yet less than 20% trust their government to do so, and only 15% trust private companies. Preferences differ across regions: in Europe and the Americas, people generally trust their doctors, but are not willing to share data with governments and private companies to

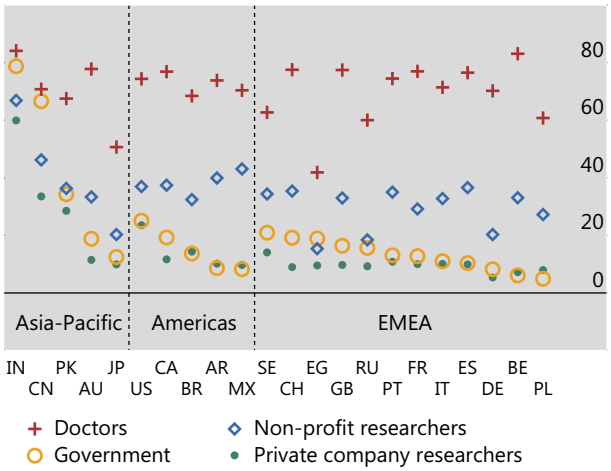
[4] Even when users willingly report these data, this may affect the privacy of other actors, such as businesses that a potentially infected person has visited (Raskar et al (2020)). Individual decisions to share data may thus have externalities (Bergemann and Bonatti (2019)).

a similar extent. In Asia-Pacific, trust is on average higher, which could reflect the fact that recent experiences with other epidemics may have increased the willingness to share data when public health is in danger.[5] Respondents in India and China report the highest values in the sample.

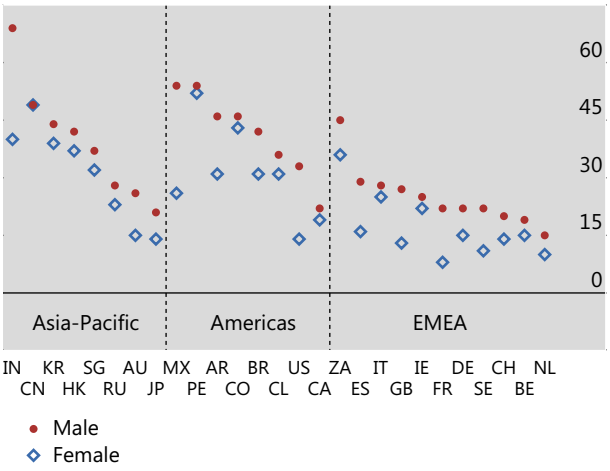
Views on privacy of health and financial data differ across and within societies

Percentage of respondents — Graph 2

Trust in doctors to handle DNA and health information is higher than trust in governments and private companies[1]



Men are more willing to share financial data than women[2]



EMEA = Europe, Middle East and Africa.

[1] Based on a global meta-analysis for 22 countries. Respondents were asked if they agree with the statement: "I trust (a) my own doctor, (b) any doctor in my country, (c) a non-profit researcher in my country, (d) a company researcher in my country or (e) my government with my DNA and health information". We omit category (b). [2] Based on a survey of 27,000 individuals across 27 countries. The exact question reads: "I would be comfortable with my main bank securely sharing my financial data with other organisations if it meant that I received better offers from other financial intermediaries". For Belgium, the figure covers Belgium and Luxembourg.

Sources: Middleton and Milne (2019); EY (2019); Chen et al (2020).

An additional dimension is the heterogeneity *within* societies. Although not directly comparable with medical data, recent work that analyses individuals' willingness to share financial data with fintechs provides valuable insights. The willingness to share financial data is lower in countries and for individuals with higher incomes (EY (2019), Chen et al (2020)). Further, in all regions, men are more willing to share their financial data with other organisations than women are (Graph 2, right-hand panel). Similarly, younger generations are in general less concerned about privacy than older generations (Bain & Company and Research Now (2017)). In the case of Covid-19, these differences matter greatly: men are more at risk than women, and seniors are more at risk than younger individuals. If the adoption of contact tracing apps differs significantly across demographic groups, their usefulness may be limited.

These differences across regions and demographic groups could explain why countries have taken different approaches to the use of mobile apps in the fight against the global pandemic. A number of countries have revised their legal frameworks to govern medical information-sharing. As regards contract tracing apps, Asian countries, such as China, Korea and Singapore, favour the centralised model. By contrast, many western countries opt for decentralised models (Apple and Google (2020)).

[5] For example, Koreans show high support for the government publishing individuals' movements (Zastrow (2020)). Notably, the country also revised the Infectious Disease Control and Prevention Act after the Middle East respiratory syndrome in 2015 to allow data collection and sharing in the event of infectious diseases endangering public health.

Implications for future data control and policy options

Actions taken during the pandemic may have implications for control over data going forward. If public authorities and their private partners successfully use technology-based applications to fight the pandemic while at the same time managing the shared data responsibly, they can build strong public support. However, while it takes a long time to build trust, it can be easily lost. Should the data management during the pandemic be experienced as negative, this could deter future compliance also outside the realm of public health crises. For example, distrust in companies or governments could result in lower adoption of methods of digital payments or financial services, hindering the advancement of financial inclusion in emerging market and developing economies.

Transparent public policies can help to tailor applications to societal preferences and to build trust. A number of Asian countries have begun to adapt legal and policy frameworks to ensure proper use of data, and communicated that measures will be temporary.[6] In Europe, a number of data protection authorities have issued opinions on specific applications to protect the public interest and promote trust, and some have been actively consulted on the design of applications.[7] Adequate governance and oversight of applications can also build trust and increase accountability, including oversight committees with public involvement and auditable algorithms (Ferretti et al (2020)). Setting up transparent rules and communicating clearly to the public are key to achieving a positive outcome.

The use of personal data in finance shows that there are several, potentially complementary, approaches to address the broader policy concerns. Medical and financial data are both sensitive, and are often kept by a trusted custodian – healthcare providers and financial institutions. In finance, a range of policies have been used to address data privacy concerns (BIS (2019)). One approach consists in restricting the processing of user data. For example, recent data protection laws (eg in the European Union, Brazil, Japan, Singapore and California) regulate data collection and use for personally identifiable information. The challenge with these laws is how to balance the protection of privacy and diligent use of data. A second approach is to give consumers greater control over their personal data. Customers could decide to which firms to grant access to data, and thereby foster competition and increase welfare (Jones and Tonetti (2020)). Recent open banking initiatives (eg in the European Union, Australia and Mexico) are examples of concrete policy actions in this direction. While there are also strong differences between health and financial data, a common factor is that policy approaches will vary in line with the preferences of the public in each jurisdiction.

Going forward, there may be a need to differentiate between data use during a public health crisis and during normal times. The current pandemic offers a unique opportunity to use digital technologies to promote the public good. Yet care needs to be taken to ensure that the use of data respects preferences of the public in each jurisdiction. If governments or companies handle shared data responsibly and fight Covid-19 successfully, this could greatly enhance the trust in technology, as well as in governments and companies, for years to come.

[6] In Chinese Taipei, the authorities have announced that a geofencing tracking system would be discontinued after the pandemic passes. The TraceTogether app developed by the Singapore government only stores data in an encrypted form using "cryptographically generated temporary IDs". China has issued three new policies governing the use of information technology in the prevention and control of coronavirus and the development of internet-based medical consultations. The new policies also stress the need to safeguard data security and privacy. In Israel, the government had used location tracking to map individuals' movements and infection patterns; on 22 April, a parliamentary oversight committee suspended these measures.

[7] For instance, the UK Information Commissioners Office (ICO) has issued a statement on flow modelling with mobile phone data, and an opinion on the Apple-Google initiative. In France, the Commission nationale de l'informatique et des libertés (CNIL) has issued an opinion on the "StopCovid" mobile application project.

References

Apple and Google (2020): "Apple and Google partner on COVID-19 contact tracing technology", 10 April.

Bain & Company and Research Now (2020): "Evolving the customer experience in banking".

Bank for International Settlements (BIS) (2019): "Big tech in finance: opportunities and risks", *Annual Economic Report 2019*, Chapter III, June.

Bay, J, J Kek, A Tan, C Hau, Y Lai, J Tan and A Tang (2020): "BlueTrace: a privacy-preserving protocol for community-driven contact tracing across borders", *BlueTrace Protocol White Paper*, Government Technology Agency of Singapore.

Bergemann, D and A Bonatti (2019): "The economics of social data: an introduction", *Cowles Foundation Discussion Papers*, no 2171, Yale University, March

Chandran, R (2020): "Here's how Asia is using tech to tackle COVID-19", World Economic Forum, 18 March.

Chen S, S Doerr, J Frost and L Gambacorta (2020): "Data versus privacy: the role of gender and social norms", mimeo.

The Economist (2020): "Countries are using apps and data networks to keep tabs on the pandemic", Briefing, 26 March.

Ernst & Young (EY) (2019): "FinTech Adoption Index", September.

Ferretti, L, C Wymant, M Kendall, L Zhao, A Nurtay, L Abeler-Dörner, M Parker, D Bonsall and C Fraser (2020): "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing", *Science*, 31 March.

Hellewell, J, S Abbott, A Gimma, N Bosse, C Jarvis, T Russell, J Munday, A Kucharski, J Edmunds, S Funk and R Eggot (2020): "Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts", *The Lancet Global Health*, vol 8, no 4, pp 488-96.

Hinch R, W Probert, A Nurtay, M Kendall, C Wymant, M Hall, K Lythgoe, A Bulas Cruz, L Zhao, A Stewart, L Ferretti, M Parker, A Meroueh, B Mathias, S Stevenson, D Montero, J Warren, N Mather, A Finkelstein, L Abeler-Dörner, D Bonsall and C Fraser (2020): "Effective configurations of a digital contact tracing", mimeo.

Huang, Y, M Sun and Y Sui (2020): "How digital contact tracing slowed Covid-19 in East Asia", *Harvard Business Review*, 15 April.

Jones, C and C Tonetti (2020): "Nonrivalry and the economics of data", Stanford University, mimeo.

Middleton, A and R Milne (2019): "Your DNA, your say", invited plenary presentation at the Global Alliance for Genomics and Health 7th Plenary, Boston, 22 October.

Raskar, R, I Schunemann, R Barbar, K Vilcans, J Gray, P Vepakomma, S Kapa, A Nuzzo, R Gupta, A Berke, D Greenwood, C Keegan, S Kanaparti, R Beaudry, D Stansbury, B Botero Arcila, R Kanaparti, V Pamplona, F Benedetti, A Clough, R Das, K Jain, K Louisy, G Nadeau, S Penrod, Y Rajaee, A Singh, G Storm and J Werner (2020): "Apps gone rogue: maintaining personal privacy in an epidemic", Whitepaper, PrivateKit: Massachusetts Institute of Technology.

Servick, K (2020): "Cellphone tracking could help stem the spread of coronavirus. is privacy the price?", *Science*, March.

Stanford News (2020): "Stanford researchers help develop privacy-focused coronavirus alert app", 9 April.

Xinhua Net (2020): "East China's Hangzhou adopts QR codes for medical services", 21 February.

Yoneki, E (2011): "FluPhone study: virtual disease spread using Haggle", University of Cambridge.

Zastrow, M (2020): "South Korea is reporting intimate details of COVID-19 cases: has it helped?", *Nature*.

Previous issues in this series

No 16 15 May 2020	Covid-19 and regional employment in Europe	Sebastian Doerr and Leonardo Gambacorta
No 15 13 May 2020	US dollar funding markets during the Covid-19 crisis – the international dimension	Egemen Eren, Andreas Schrimpf and Vladyslav Sushko
No 14 12 May 2020	US dollar funding markets during the Covid-19 crisis – the money market fund turmoil	Egemen Eren, Andreas Schrimpf and Vladyslav Sushko
No 13 11 May 2020	The CCP-bank nexus in the time of Covid-19	Wenqian Huang and Előd Takáts
No 12 7 May 2020	Effects of Covid-19 on the banking sector: the market's assessment	Iñaki Aldasoro, Ingo Fender, Bryan Hardy and Nikola Tarashev
No 11 5 May 2020	Releasing bank buffers to cushion the crisis – a quantitative assessment	Ulf Lewrick, Christian Schmieder, Jhuvesh Sobrun and Előd Takáts
No 10 28 April 2020	Covid-19 and corporate sector liquidity	Ryan Banerjee, Anamaria Illes, Enisse Kharroubi and José María Serena
No 9 24 April 2020	Buffering Covid-19 losses – the role of prudential policy	Mathias Drehmann, Marc Farag, Nikola Tarashev and Kostas Tsatsaronis
No 8 21 April 2020	Identifying regions at risk with Google Trends: the impact of Covid-19 on US labour markets	Sebastian Doerr and Leonardo Gambacorta
No 7 17 April 2020	Macroeconomic effects of Covid-19: an early review	Frederic Boissay and Phurichai Rungcharoenkitkul
No 6 14 April 2020	The recent distress in corporate bond markets: cues from ETFs	Sirio Aramonte and Fernando Avalos
No 5 7 April 2020	Emerging market economy exchange rates and local currency bond markets amid the Covid-19 pandemic	Boris Hofmann, Ilhyock Shim and Hyun Song Shin
No 4 6 April 2020	The macroeconomic spillover effects of the pandemic on the global economy	Emanuel Kohlscheen, Benoît Mojon and Daniel Rees
No 3 3 April 2020	Covid-19, cash, and the future of payments	Raphael Auer, Giulio Cornelli and Jon Frost
No 2 2 April 2020	Leverage and margin spirals in fixed income markets during the Covid-19 crisis	Andreas Schrimpf, Hyun Song Shin and Vladyslav Sushko

All issues are available on our website www.bis.org.