Data, the Future of Financial Information

A SIX White Paper

Foreword

The SIX Board of Directors has mandated the business unit Innovation & Digital (I&D) to develop future scenarios to increase SIX' future readiness by sharpening its understanding of the many developments we are currently witnessing from new technologies, to political shifts, social changes, and business model innovations. White papers are one of the by-products of I&D's efforts in developing such scenarios.

The publication of this white paper serves several goals: to underscore the cultural shift going on at SIX, to elicit feedback from a broader audience, to serve as a basis for starting conversations with various external stakeholders, to suggest possible avenues for joint innovation with start-ups and established players, and to communicate to prospective employees the types of innovation initiatives/projects that could be ongoing at SIX in the years to come.

We understand white papers as a stepping stone in a never-ending journey of better understanding possible futures. We therefore inherently understand it as a work in progress, rather than an end-product, capturing our current views but ready to be updated as new information comes along.

The present white paper is the result of a joint effort between the Financial Information and Innovation & Digital business units of SIX. We thank the authors and the many contributors, internal and external.

We hope you will enjoy the reading, and look forward to constructive discussions.

Robert Jeanbart
Head Financial Information
SIX

Daniel Dahinden
Head Innovation & Digital
SIX

Dr. Alexander Roitinger
Head Strategic Transformation
SIX

Dr. Gregor A. Kalberer
Head Innovation Exploration
SIX

Executive Summary

Data, the Future of Financial Information

Data is considered the world's most valuable resource. How will data change investment behaviors? Who owns the data? What infrastructure is needed? The SIX white paper on «Data, the Future of Financial Information» provides guidance on these questions, and many more.

"90% of all data in the world was created in the prior two years." This quote appears prominently in almost every presentation. However, what isn't highlighted is the fact that this finding from a Norwegian think tank is already six years old (2013).[1] Global data volume has since continued to grow exponentially. "Data Peak" seems far from having been reached. The term "peak" originates from the extractive industry — The Economist already described data in a cover story in 2017 as the new oil, even noting that data had become the "world's most valuable resource".[2]

This white paper examines the spectacular development of this new asset. The central questions are: On what data basis will investment decisions be made in the future? In what form will data exist and be used? What infrastructure will underlie it? These issues are discussed and analyzed in the context of the rapid development and spread of digital assets, data sovereignty shifting to data subject, increased demands for the protection of privacy, increasing consideration of sustainability and social impact, technological advances in privacy-preserving systems, fake data, powerful AI systems, increasing cybercrime, and a general decentralization of data. The report presents the future in five scenarios, sorted by probability of occurrence. The time horizon is 10+ years.

Data is the future of financial information — that may come as little surprise. But this report shows that there will be profound changes surrounding this constant. The conclusion of the authors: "Besides the centrality of data, it looks as if nothing will look like the past."

The following summarizes the five scenarios for the year 2030.

Financial information describes all information that is used by financial entities or market participants for investment decision-making.

Most Likely Scenario

Freedom to Generate, Right to Control, and Ability to Monetize

People have greater freedom, rights, and ability in their capacity as asset owners, data owners, and investors.

Anyone can transform their assets into investable assets by creating rights to them *(digitally tradable rights to assets): The number of investable assets has exploded* and ranges from seats at a restaurant, usage rights to a parking spot, rights to a share of a student's future income, rights to use a room in an apartment, and usage rights to your data. New types of assets may necessitate new types of data for valuation.

Digitalization and automation have simplified the process of defining/describing digital and non-digital assets, and of creating rights to these assets — thus reducing monetary and time costs of making an asset investable. *Digital platforms* have also permitted reaching a global market, thus rendering it substantially more attractive for asset owners to make their assets investable.

Anyone can control usage of their data and create rights to it *(digitally tradable rights to data). Data subjects have been granted sovereignty* over their data. Governments have taken substantial action to enforce property rights and competition in the digital sphere by reducing user lock-ins, unbundling services, breaking up vertical supply/value chains, requiring data mobility, and allocating rights to data. *The fraction of data that is accessible for processing by third parties has exploded.* Users of digital services can prevent service providers from processing their data and can provide third parties with access to their data — data which may not have been accessible to third parties before, as service providers may have kept it for themselves. The *crowd* has become an important data source.

1 Eric Luellen, 2017, Big Data will First Slow, Not Accelerate, Discovery, Medium (17 January 2017).

2 Economist, 2017, The world's most valuable resource: Data and the new rules of competition (6 May 2017) and Economist, 2017, Regulating the internet giants: The world's most valuable resource is no longer oil, but data (6 May 2017).

Explosion in volume and type of digital data. Everything we do produces digital data. Social interactions take place in the virtual sphere (chat, VR). Real world experiences are augmented with a digital layer (voice interfaces and/or AR). Everyday objects let appliances know how to interact with them (e.g., clothes tell washing machines how to treat them). This has led to an explosion in *theme-related information.* There is data allowing investors to evaluate investable assets in any dimension, helping them to better tailor their investments to their preferences (e.g., sustainability, ESG, gender equality). *The majority of digital data is hidden/private (e.g., encrypted, stored at the edge).* Data owners and producers have placed high data privacy demands on service providers. Data privacy calls for the raw data to be decentrally stored where it is produced, always encrypted, and that the raw data never moves. *Secure and privacy-preserving systems are a foundational technology* of FI infrastructure. They give data owners the ability to monetize their data while still respecting their data privacy. These systems have increased data owners' willingness to even share access to their (sensitive) data, and have therewith further increased the data that is accessible for processing by third parties. *A large fraction of FI data sources stored decentrally.* The explosion in digital data makes central storage (i.e., duplication) at data distribution intermediaries or investors too costly and arguably infeasible.

Anyone can invest in perfect alignment with what matters to them *(investment tailoring)* due to the broad availability of theme-related information. Driven by the explosion in new (accessible) digital data, *alternative data* has established itself alongside traditional financial information as key input for investment decision. As new types of assets become investable, further data types and sources may become relevant inputs for investment decision-making. *Social impact and sustainability considerations* play an increasingly important role in investment decisions. Investors continue to take some decisions themselves, but *delegate most of their investment decisions* to professional asset managers (e.g., funds, collective or individual mandates). Tailored robo-funds, where algorithms automatically take investment decisions, have increased in popularity.

Medium-Likelihood Scenario

Middle- and back-office consolidation in finance

Financial services providers outsource virtually all their middle- and back-office activities to utilities in order to benefit from economies of scale on non- differentiating activities and to access rare skills/capabilities.

Medium-Low-Likelihood Scenarios

Extreme Consolidation in FI Infrastructure

Digitalization has turned most markets into *winner-takes-it-all.* The most likely path to this scenario is *lack of government action aimed at enforcing competition* in the digital sphere by reducing user lock-ins, unbundling services, breaking up vertical supply/value chains, and restricting exclusive access/usage of data. *All platforms in the FI space have global scale.* There is a single global digital marketplace in the FI-services space and a single global data-distribution and data-access intermediary. *(Niche) FI-service providers around these global platforms also have global scale wherever scale provides an advantage.*

Extreme Protectionism

Services/products face *import and export* barriers and *raw data is restricted from leaving the country (data protectionism).* Anti-globalization sentiments, national security concerns, and weaponization of economic tools to further national interests have all been on the rise. Governments want a *locally operated FI infrastructure* to ensure a functioning local market that efficiently allocates capital. Privacy-preserving systems are necessary to allow cross-border access to data without the raw data ever leaving the country.

Low-Likelihood Scenarios

Crypto-Assets Everywhere

The *world runs on permissionless distributed ledgers.* Crypto-assets are the dominant form of digital assets and of investable assets. Decentralized crypto-currencies have replaced central-bank-issued currency as the dominant medium of exchange. Commercial digital operations take the form of open-source code stored and executed on top of these permissionless distributed ledgers, known as 'decentralized applications' (DApps).

Kurzfassung

Daten, die Zukunft von Finanzinformationen

Daten werden auch als der wertvollste Rohstoff der Welt bezeichnet. Wie werden sie das Anlegen in Zukunft verändern? Wem gehören sie? Welche Infrastruktur braucht es dazu? Einordnung bietet das neue SIX White Paper zu «Data, the Future of Financial Information».

«90 Prozent der Daten in der Welt wurden in den letzten zwei Jahren kreiert». Dieses Zitat fehlt bei kaum einer Präsentation über die Datenindustrie. Unerwähnt bleibt jedoch meist, dass diese Erkenntnis eines norwegischen Think-Tanks bereits sechs Jahre alt ist (2013).[3] Seither hat die globale Datenmenge nochmals exponentiell zugenommen und der «Data Peak» scheint noch lange nicht erreicht. Der Begriff «Peak» stammt aus der Rohstoffindustrie und tatsächlich bezeichnete The Economist bereits 2017 in einer Titelgeschichte Daten als das neue Erdöl, sie seien heute gar der «wertvollste Rohstoff der Welt».[4]

Dieses White Paper untersucht die spektakuläre Entwicklung dieses neuen Vermögenswerts. Die zentralen Fragen lauten: Auf welcher Datengrundlage wird man künftig Anlageentscheide treffen? In welcher Form werden Daten überhaupt vorhanden sein und eingesetzt? Und welche Infrastruktur steht dahinter? Diskutiert und analysiert werden diese Fragen vor dem Hintergrund der rasanten Entwicklung und Verbreitung digitaler Assets, der Rückgewinnung der Hoheitsgewalt der Menschen über ihre einen Daten, einer gestiegenen Nachfrage nach dem Schutz der Privatsphäre und besseren technischen Möglichkeiten, diesen zu garantieren, der zunehmenden Bedeutung von Nachhaltigkeit und vom sozialem Impact, Fake Data, leistungsstarken KI-Systemen, einer zunehmenden Cyberkriminalität und einer generellen Dezentralisierung der Daten. Der Report präsentiert die Zukunft in fünf Szenarien, geordnet nach Eintrittswahrscheinlichkeit. Dabei wird von einem Zeithorizont von 10 Jahren und mehr ausgegangen.

Daten sind die Zukunft der Finanzinformationen – das mag wenig überraschen. Doch dieser Report zeigt, dass um diese Konstante, tiefgreifende Umwälzungen stattfinden werden. Die Schlussfolgerung der Autoren: «Ausser der enormen Bedeutung der Daten, scheint nichts mehr so zu sein wie in der Vergangenheit».

Im Folgenden werden die fünf Szenarien zusammengefasst für das Jahr 2030.

Unter Finanzinformationen werden in diesem Report alle Informationen subsumiert, die von Finanzunternehmen oder anderen Marktteilnehmern für Investitionsentscheidungen verwendet werden.

Das wahrscheinlichste Szenario

Freiheit zur Erzeugung, Recht auf Kontrolle und Möglichkeit zur Monetarisierung

Die Menschen haben mehr Freiheiten, Rechte und Möglichkeiten, sowohl als Asset- oder Daten-Besitzer wie auch als Investoren.

Jeder kann seine Vermögenswerte investierbar machen durch die Schaffung von *digital handelbaren Rechten an den Assets. Entsprechend ist die Anzahl investierbaren Vermögenswerte explodiert,* das Spektrum reicht von Sitzplätzen in einem Restaurant, zu Nutzungsrechten an einem Parkplatz, zu Rechten auf einen Anteil am zukünftigen Einkommen eines Studierenden, zu den Nutzungsrechten eines Zimmers. Neue Anlagemöglichkeiten erfordern neue Daten für deren Bewertung.

Die *Digitalisierung und Automatisierung* haben den Prozess der Definition/Beschreibung digitaler und nicht-digitaler Assets und die Schaffung von Rechten an diesen Assets vereinfacht — und damit den Geld- und Zeitaufwand reduziert, um einen Asset «investitionsfähig» zu machen. *Digitale Plattformen* eröffnen den Zugang zu einem globalen Markt, was es wesentlich attraktiver macht, Vermögenswerte investierbar zu machen.

Jede Person *hat die Hoheitsgewalt über seine eigenen Daten,* kann die Nutzung kontrollieren und *digitale Rechte dafür kreieren.* Regierungen haben umfangreiche Massnahmen ergriffen, um Eigentumsrechte und mehr Wettbewerb im digitalen Bereich durchzusetzen, sie haben die strikte Nutzerbindung (Lock-in) erschwert, Dienste entbündelt, vertikale Liefer- und Wertschöpfungsketten aufgebrochen, die Datenmobilität gefördert und die Rechte an den

3 Eric Luellen, 2017, Big Data will First Slow, Not Accelerate, Discovery, Medium (17 January 2017).

4 Economist, 2017, The world's most valuable resource: Data and the new rules of competition (6 May 2017) und Economist, 2017, Regulating the internet giants: The world's most valuable resource is no longer oil, but data (6 May 2017).

eigenen Daten den Benutzern zurückgegeben. *Der Anteil der Daten, der für Dritte zugänglich ist, hat stark zugenommen.* Die Nutzer können Dienstleister an der Verwendung ihrer Daten hindern und dafür Dritten Zugang gewähren – zu Daten, die ihnen zuvor möglicherweise nicht zugänglich waren, da die originären Dienstleister sie für sich behielten. Die Masse (*Crowd*) ist zu einer wichtigen Datenquelle geworden.

Explosion des Volumens und der Vielfalt von digitalen Daten. Alles, was wir tun, produziert digitale Daten. Soziale Interaktionen finden im virtuellen Raum statt (Chat, VR). Die Erfahrungen aus der Praxis werden durch eine digitale Ebene (Sprachschnittstellen und/oder AR) ergänzt. Alltagsgegenstände teilen Geräten mit, wie sie mit ihnen interagieren sollen (die Kleidung sagt zum Beispiel den Waschmaschinen, wie sie sie behandeln sollen). Dies hat zu einer starken Zunahme an *themenbezogenen Informationen* geführt. Es gibt Daten, die es den Anlegern ermöglichen, investierbare Vermögenswerte in jeder Dimension zu bewerten, um ihnen zu helfen, ihre Investitionen besser auf ihre Präferenzen abzustimmen (z.B. Nachhaltigkeit, ESG, Gleichstellung). *Die Mehrheit der digitalen Daten ist versteckt/privat (z.B. verschlüsselt, dezentral gehalten).* Datenbesitzer und -produzenten stellen hohe Datenschutzanforderungen an Dienstleister. Der Datenschutz erfordert, dass die Rohdaten dort gespeichert werden, wo sie erzeugt werden, immer verschlüsselt sind, und dass die Rohdaten nie geteilt werden. *Sichere und die Privatsphäre schützende Systeme sind eine grundlegender Teil* der FI-Infrastruktur. Sie geben den Datenbesitzern die Möglichkeit, ihre Daten unter Wahrung des Datenschutzes zu monetarisieren. Diese Systeme haben die Bereitschaft der Datenbesitzer erhöht, den Zugriff auf ihre (sensiblen) Daten zu teilen, und damit die Datenmenge erhöht, die für die Verarbeitung durch Dritte zugänglich ist. *Ein grosser Teil der FI-Datenquellen wird dezentral gespeichert.* Die grosse Zunahme der digitalen Daten macht die zentrale Speicherung (d.h. Duplizierung) bei Datenverteilern oder Investoren zu kostspielig und nicht durchführbar.

Durch die breite Verfügbarkeit von themenbezogenen Informationen kann jeder in perfekter Abstimmung mit dem, was ihm wichtig ist (*Investment Tailoring*) investieren. Angetrieben von der Explosion neuer (zugänglicher) digitaler Daten haben sich *alternative Daten* neben traditionellen Finanzinformationen als wichtige Entscheidungsgrundlage für Investitionen etabliert. Wenn neue Arten von Vermögenswerten investierbar werden, können weitere Datentypen und Quellen zu relevanten Inputs für die Investitionsentscheidung werden. *Soziale Auswirkungen und Nachhaltigkeitsaspekte* spielen bei Investitionsentscheidungen eine immer wichtigere Rolle. Die Anleger entscheiden weiterhin selber, doch sie *delegieren die meisten ihrer Anlageentscheidungen* an professionelle Vermögensverwalter (z.B. Fonds, kollektive oder individuelle Mandate). Massgeschneiderte Robo-Fonds, bei denen Algorithmen automatisch Investitionsentscheidungen treffen, erfreuen sich zunehmender Beliebtheit.

Szenario mit mittlerer Eintrittswahrscheinlichkeit

Mittel- und Backoffice Konsolidierung im Finanzbereich

Finanzdienstleister lagern praktisch alle ihre Mittel- und Backoffice-Tätigkeiten an Versorgungsunternehmen aus, um von Grössenvorteilen bei nicht differenzierenden Tätigkeiten zu profitieren und auf seltene Fähigkeiten/Kapazitäten zuzugreifen.

Szenarien mit mittlerer und niedriger Eintrittswahrscheinlichkeit

Extreme Konsolidierung in der FI-Infrastruktur

Die Digitalisierung hat die meisten Märkte in *winner-takes-it-all* Situationen verwandelt. Der wahrscheinlichste Weg zu diesem Szenario ist *das Fehlen staatlicher Massnahmen zur Durchsetzung des Wettbewerbs* im digitalen Bereich. Es gibt fast keine Reduzierung der Nutzerbindung (Lock-in), Entbündelung von Diensten, kein Aufbrechen vertikaler Liefer- und Wertschöpfungsketten und keine Beschränkung des exklusiven Zugangs/Nutzens von Daten. *Alle Plattformen im FI-Bereich haben einen globalen Massstab.* Es gibt einen einheitlichen globalen digitalen Marktplatz im Bereich der FI-Dienste und einen einzigen Zwischenhändler für globalen Datenverteilung und Datenzugriff. *(Nischen-)FI-Dienstleister rund um diese globalen Plattformen haben auch eine globale Ausrichtung, wo immer die Grösse einen Vorteil bietet.*

Extremer Protektionismus

Dienstleistungen/Produkte haben *Import- und Exportschranken* und *Rohdaten dürfen das Land nicht verlassen (Datenschutz).* Die Stimmung gegen die Globalisierung, die Sorgen um die nationale Sicherheit und der Einsatz von wirtschaftlichen Mitteln zur Förderung nationaler Interessen haben zugenommen. Regierungen wollen

eine *lokal betriebene FI-Infrastruktur,* um einen funktionierenden lokalen Markt zu gewährleisten, der effizient Kapital bereitstellt. Systeme, welche den Datenschutz sicherstellen, sind notwendig, um den grenzüberschreitenden Zugang zu Daten zu ermöglichen, ohne dass die Rohdaten das Land verlassen.

Szenario mit geringer Eintrittswahrscheinlichkeit

Krypto-Assets sind überall

Die *Welt läuft auf permissionless distributed ledgers.* Krypto-Assets sind die dominante Form der digitalen Assets und der investierbaren Assets. Dezentrale Krypto-Währungen haben die von der Zentralbank ausgegebene Währung als dominantes Tauschmittel abgelöst. Kommerzielle digitale Transaktionen erfolgen in Form von Open-Source-Code, der auf diesen permissionless distributed ledgers gespeichert und ausgeführt wird, auf so genannten «dezentralen Anwendungen» (DApps).

Table of Contents

1 Introduction

How will financial information change? What developments are driving these changes? What does it mean for the financial information infrastructure?

What data amounts to relevant inputs for investment decision-making, what form it takes, how it is used, and what its infrastructure looks like, all look set to change dramatically over the next years.

The number of things producing digital data increases incessantly, while the volume of data seems to be growing exponentially. From your smartphone, to your streaming choices, to your shopping list, to the pictures your take, everything we do produces data in one way or another. And this is not counting all the sensors and cameras from third parties tracking everything and everyone.

Surveys suggest that investors are increasingly taking social-impact and sustainability considerations into account in their investment decisions.

Not a day seems to go by without news of yet another digital data breach or incident. From hospitals sharing the data of up to 50 million patients without informing them (Ascension with Google, 2018), to payment schemes selling their purchase data (Mastercard with Google, 2018), and biotech companies selling their clients' genetic data (23andMe with GlaxoSmithKline, 2018). From hackers stealing the social security numbers of over 200 million Americans (Equifax breach 2017, Anthem breach 2015), and the financial data of over 100 million bank clients (Capital One, 2019), to technology companies enabling their employees to sift through their clients' data (Uber, 2014), and government spies working at technology companies to monitor and track dissenters (LinkedIn, 2019).

Digital platforms seem to be popping up in almost every industry, displacing existing players, and taking over the orchestration between the various participants — from apartment renting (AirBnB), to ride hailing (Uber), shopping (Amazon, eBay), capital raising (Loanboox, Seedrs), trading financial products (SIX Exchange), and taking out a mortgage (Atrium, Kreditfabrik). At the same time, digitalization keeps unbundling services and vertical supply chains into their constituent elements, giving customers more choice and better tailoring. We can try a pair of shoes in a shop, compare prices online, and buy them at the cheapest online retailer. We can ask our trusted financial advisor whether we can afford the house with the nice garden, and then take out the mortgage via an online aggregation platform.

Governments in Western countries with liberal traditions are passing laws and regulations that grant data subjects increasing sovereignty over the data they produce, through rights to restrict data usage and rights to share their data with third parties ('data mobility'). At the same time, governments increasingly make their own data publicly available for free and in machine readable form, and are requiring some private companies to do the same (e.g., trading venues' trading data). Elsewhere, governments are increasingly weaponizing economic tools, prohibiting private companies from servicing certain foreign countries or doing business with certain foreign companies. Protectionist sentiments are rising around the world, and trade barriers are at times erected in the form of tariffs and market-access restrictions.

The pressure on financial institutions to reduce operational costs remains unabated. Calls for outsourcing and standardizing non-differentiating activities, in order to increase efficiency, continue.

Almost every industry has been touted as being on the cusp of seeing the big tech companies, from Amazon to Facebook, enter and disrupt incumbent players. Artificial intelligence, machine learning, and robotics offer the promise of doing everything humans can, and perhaps even more — such as freeing humans from tedious repetitive work, driving our cars, writing our good night stories, and being the ideal conversation partner. Crypto-assets, such as Bitcoin, are rising and falling in value, and have repeatedly been pronounced dead, but are still here.

Even though the future of financial information is, perhaps unsurprisingly, data, there is a lot more to it than meets the eye. The type and volume of data is set to change dramatically. Beneath the surface, a lot is changing too: from new investable assets, to shifting preferences and behaviors of both data owners and investors, to the spread of digital platforms and marketplaces, to increased sophistication of tampered/fake data, advances in AI and decentralized systems, ubiquity of data breaches, new laws regulating data, and new competitors.

Besides the centrality of data, it looks as if nothing will look like the past.

This white paper **presents several possible futures for the financial information space.**

Our goal is to **help strategic decision-makers in setting the strategic direction**. We hope it will help in identifying potential market opportunities, in spotting one of the next big waves,[5] in better understanding new technologies,[6] in getting a sense of the implications of possible technological and societal developments,[7] in creating awareness for implicitly-held assumptions and beliefs underlying current strategic directions,[8] in recognizing strategic risks, in providing a mental framework for making sense of the never-ending feed of news, and/or in the communication of their strategies.

Our findings are synthesized in the form of future scenarios because we view scenarios as an optimal means of communication.[9] Our time **horizon is 10+ years**.

Financial information describes all information that is used by financial entities or market participants for investment decision-making.[10]

When thinking about the future of 'something', it is dangerous to think in terms of today's structures, concepts, and vocabulary because we risk inadvertently biasing our thinking to 'what is'. Instead, ***we should start by defining this something at an abstract level***. More specifically, we believe that we should try to describe this something ***in terms of the value it creates (or the 'jobs it is hired to do') at an abstract level***.[11]

We believe that **financial-information infrastructure[12] essentially creates value for people and society in three distinct ways:[13]**

- *by making assets findable & describing them*
- *by helping monetize data*
- *by delivering issuing & investment decision support*

This introduction first describes the method we used to arrive at our scenarios. It then shows the various developments we considered, and provides a brief overview of our different scenarios. It ends with a discussion of some of the strategic implications. **The introduction contains all our statements about the future — the rest of the document offers interested readers the possibility to dive deeper into the different topics**.

The remainder of this white paper is then organized as follows. Chapter 2 describes the scenarios we view as most relevant. And Chapter 3 provides some useful definitions and concepts.

---

5 Our SIX, 2019, Future of the Securities Value Chain (January 2019), for example, points out that there will likely be an explosion in digital assets and that existing securities-infrastructure providers (e.g., Exchanges, CCPs, custodians, CSDs) can leverage their capabilities by expanding from traditional financial securities (e.g., equities, bonds, structured products) to digital assets more generally.

6 Our SIX, 2019, Future of the Securities Value Chain (January 2019) clarifies that permissionless distributed ledgers (i.e., the crypto-assets world) describe a completely different future than the one(s) in which central or permissioned-distributed ledgers are dominant.

7 The SFTI, 2019, Future of Financial Institutions, for instance, discusses in-depth the consequences of increasing (possibly mandated by regulators) interoperability and unbundling on business models and competitive advantage.

8 Our SIX, 2019, Future of the Securities Value Chain (January 2019), for example, points out in its second-most likely scenario that 'listing at an Exchange' may cease being perceived by market participants as an indicator for the quality of the financial product, leading to the disappearance of 'listing'. It suggests that the explosion in initial coin offerings (ICOs) of the mid-2010s may have been driven by a shifting preference of issuers and investors towards non-listed financial products —rather than driven by a preference for ICOs' underlying technology (permissionless distributed ledgers), which tends to be the popular explanation for that development.

9 See Section 'Method' on page 14 for a description of how we arrive at our scenarios.

10 For a more detailed definition, see Chapter 3.

11 This approach has been referred to as 'first principles design thinking'; see e.g. Brett King, 2018, Bank 4.0: Banking Everywhere, Never at a Bank (Marshall Cavendish: Tarrytown, NY), pages 23-32, noting that this kind of thinking is characteristic of the likes of Carl Benz, Steve Jobs, or Elon Musk.
This approach is identical to the one advocated by IDEO for thinking about the future of something. See e.g., Joe Gerber, 2019, Prototype the Future of Your Business With This 4-Step Design Exercise, IDEO Journal (18 September 2019).

12 We use 'FI infrastructure' to point out its role as a key, not always perceptible, fundament for the functioning of capital markets.

13 There undoubtedly exists an even higher level of abstraction that captures financial institutions' value propositions. We, however, believe that our categories strike a nice balance by opening our thinking while providing enough structure to facilitate communication. See Exhibit 1 on page 13 for a brief description of these three aspects.

How Financial-Information Infrastructure Abstractly Creates Value for Clients and Society, Or: Why Financial-Information Infrastructure Is Being Hired by Clients and Society

Making assets findable and describing them

It **maps and categorizes the asset universe** by making assets uniquely identifiable and by providing descriptive information about these assets.

It acts as ***numbering agency*** by providing securities with a unique identifier (known as ISIN).

It acts as ***reference-data source*** by producing structured

- *issuer data (e.g., legal identifiers, corporate structure and hierarchies, capital structure, PEP checks, sanction screening; credit, risk, or sustainability ratings)*
- *asset data (e.g., ISIN, Terms and Conditions, clearing-code identifiers)*
- *issuer-asset data (e.g., corporate actions, interpreting nuanced non-standardized corporate actions, regulatory and tax implications).*

Helping monetize data

It helps data owners monetize their data.

It acts as ***data-distribution intermediary*** (connectivity intermediary) by helping data owners provide access to their (raw) data to third parties.

It acts as ***rights-to-data marketplace*** (platform operator) by helping data owners create, sell, and enforce rights to their data. It has hence contributed to the creation of data as an asset, and more recently as a digital asset ('data-as-digital-assets').

Delivering issuing and investment decision support

It facilitates/improves issuing and investment decisions by **providing information & intelligence and/or by reducing costs** (cost mutualization).

It acts as ***data-access intermediary*** by

- *checking veracity* of the raw data (e.g., identify, verify, trace source of data)
- *cleaning and preparing* the raw data (e.g., eliminate incorrect data records, correct incorrect/incomplete data, eliminate redundancies, resolve data-source conflicts, parse unstructured data, structure unstructured data, build data models)
- *aggregating/normalizing* the raw data into a single internally-consistent unified data model (consolidating/ translating multiple data models into one).

It acts as ***FI source*** (which may amount to reference data) by

- *creating/producing new digital data* (e.g., satellite and sensor data, non-digital regulatory data)
- *creating/deriving new data* out of existing digital data (e.g., trained analytics algorithms, interpreting regulatory data, news data, calculating prices for illiquid assets, rating data)

It acts as ***data-related services provider*** by deploying digital UIs, algorithms-as-a-service, cloud-based advanced-analytics environment, etc.

It acts as ***FI-services marketplace*** (platform operator) for issuers and investors to access FI-sources and FI-services from various providers.

Method

We use a five-step process to identify our scenarios.

- We start by **abstracting the system under analysis in terms of 'jobs it is hired to do'**. The high-level categories we abstracted to are depicted in Exhibit 1 on page 13.
- We consider a vast array of **factors** across all STEEP dimensions (social, technological, economic, environmental, political) and identify **possible future developments** (or 'projections') for each of these factors.
- We then assess how both individual and combinations of developments could **impact** the above-mentioned high-level categories. This is both a rational as well as creative exercise.
- It is difficult to work with this unstructured information about the future. We therefore synthesize this information about the foreseeable future variability in the form of **scenarios** by combining internally consistent future developments.
- We finally **challenge** this set of future scenarios from different angles to reduce the likelihood of missing key developments.

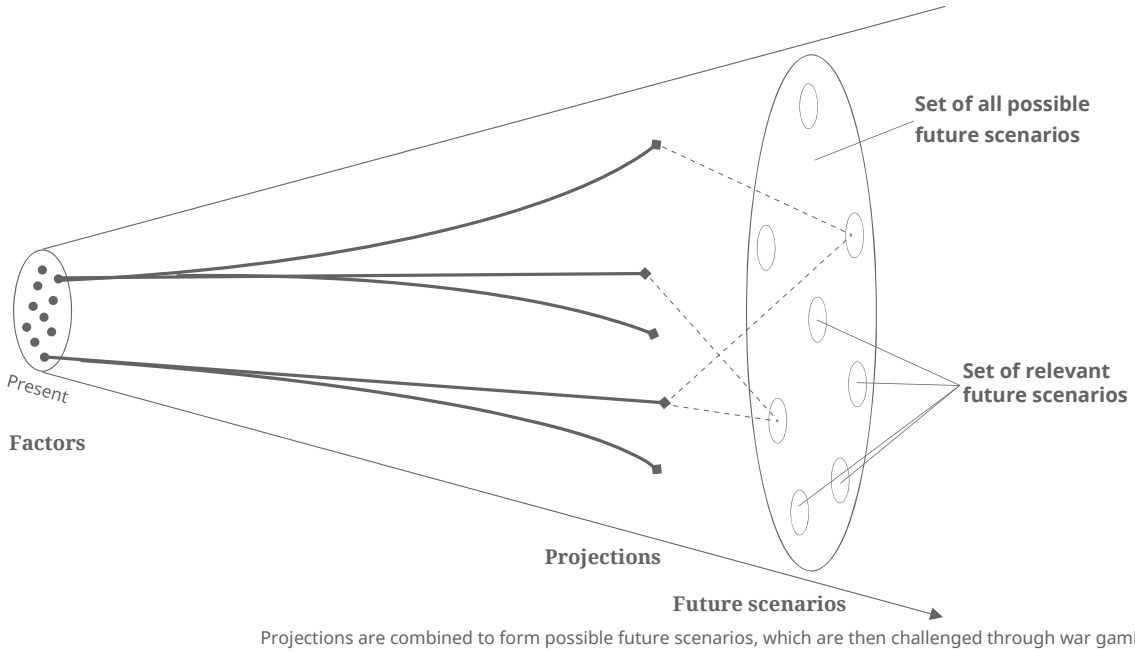
Our set of scenarios does **not aim to provide a map of all the foreseeable future variability** — *we provide a set of possible future scenarios that we view as most helpful for strategic decision-makers setting the strategic direction for the future.*

The scenarios **need not be mutually exclusive**. And a scenario may amount to a more extreme version of a development already captured by another scenario.

We strive for a **heterogeneity in the sources of data and information**. A large and diverse number of people were involved throughout this exercise in the form of workshops, brainstorming sessions, interviews, and reviews. We attended conferences, read lots of books, papers, blogs, and watched our fair share of science-fiction movies.

A note of caution. We try to ground all our statements on empirical (qualitative and quantitative) data. But this data does not give definitive answers regarding how likely a development might be, or what its potential impact might be. The data must be interpreted and creatively expanded. Hence, **our statements capture our empirically informed beliefs**. To help each of you make up your own mind, we pay special attention to always explicitly provide our assumptions, reasoning, arguments, and supporting evidence.

If you disagree with our assessments, or if you believe we missed a crucial development/scenario, please let us know. This is a learning journey for all of us.



Projections are combined to form possible future scenarios, which are then challenged through war gaming, greenfield designing, tipping-point crossing, what-if questioning, 30-year-horizon backward thinking, black-swan scouting

Factors: Catalysts, Drivers, Developments, Trends

This Section depicts some of the factors that were considered in the development of our future scenarios. Factors we consider having the greatest impact are indicated in bold.

Social/Cultural	Technological	Economic	Environmental	Political[14]
24/7 availability	**Advanced analytics**	Diffusion of knowledge and intellectual property	Decentralized energy production/smart grid	Anti-competition concerns
Convenience	Augmented reality (AR)	**Digital assets**	Global warming	**Anti-globalization**
Crowd collaboration	**Artificial intelligence**	**Digital data**	Increasing environmental pollution	Big-tech criticism ('tech-lash')
Customization/Individualization	**Automation**	**Digital marketplaces**	Post-oil electricity	Challenge of public finances
Demographics (aging population)	**Cybercrime**	**Disintermediation**	Renewable energy	**Data sovereignty/control**
Digital natives	**Data veracity**	E-business	Shortage of raw materials	Digital warfare
Digital User Interfaces	**Digital Rights Management**	Eco-capitalism		Global power struggles/redistribution
Do-it-yourself mentality	**Distributed Ledger Technology (DLT)**	Global economic growth		Global stability
Entrepreneurship	Edge computing	Growing education markets		**Government trust**
Voice-based HMI	**Federated AI**	**Growing global middle class**		Nationalism
Instantaneity	**Homomorphic encryption**	Increasing intensity of competition		**National-security concerns**
Privacy	**Human-machine interfaces**	**Increasing speed of change**		**Protectionism**
Security	Internet of Things (IoT)	Interoperability/APIs		Rise of China and India
Sustainability	Internetization	Management innovations		State surveillance
Mobility	**Knowledge systems**	**New economic powers**		Weaponization of economic tools
Omni channel	**Privacy-preserving algorithms, systems, and analytics**	Open data standards		
One-stop shops	**Privacy-preserving advanced analytics**	**Platformification**		
Polarization of wealth	**Secure multi-party computation**	Productivity growth		
Social media	(Smart) Chatbots	Skill scarcity		
Social sharing	Quantum computing	Strong economic blocs		
	Quantum-resistant encryption	Productivity growth		
	Virtualization and dematerialization	Strong economic blocs		
	Virtual reality (VR)			

14 Includes legal and regulatory factors and international relations.

Summary of the Scenarios

We have identified **five future scenarios** that we think will be of interest to strategic decision-makers in the financial-information space. We focused on alternative scenarios that we believe would have a substantial impact on the financial-information infrastructure, would necessitate considerable adaptations in decision-makers' mental models, and/or should receive more attention and thought. This Section briefly summarizes the key points captured by these scenarios.

All scenarios are divided/described in two parts: a **context part**, which describes how the broader world looks, and an **FI-Infrastructure part**, which describes how the financial-information space looks. Our most likely scenario is described in significantly more detail than the alternative scenarios because it captures a multiplicity of concurrent possible future developments — alternative scenarios generally capture only one possible development, making them easier to grasp. Although we strive to make each alternative scenario stand by itself, we recommend first reading the most likely scenario.

All our scenarios make an implicit underlying assumption: **There will continue to be a supply of and demand for investable (digital) assets in the future**. In other words, there will still be entities wanting to sell assets such as financial products, and there will still be entities wanting to invest in those financial products. We do not deal with the alternative scenario in which this is no longer the case here. We also believe this to be a very-low-likelihood scenario: The reasons for supplying investable assets (capital raising, hedging, liquidity provision, speculation, capital gains, monetizing of idle/underutilized assets, etc.) as well as for investing/trading in them (capital gains, hedging, societal impact, speculation, etc.) are likely to remain relevant in the future.

Exhibit 2 on page 20 summarizes all our statements about the future in one graphic.

Most Likely Scenario: *Freedom to Generate, Right to Control, and Ability to Monetize*

*From the perspective of a person, our most likely future is primarily characterized by **people having greater freedom, rights, and ability in their capacity as asset owners, data owners, and investors**. Anyone can transform their assets into investable assets by creating rights to them (digitally tradable rights to assets). Anyone can control usage of their data and create rights to it (digitally tradable rights to data). Anyone can invest in perfect alignment with what matters to them (investment tailoring). For a full human-centric description of this most likely scenario, see page 27.*

Context: **The number of investable assets has exploded**. *Investable assets range from seats at a restaurant, usage rights to a parking spot, rights to a share of a students' future income, rights to use a room in an apartment, usage rights to your data, rights to advertise in a spot on a webpage, to rights to a share of the proceeds from a newly released song.*

Digitalization has propelled the number of investable assets in two ways. On the one hand, digitalization has simplified the process of defining/describing digital and non-digital assets, and of creating rights to these assets (digitally tradable rights to assets) — thus reducing monetary and time costs of making an asset investable. On the other hand, digitalization (digital platforms) has permitted reaching a global market, thus rendering it substantially more attractive for asset owners to make their assets investable.

In parallel, there has also been an **explosion in digital data and in its accessibility**. Three drivers mainly underlie this development.

First, *everything produces digital data*. People wear sensors in all shapes, forms, and places for self-optimization and self-monitoring. Social interactions increasingly take place in the virtual sphere (chat, VR). And real-world experiences are augmented with a digital layer (voice interfaces and/or AR).

Second, *data subjects have been granted sovereignty over their data*. Governments have taken substantial action to enforce property rights and competition in the digital sphere by reducing user lock-ins, unbundling services, breaking up vertical supply/value chains, and allocating rights to data. New laws and regulations have, among other things, focused on giving subjects extensive rights and control over their data (incl. data mobility via APIs), and on requiring digital services to easily talk to each other (interoperability and API standards). Users of digital services can prevent service providers from processing their data and can provide third parties with access to their data — data which may not have been accessible to third parties before, as service providers may have kept it for themselves.

Third, the *advent of privacy-preserving data distribution systems* has increased people's willingness to provide third parties with access to their data. Individuals can provide access to their digital photos while preventing any query that would reveal anything private (e.g., queries that could allow facial recognition would automatically be blocked, while queries about the places that were visited would be allowed). Corporations can provide access to their HR data, allowing queries on gender ratios or age distribution, while being certain that queries that could reveal information about any specific employee would automatically be blocked.

The crowd itself has thus increasingly become a data source (**crowd-sourced data**). The explosion in data has led to an **explosion in theme-related information**. There is data allowing investors to evaluate investable assets in any dimension, helping them to better tailor their investments to their preferences (e.g., gender equality track record, specific machine learning algorithm development or deployment, video-gaming industry, social/sustainability impact).

Access to data has been strongly democratized. Three drivers mainly underlie this development. First, *the price of access to data has fallen substantially* due to digitalization (everything produces digital data) and technological advances (automation, digital platformification). Second, *data subjects have been granted sovereignty over their data* (see above), putting all data users (incl. those providing the digital services wherein the data is generated) on equal footing to access this data. Third, *people have been granted equal access to data*. In their efforts to enforce competition in the digital sphere, governments have levelled the playing field for data access. They have prevented exclusive usage/access to data sets, requiring companies to provide third parties with access to their data (against compensation or for free) and breaking up vertical supply/value chains to carve out data-producing entities.

Investors continue to take some decisions themselves, but **delegate most of their investment decisions** to professional asset managers (e.g., funds, collective or individual mandates). Tailored robo-funds, where algorithms automatically take investment decisions, have increased in popularity. Actively-managed funds, where humans are involved in defining the investment strategy and/or take the investment decisions, co-exist alongside passively-managed funds such as ETFs.

Driven by the explosion in new (accessible) digital data, **alternative data has established itself alongside traditional financial information** as key input for investment decisions. As new types of assets become investable, further data types and sources may become relevant inputs for investment decision-making. Social impact and sustainability considerations play an increasingly important role in investment decisions.

Investors have strongly **outsourced non-differentiating processes and activities, especially in the regulatory space**, to benefit from cost mutualization. Investors have also deployed cloud solutions at scale to further reduce costs, improve cyber defenses, and access new technologies.

Finally, we do not expect the raw data by itself to be the main value driver in this future economy. Instead, we expect **most value creation to be driven by the players that invent on top of this data**, combining and expanding the data with their unique capabilities.

FI Infrastructure: **Ever more data is stored decentrally and accessed in real-time**. The explosion in digital data makes central storage (i.e., duplication) at data-distribution intermediaries or investors too costly and arguably infeasible.

The majority of digital data is hidden/private (e.g., encrypted, stored at the edge). Data owners want to keep their data hidden/private because of privacy concerns and/or because they want to optimally monetize their data.

Companies have strong incentives to build their digital services upon privacy-preserving technologies.

Data privacy also calls for the raw data to be decentrally stored where it is produced — specifically, it calls for *'raw data to never move'* beyond what is required by the application/service generating that data.

Data privacy thus states that the raw data, even in its encrypted form, should never move — only the results of data processing are to be distributed (e.g., trained model parameters). Where latency or data-query volumes are too high for existing technologies, trusted intermediaries may (temporarily) continue to centrally store the encrypted raw data — but without further distributing this encrypted raw data.

Data privacy also requires the *'raw data to always be encrypted'*. Data distribution systems crucially build upon 'secure multi-party computation' and 'federated AI'.

Secure and privacy-preserving systems are a foundational technology of FI infrastructure. Data owners demand data security/privacy from data-distribution systems because of privacy concerns and because they want to optimally monetize their data. Investors demand security/privacy from data-access systems and from (cloud-based) advanced-analytics environments because real-time data queries/sourcing and algorithm calibrations could reveal their investment/trading strategies.

The FI infrastructure space has experienced **digital platformification (marketplaces)**, which market participants can directly access, and whereon market participants can interact directly with each other (**disintermediation**). Two types of platforms define the FI landscape for issuers, investors, and data sources.

First, *rights-to-data digital marketplaces* allow data owners/sources to easily create and sell rights to their data (digitally tradable rights to data). The ownership to these rights is stored in a (digital-assets) ledger. Western corporations are leaders in this space because Western countries were first movers in giving data subjects extensive rights over their data.

Second, FI-*services digital marketplaces* aggregate FI services and FI-services providers to provide issuers and investors with convenience and comparability (transparency). Issuing-and-investment-decisions solutions range from access to some raw data, to cleaned data, to rights to data, to regulatory solutions (e.g., regulation monitoring, issuing-document generation), to ratings (e.g., credit ratings, sustainability ratings), to data playgrounds, to cloud-based privacy-preserving advanced-analytics environments, and to digital UIs (e.g., desktop, smartphone, AR, VR). FI services are **fully unbundled**: Investors can even choose different providers for access to raw data, for cleaning the raw data, for verifying the raw data (data veracity), for normalizing/translating the raw data into a single unified data model, for analyzing the data (e.g., big data infrastructure), and for visualizing the data and results (digital UIs). **The selected services are seamlessly integrated** with the buyers' existing software and applications. This **plug-and-play** world (interoperability, zero technical switching costs) provides customers with greater choice, better tailoring, and a seamless UX (convenience). Buyers can, of course, choose to continue sourcing all FI services from the same provider.

***Technical* switching costs between data sources have fallen to zero**. Investors can readily switch between providers of data sources. Providers of non-unique data sources see their profits fall as customers can readily switch between providers. Profits of non-unique data sources/intermediaries may, however, not fall to zero because differentiation may still be possible on the quality of the data (i.e., data veracity, data cleaning and preparation, unified data model).

Big tech companies have become buyers of FI services as they expanded into offering wealth-management and investment solutions to their users (further increasing engagement and data). Although big tech companies' activities strongly overlap with the FI-services space, it is **unclear whether they will leverage those capabilities and become FI-services providers themselves**. They may instead opt to provide technology to FI-services providers (**TechFin**) to avoid a possible regulatory focus on FI-services providers and not further ignite anti-trust concerns they already face.

Exchanges and trading venues continue expanding into the FI-services space to counter eroding margins in their traditional businesses.

Alternative Scenario: *Middle- and Back-Office Consolidation in Finance*

This scenario describes a more extreme version of a development also found in a more subdued form in the most likely scenario.

Context: From banks, to insurances, to asset managers, all financial services providers **outsource virtually all their middle- and back-office activities to utilities** in order to benefit from economies of scale on non-differentiating activities and to access rare skills/capabilities.

FI Infrastructure: The number of middle- and back-office clients has reduced significantly. **FI-infrastructure providers serving the middle- and back-office are likely to experience a reduction in profits even on differentiating services (unique content)**.

Alternative Scenario: *Extreme Consolidation in FI Infrastructure*

This scenario describes a more extreme version of a development also found in a more subdued form in the most likely scenario.

Context: **Global players dominate most markets**. Digitalization has turned most markets into **winner-takes-it-all**. The most likely path to this scenario is **lack of government action aimed at enforcing competition in the digital sphere** by reducing user lock-ins, unbundling services, breaking up vertical supply/value chains, and restricting exclusive access/usage of data.

FI Infrastructure: **All platforms in the FI space have global scale**. There is a single *global digital marketplace in the FI-services space* and a single *global data-distribution and data-access intermediary*.

(Niche) FI-service providers around these global platforms have global scale wherever scale provides an advantage. Local niche FI-service providers co-exist with these global players — where scale provides no advantage, and/or where scale benefits alone do not allow offering a strictly superior value proposition.

Alternative Scenario: *Extreme Protectionism*

Context: Services/products face **import and export barriers** and raw data is restricted from leaving the country (**data protectionism**). Anti-globalization sentiments (e.g., stagnating/falling job prospects and incomes), national-security concerns (e.g., foreign spying through pre-installed backdoors, system breakdowns through pre-installed kill switches), and weaponization of economic tools to further national interests (e.g., restricting domestic corporations from doing business with foreign corporations) have all been on the rise.

FI Infrastructure: The FI infrastructure is considered **critical infrastructure**. Governments want a **locally-operated FI infrastructure** to ensure a functioning local market that efficiently allocates capital. FI-infrastructure providers have been **forced to sell the systems they operated in foreign countries**. Domestic FI-infrastructure providers **operate local secure and privacy-preserving data-distribution systems** that allow domestic data owners/sources to sell rights to their data abroad and that allow domestic investors to access foreign data — without any raw data crossing borders.

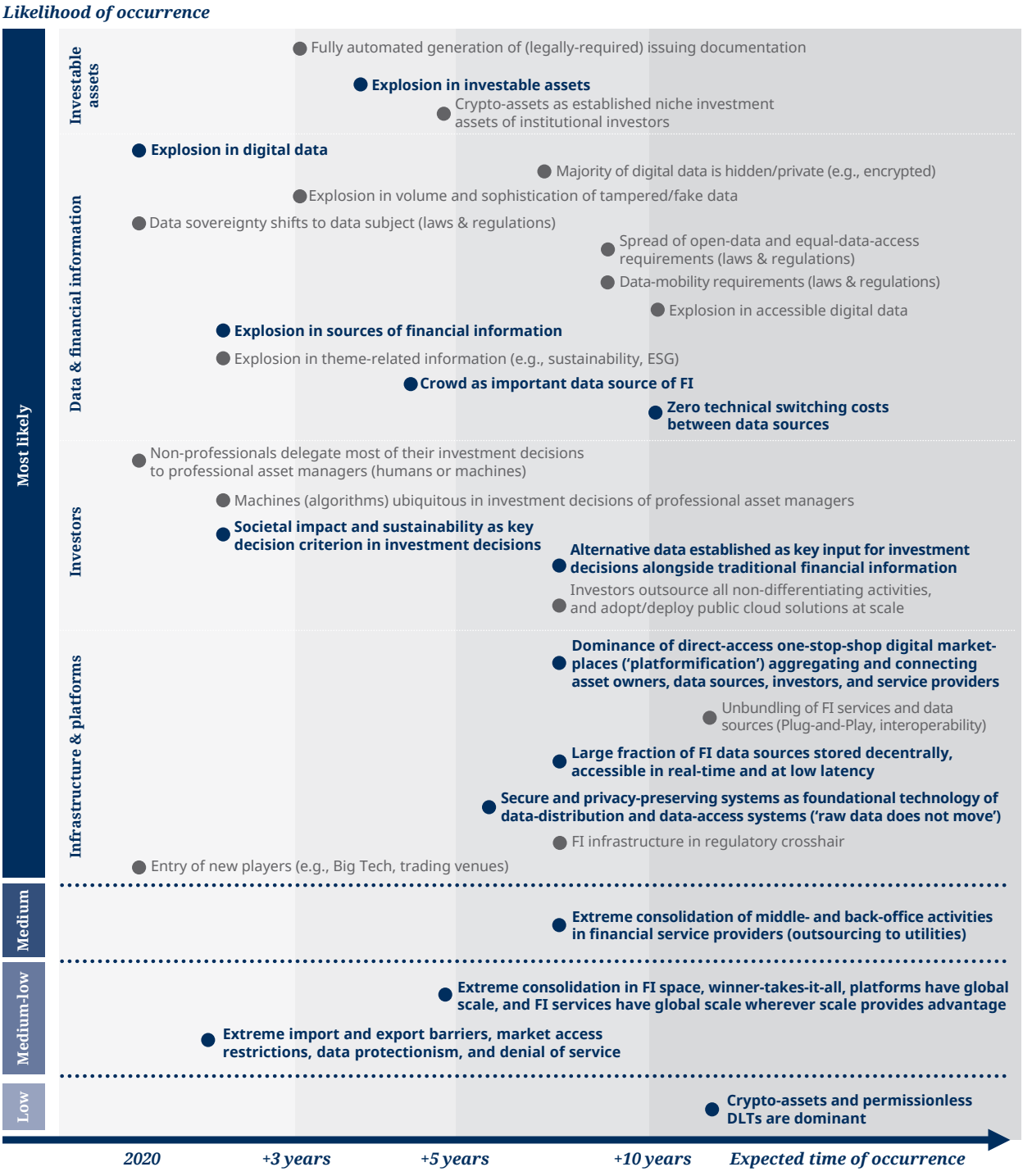
Alternative Scenario: *Crypto-assets Everywhere*

Context: **The world runs on permissionless distributed ledgers.** *Crypto-assets* are the dominant form of digital assets and of investable assets. *Decentralized crypto-currencies* have replaced central-bank-issued currency as the dominant medium of exchange. Commercial digital operations take the form of open-source code stored and executed on top of these permissionless distributed ledgers, known as 'decentralized applications' (*DApps*).

FI Infrastructure: **'Rights to data' take the form of crypto-tokens** that are registered on these permissionless distributed ledgers. Secure and privacy-preserving data-distribution systems and FI-services more generally take the form of **open-source DApps**.

Overview of All Statements

The graphic summarizes our statements about the future, and classifies them according to their 'likelihood of occurrence' and 'expected time of occurrence'. The key statements describing our possible futures are indicated in bold.



Inputs for Strategy

This Section discusses some of the strategic implications of our scenarios for players active in the FI space.

Changes in the Fundamentals of How the Business Works

Data sovereignty shifts toward data subjects. The users of digital services have extensive rights and control over their data, enabling third parties to access data that was hitherto the unique preserve/asset of the service providers.

Sources of relevant data for investment decisions are increasing exponentially. There is an explosion in digital data, and this new data may carry information relevant to the investment sphere. Findability is key as people need help with finding what they are looking for. There is an explosion in investable assets, which may require new types of data. And there is an increasing demand for social impact and sustainable investments, necessitating new types of data.

Issuers and investors can readily switch between data sources. There are zero technical switching costs between data sources. Government-mandated or market-participant-driven standards may appear. And if not, intermediaries enable issuers and investors to seamlessly switch between data sources by aggregating different APIs (or 'data models') into a standardized one, and/or by providing matching algorithms that (semi-)automatically translate one API (or 'data model') into another.

Providers of non-unique data sources, including data-distribution and data-access intermediaries, see their profits fall. Customers can readily switch between data sources/intermediaries carrying this non-unique data as well. But profits from distributing non-unique data sources may not drop to zero because differentiation may still be possible on the quality of the data (i.e., data veracity, data cleaning and preparation, unified data model).

FI services are offered via digital marketplaces (platformification) and can seamlessly integrate with one another (interoperability, plug and play). Customers demand aggregation across FI services and FI-services providers for convenience and comparability. Customers also expect interoperability between FI services to freely combine them (greater choice, better tailoring) while providing for a seamless UX (convenience).

'Rights to data' take the form of digital contracts. Rights to data evolve from unstructured contractual statements to formalized digital usage policies. Anyone can seamlessly create and sell rights to their data (digitally tradable rights to data). Enforcement of these rights ('rights management') is increasingly automated.

Ever more raw data is decentrally stored, encrypted, and immobile. The explosion in digital data makes it virtually impossible to store all data centrally. It is widely accepted that data privacy requires that the 'data is always encrypted' and that the '(raw) data never moves'.

There is therefore a paradigm shift in data distribution and data access. The raw data, even in its encrypted form, should never move — only the results of data processing (e.g., trained model parameters) are to be distributed. Data-distribution and data-access systems must provide access to encrypted raw data in real-time and at low latency. They must handle a high volume of simultaneous data processing queries — while preserving the privacy/secrecy of both the data queries and raw data. Where latency or data-query volumes are too high, trusted intermediaries may (temporarily) continue to centrally store encrypted raw data, but without further distributing it.

Data cleaning and preparation is exponentially more challenging. Data cleaning and data preparation must be performed on decentrally-stored always-encrypted not-to-be-distributed raw data.

Data veracity is an increasingly valuable service. Demand for data veracity is increasing because of rising data-tampering risks (hacking), because of advances in fake data (deep fakes), and because of new data sources (e.g., smartphone pictures, social-media data).

Middle- and back-offices of financial institutions are increasingly outsourced and possibly consolidated at some utility. They outsource their activities to benefit from economies of scale on non-differentiating activities and to access rate skills/capabilities. This reduces the number of customers for FI services aimed at the middle- and back-offices, and thus increases their bargaining power.

Big tech companies must be monitored closely. Their business models, capabilities (e.g., customer base, data sets), and technology stacks transfer well into the FI space.

Possible Moves

Consider providing theme-related information to help investors better tailor their capital deployment to their preferences. This information may help investors ameliorate their financial returns (e.g., specific machine learning algorithm exposure), and/or may help them invest according to non-financial preferences (e.g., social impact, sustainability). The explosion in digital data and technological advances reduces the costs and latency of producing this information.

Consider increasing efforts to acquire unique data and/or developing unique content. Profits from distributing non-unique data are dropping, driven by the falling technical switching costs. High-profit pools persist in unique data as well as in unique content (FI services), both of which may result from combining one's unique assets/capabilities with non-unique data.

Consider evaluating data veracity by building a brand as trusted partner. Data veracity increases in importance because of increasing risks of third-party data tampering (e.g., hacking, deepfakes) and because of increasing reliance on new data sources that may be less reliable/trustworthy (tampering by the source itself).

Consider building a brand as trusted partner by assessing data usefulness. Ex ante information of the potential usefulness of data sets increases in importance as data sources rise exponentially. Investors' opportunity costs of spending time analyzing/processing a useless data set rise exponentially as well.

Consider helping issuers and investors seamlessly switch between data sources. In the absence of a government-mandated standard, market participants may self-organize to agree on a standard. If not, an intermediary may reduce technical switching costs by aggregating APIs (or 'data models') into a standardized one or by training a matching algorithm to (semi-)automatically translate between APIs.

Consider helping issuers and investors reduce regulatory costs. Compliance costs and non-compliance fees are likely to remain high. The necessary activities/processes are highly non-differentiating and increasingly scalable (due to advances in automation/AI). Large economies of scale can be reached through outsourcing these activities/processes.

If you aim at helping data owners/sources with the creation and sale of 'rights to their data', then consider leveraging an existing digital-assets ledger. Building on a third-party (centralized or distributed) ledger infrastructure allows leveraging its scale and focusing on your core — enabling anyone to seamlessly create and sell digital usage rights to their data.

If you aim at owning the customer relationship, then consider building/operating an open digital platform. One-stop-shop digital marketplaces, aggregating across service providers, are replacing traditional distribution channels and may become the customer interface.

Consider supporting non-investment decision-making. Boards and management teams across industries need data to make strategic and operational decisions. Improved demand forecasting reduces out of stock events, reduces inventory needs, and ameliorates planning (reduces the number of goods needing discounting). New data sources (alternative data) may also be of value in non-investment decision-making.

Consider expanding into helping financial institutions in underwriting or advisory. Help lenders and insurers access data about their clients that sits in third-party systems (e.g., social media platforms) and that provides valuable input for decision-making. The lending business of financial institutions, in particular, is under pressure from new players (e.g., big tech companies) with enormous data on customer behaviors and preferences.

Consider expanding into helping customers make more informed purchasing decisions. Leverage the new sources of data to help customers better choose services/products that align with their preferences by providing theme-related information on producers (e.g., diversity, sustainability, social impact, employee happiness).

Consider helping banks become 'data brokers' for their clients. Banks could leverage their reputation as trusted partners to expand from brokering investment deals to brokering data deals. Banks could help their clients optimally monetize their data, while preserving its privacy, by creating and selling 'usage rights' to this data.

Consider partnering with big tech companies. Although their technologies and capabilities transfer to the FI space, they may not be inclined to enter the FI-infrastructure space. They may therefore be open to (licensing) partnerships.

Consider joining a permissioned-distributed-ledger consortium to develop FI services as Dapps. This could help develop at low cost the ability to move fast if a crypto-assets world becomes more likely.

2 Relevant Future Scenarios

Freedom to Generate, Right to Control, and Ability to Monetize

Most-Likely Scenario

Early-detection signals: Early-detection signals: Explosion in investable assets; explosion in digital data; high privacy concerns; connected sensors everywhere and in everything; high sustainability considerations; demand for data monetization; rising data privacy/security concerns; advances in privacy-preserving data processing algorithms; advances in secure multi-party computation (e.g., homomorphic encryption); advances in automated API (data-model) translation algorithms; spread and adoption of API (data model) standards; digital platformification; high regulatory costs in investment sphere; government action to enforce private property rights and competition in the digital sphere (e.g., data subjects have sovereignty over their data; data mobility, interoperability, and API standards requirements; restrictions to exclusive usage/access of data).

Probably not everything will be investable, not anything will produce data let alone information, and not everyone will be investing. But we believe that these more extreme statements help better grasp the essence of our most likely scenario: Everything could be investable, anything could amount to information, and everyone could be investing.

Freedom to Generate, Right to Control, and Ability to Monetize

The Human-Centric Story

From the perspective of a person, our most likely future is characterized by one core message: **People have greater freedom, rights, and ability in their capacity as asset owners, data owners, and investors.**

- Anyone can transform their assets into investable assets by creating rights to them (digitally tradable rights to assets).
- Anyone can control usage of their data and create rights to it (digitally tradable rights to data).
- Anyone can invest in perfect alignment with what matters to them (investment tailoring).

Choice (freedom, ability) and private property (control, ability) encapsulate the liberal principles we associate with development. **Our most likely scenario therefore describes an optimistic and desirable future of sustainable development** — where progress is understood more holistically than economic growth. In the following, we will discuss some concrete ways in which freedom, rights, and ability in these three dimensions contribute to the sustainable development of our societies. We will also suggest that the status quo falls significantly short with regard to 'freedom, rights, and ability' in these dimensions.

The world seems to be changing at an ever-faster speed and becoming increasingly unpredictable. Globalization has led to events happening on the other side of the globe having impacts here, locally. Job skills become obsolete faster than it takes us to master them. While the prospect facing younger generations is that they will be at best as wealthy as their parents, and most likely poorer than them. Concerns abound that pension funds will not be able to meet their future financial obligations. The most promising parts of the economy are ruled by monopolies and oligopolies, making a few lucky ones extremely rich, and seemingly leaving little opportunities for the rest of us unless we join them. Growing protectionist sentiments threaten economic opportunities for most of us. All the while negative interests are eating away what we saved. In this world of economic uncertainty and insecurity, *it is important that we can monetize what we own, and own what we produce*.

But monetizing what we produce and own is difficult. Creating rights to our assets is both time consuming and costly, requiring the involvement of lawyers and notaries. Offering these rights for sale is then limited in scope to who we know, unless we are willing to involve costly professional intermediaries. Furthermore, the data we produce is owned, controlled, and monetized by others, with little regard to our privacy. Finally, freely deploying, and therewith monetizing, capital is to a large extent restricted to the rich as intermediaries restrict access to certain investable assets in order to offer exclusive access to their higher-business clients.

At the same time, climate change is happening all around us, and our chance to avoid extreme warming seems to be slipping away. True (gender, race, age) diversity and equality is still a future dream. Authoritarian regimes hijack and disrupt democratic elections in foreign countries, leveraging digital technologies to polarize people by feeding on their deepest fears and prejudices. All the while tensions between old and new global superpowers are on the rise. In this context, *it is important that we have the freedom and ability to generate the greatest impact possible with what we own*.

But using what we own and produce to generate the impact we want is difficult. Our data — which contains information on our fears, beliefs, prejudices, or intentions that not even our spouses may know about — is not under our control. We cannot prevent it being harvested and misused against us by influencing our decisions in elections, creating social unrest, tailoring advertisements to better monetize us ('surveillance capitalism'), or keeping us glued to our screens (the euphemism is 'engagement'). We also cannot give others seamless access to most of our digital data, sitting in some service provider's database, in order to help improve their decision-making. Furthermore, capital, which is a key driver of where we are heading, is not flowing freely. Its deployment is hindered because certain investment classes are only accessible to a select few (see above). And it is also hindered because the necessary data/information to assess the impact, which we would generate with our capital, is either not always available, too costly to produce, or simply not accessible to third parties.


EVERYTHING
IS INVESTABLE
The marketplace for issuers.
Need help navigating and fulfilling regulations? Need help making your assets findable? Need help structuring and timing your issuing?
We have it all.
CLICK NOW
Grand Opening on Saturday
BAKERY
UNLOCK THE VALUE IN YOUR ASSETS.
Make your assets investable in one click.
BAKERY

Freedom to Generate, Right to Control, and Ability to Monetize

But digitalization, technological advances, and an upgraded legal framework can create a future giving people greater freedom, control, and ability in their capacity as asset owners, data owners, and investors. Based on our interpretation of the data, we hold that the most likely future is one of greater 'freedom, rights, and ability'. **But, although it has the highest likelihood, this desirable future is still far from certain.** We therefore hope that this white paper will motivate and inspire governments to step up their efforts toward designing the necessary framework. And that it will motive businesses to allocate resources into building the products and services that will help us reach this desirable future.

The next pages describe the perspective of an asset owner, data owner, and investor in this most likely scenario in more detail.

Asset Owners

Freedom to generate investable assets. Right to control access, usage, and ownership to our assets. Ability to monetize our assets.

Asset owners can transform the assets they own into investable assets by creating rights to them. Imagine selling the usage right to your parking spot that lays empty while you are at work. Imagine selling the usage right to your apartment (like 'AirBnB') or car, or selling some ownership rights to your luxury car. Imagine selling the right to place a product in a specific scene of your upcoming movie. Imagine selling the rights to the second and third interest payment of a loan you gave to a friend. If you are a student, imagine selling rights to your future income. If you are a football club, you may sell rights to a percentage of a player's future transfer price. If you are a restaurant owner, imagine selling the usage right to a seat/table on Saturday evening (instead of letting people book for free). If you are a musician, imagine selling rights to the future proceeds of your new song or album. If you own a popular website, you may sell the rights to use certain areas for advertisement (Google and Facebook have built their business on selling such rights). If you are a mayor, you may sell ownership rights to trees or public work of art (e.g., a fountain). The possibilities are truly endless.

At the press of a button, an algorithm pulls all the data imaginable and necessary to describe the asset. Everything is in digital form. The notarized and legal documents, the physical integrity and usage status based on the many built-in sensors, etc. The algorithms working in the background not only collect the data, they also put it in the form that has worked best with investors and buyers over past years. A standard has not emerged yet, but does not seem to be far off. There is now a digital description/definition of the asset.

Asset owners can easily create rights to any type of asset (digitally tradable rights to assets), leading to an explosion in number and variety of rights to (digitized, native digital, or underlying non-digital) assets, and therewith to an explosion in investable assets. You choose the kind of rights you want to associate with an asset. You may tell it to your digital voice assistant, and algorithms in the background then automatically generate the legal documents. When the algorithms do not feel confident enough to take a decision by themselves, they request a human for review — this is no longer happening as frequently, as machines have learned from the many earlier rounds of review. The rights can then easily be partitioned into small pieces (fractionalization), to democratize access and increase secondary-market liquidity.

Assets owners can issue these rights to a global customer base via digital platforms (marketplaces). You can directly interact with potential buyers/investors from around the world, without having to go through a middleman (disintermediation). This is similar to how the digital marketplace eBay allowed you to find the one person on the face of the earth collecting the playing cards from 1983 you still have in your basement (access to the long tail). As a result of this disintermediation and digital platformification, **access to investable assets has been democratized**.

Finally, asset owners' willingness to transform their assets into investable assets has further increased due to falling monitoring costs. Data feeds, generated by connected sensors in non-digital assets, allow asset owners to automatically track the asset's usage and thus to monitor whether the agreed-upon conditions are being respected.


EVERYWHERE
IS INFORMATION
We help you monetize your data.
Create and sell rights to your data.
Give others access to your data.
Data security and privacy guaranteed.
Click here to start sharing.
WE NEED YOUR DATA
COURTHOUSE

Freedom to Generate, Right to Control, and Ability to Monetize

Data Owners

Freedom to generate data. Right to control access, usage, and ownership to the data we produce. Ability to monetize our data.

Data is a specific type of asset. Everything said for asset owners thus applies here as well. But data exhibits some peculiarities that we wanted to point out.

Everything produces digital data — the volume and types of digital data have continued to explode. People wear sensors in all shapes, forms, and places for self-optimization and self-monitoring. Social interactions take place in the virtual sphere (chat, VR). Real world experiences are augmented with a digital layer (voice interfaces and/or AR) to provide additional information and to interact with the objects themselves. Cities are riddled with sensors and cameras (smart cities). Clothes tell washing machines how to treat them. It is as if whatever we do, digital data is being produced.

The majority of digital data is hidden/private (e.g., encrypted, stored at the edge). Data owners and producers have placed high data privacy demands on service providers. Indeed, we have all experienced Uber employees snooping on their ride and location data, have observed Facebook losing their data, have seen even the richest person Jeff Bezos blackmailed with his hacked data, and have witnessed big tech companies make a fortune on the back of our data. Data privacy, most notably, requires that the raw data is always encrypted, and states that the raw data should never move beyond what is required by the application/service generating that data.

The demand for data privacy also has indirect consequences for digital service providers: They might no longer see the raw data of their users' activities. Facebook, for example, itself believes that the future lies in end-to-end encrypted communication — which would prevent it from seeing the usage data of its users. And encrypted communication is only the start. Where service providers do not by themselves offer sufficient data privacy to clients, they can easily be prevented from seeing your data. You could, for example, start on Amazon's marketplace to search for a product, switch onto a communication medium that offers end-to-end encryption to contact the seller, and finally, use a third-party payment provider for the payment. You may even prevent Amazon from seeing your searches and clicks by letting your UI (e.g., web browsers, mobile phone) automatically generate many different searches that Amazon cannot distinguish from your real search.

There is a lot of data that contains private information we want to keep to ourselves, but that cannot be attributed to data subjects without first analyzing this data. Think of data from cameras in satellites, self-driving cars, or AR glasses. Even this type of data now preserves people's privacy. At recording, the data is encrypted, anonymized, and/or kept at the edge. And statistical queries that could reveal (distribute) personally identifiable information are automatically intercepted and blocked.

Data owners are in full control over the usage of the data they produce. You can prevent digital service providers from processing your data — and hence from monetizing it. And, more importantly, you can give third parties access to your data, wherever this data is stored, from within video games, to social-networking apps, to health-tracking services.

Advances in privacy-preserving systems give data owners the ability to monetize their data while still protecting data privacy. You can provide access to your raw data for processing without ever distributing or revealing this raw data. Statistical queries are sent to your data and only the results of the queries are returned (distributed). Statistical queries that could reveal personally identifiable data are intercepted and blocked.

The fraction of data that is accessible for processing by third parties has exploded. The shift in data sovereignty to data producers/subjects has enabled you to provide third parties access to their data — data which may not have been accessible to third parties before, as service providers may have kept it for themselves. And privacy-preserving systems have enabled you, privacy-conscious data owners (people and corporations), to provide access to ever more of your (sensitive) data.


EVERYONE
IS INVESTING
THE SMART INVESTOR
•Access to raw data
•Usage rights to data
•Cleaned data
•Data models
•Data usefulness ratings
•Cloud analytics
•Sustainability ratings
•Regulatory solutions
•Funds and Advisory
•User Interfaces
THE SMART INVESTOR
ALL you need, ALL your favorite brands, ALL inter-operable

Freedom to Generate, Right to Control, and Ability to Monetize

Data owners can easily create rights to any type of data (digitally tradable rights to data), and then issue these rights to a global customer base via digital platforms (marketplaces). After creating rights to your data, you can interact directly with data users from around the world, without having to go through a middleman (disintermediation).

You can sell, loan, or gift your rights to your data. You may sell the usage right to your data to a pharmaceutical company to serve as part of a control group in an upcoming drug test. You may pay with usage rights to access a service (think Gmail or Facebook). You may gift usage rights to a university professor for her research. And you may sell your data in exchange for an equity stake in a start-up that is building services that are built on top of such data (e.g., artificial intelligence, machine learning).

Investors

Freedom to generate impact with our capital. Right to control deployment of our capital. Ability to monetize our capital.

Investable capital is a specific type of asset. Everything said for asset owners thus applies here as well. But capital exhibits some peculiarities that we wanted to point out.

Access to information has been democratized. The democratized access to digital data in combination with advances in technologies (e.g., AI, robotics) have allowed producing inputs for investment decisions at substantially lower costs. Where, 20 years ago, a hedge fund would have sent an intern to count the number of visitors to a supermarket, today a satellite takes pictures and a machine counts. More generally, algorithms sift through accessible digital data to produce information at much lower costs than ever before.

Investors can better tailor their investments to their preferences (investment tailoring) due to the broad availability of theme-related information. We all invest for different reasons. Social-impact and sustainability considerations are increasingly important alongside financial return. Some of you may want to invest only in companies that are strong on gender equality, while others may care for environmental preservation and climate change. Some of you may want exposure to the video-gaming industry, the cement-based construction sector, or a specific ML algorithm. Some of you may want to avoid exposure to businesses involved in the production and/or supply of weapons to repressive governments, from firearms, to missiles, unmanned drones, and AI systems.

Alternative data has established itself alongside traditional financial information as key input for investment decisions. The explosion in (accessible) data has led to an explosion in theme-related information. There is data allowing you to evaluate investable assets in any dimension you can think of — and many more. You can not only see an asset's performance on some metric, but have access to the underlying data. If you want to weight poverty reduction higher, you can do so by building your own personalized sustainability metric.

Investors can find all they need on one-stop-shop digital platforms (marketplaces), aggregating across services and service providers. These one-stop-shop platforms offer high comparability and uniform UX. Services are unbundled into their constituents (sub-services) and offered as separate services. All (sub-)services can talk to each other and are thus easily integrated with each other (interoperability, plug and play). The overall experience is as seamless as selecting an app from the app store on your smartphone — but without you being restricted to a single app store, because apps, even from different app stores, seamlessly communicate and integrate with each other.

Investors can freely combine (sub-)services from different FI providers and readily switch between them (plug and play). You may for example use one service provider to give you access to the raw data, another one to buy the usage rights for this data, another one for cleaning and preparing the data, and yet another one to provide the user interface. You can also readily switch between different service providers for the raw data (between data sources), or between service providers for preparing the data (e.g., between proprietary data models) — technical lock-ins are a thing of the past.

Freedom to Generate, Right to Control, and Ability to Monetize

Investors can deploy their capital in perfect alignment with what matters to them. Anyone not only has access to the entire investment universe (democratization of access to investable assets), but also to the necessary information to make investment decisions that are perfectly tailored to their preferences.

Freedom to Generate, Right to Control, and Ability to Monetize

I. Context

Ia. Investment Universe

Explosion in and Digitalization of Investable Assets

People continue to want to optimally monetize their (underutilized) assets.[15] Monetization hinges on being able to trade the rights to one's assets, on being able to create new rights to one's assets, and on having access to a large market for selling rights. Digitalization has rendered all of this much less costly, faster, and more convenient in three ways.

First, for someone (e.g., investors) to buy a right, the underlying asset needs to be defined/described. ***Digitalization has simplified the process of defining and describing assets*** because all data and information necessary to describe and define any (digital or non-digital)[16] asset is available in digital form, exhibiting traceability and immutability. Machines and algorithms then automatically combine this data to produce the necessary documentation.[17] Note that the resulting digital description/definition of a (digital or non-digital) asset itself amounts to a digital asset.

Before digitalization, defining an asset entailed painstakingly gathering all the documents and data, and doing so from various digital and non-digital sources. It sometimes meant engaging someone to certify the veracity of the data (e.g., notarized). Other times, it meant engaging an independent evaluator to assess the state of the asset (e.g., quality of the walls of a building).

Digitalization has facilitated the gathering of all this data and information. Contractual relationships related to the asset and applicable laws/regulations are in digital form and linked to it. Virtually every non-digital asset contains a connected chip (ubiquitous connectivity and chips),[18] which not only uniquely identifies an asset, but also captures real-time data relating to the asset itself as well as its environment (e.g., GPS data, wear and tear, usage, temperature). Furthermore, as ever more human activity shifts into the digital sphere, assets themselves tend to come in a digital form (explosion in native digital assets); all relevant data and information related to these digital assets are therefore already available in digital form and linked to it. Finally, traceability to the source of the data and immutability of data history are built into the databases storing all this data, increasing the likelihood that the data is authoritative/trustworthy.

Take a house as an example: The floor plans, the exact location, the construction materials, the wear and tear of the walls, the performed maintenance and upgrade work, the companies mandated for the work, the 2D and 3D model, the air quality, the temperature and humidity history, the tenant and owner, the neighbors, the regulatory/legal rights and obligations (both statutory and contractual) — everything is digital, and since everything is digitally linked to the house, everything is instantly available at the press of a button.

Second, ***digitalization has simplified the process of creating rights to assets (tradable rights to assets)***. Asset owners can readily create new rights to their assets.[19] The pro-

15 Take AirBnB, which has helped people better monetize their apartment and individual rooms since the late 2000s.
This motivation is especially strong for those struggling to make a living with their jobs. A large portion of the population may fall into this category if the 'gig economy' and 'job/process automation' continues its course. Observe also that the millennial generation is the first generation to be worse off than their parents; see e.g. Christopher Kurz, Geng Li, Daniel J. Vine, 2018, Are Millenials Different?, FEDS Working Paper No. 2018-080.

16 See Chapter 3 for a detailed definition and list of examples of 'digital assets'.
It has been forecasted that all non-digital assets, tangible and intangible, will be digitally represented (digital representation of everything). This complete digital copy of the non-digital world has been referred to as 'mirrorworld'. See Kevin Kelly, 2019, Welcome to the Mirrorworld, Wired (March 2019).
Examples of native digital assets include crypto-assets (e.g., Bitcoin or Ether), virtual luxury goods (e.g., clothes for an avatar, clothes on a digital picture of you), usage rights to digital books and movies.

17 Most notably, technological advances (automation, AI) have substantially reduced the costs of publicly issuing investable assets. Generation of legally-required issuing documentation is automated (and reduces the costs of fulfilling the regulatory prospectus requirement for public issuing of securities).

18 Connectivity may, for instance, be over the internet (Internet of Things, IoT) or over Bluetooth.
Non-digital assets contain chips for at least two reasons. First, because these chips allow us to control the asset from a digital UI (e.g., unlock your car or start playing a song on a radio from your smartphone, voice interface, or AR glasses). Second, because these chips allow us to monitor the state of the asset (e.g., to allow for preventive maintenance).

19 If the digital ledger, which registers the ownership of rights to these (digital and non-digital) assets, runs on distributed ledger technologies (DLTs), then we refer to 'creating rights to assets' as 'asset tokenization'.

Freedom to Generate, Right to Control, and Ability to Monetize

cess is end-to-end digital and highly automated ('one-click'). Machines have replaced human lawyers in reviewing contractual terms and conditions, slashing costs and time.

Third, ***digitalization has simplified the process of issuing rights[20] and has permitted reaching a global customer base***, thus making it significantly more attractive for asset owners to make their assets investable. Digital platforms facilitate issuing, lending, sharing, trading, and collateralization of rights — to (digitized, native digital, or underlying non-digital) assets — without geographic boundaries.[21] Before digitalization, globally distributing of the so-created rights entailed asking your network and your network's network; or it entailed engaging the help of professional brokers/gatekeepers who could charge (monopolistic) fees — but even then, you would not have had the digital platforms' global reach, capturing even the last bit of the long tail.

Everyone can seamlessly create rights to their assets and issue/offer them to a global customer base. This has led to an **explosion in rights to (digitized, native digital, or underlying non-digital) assets[22] — and therewith to an explosion of investable assets** (aka 'investable financial instruments'). This explosion may lead to new asset/investment classes, but need not do so.

Examples of investable assets include:[23]

- Ownership rights to a piece of land,[24] art, luxury goods, in-game virtual objects,[25] virtual luxury goods,[26] crypto-assets,[27] crypto-currencies,[28] etc.
- Usage rights to your personal data,[29] usage rights to data[30] (data-as-digital-assets).[31]
- Usage rights of your home or extra bedroom,[32] your boat, your car, your car with you as a driver,[33] your private jet, your pool, your spare garage space, your unused rooftop, your empty lawn or backyard space, etc.[34]
- Usage rights of some billboard at some future sports event or some spot on a website (advertising rights),[35] of some place in some future movie (product-placement rights).
- Priority rights to some future product.[36]
- Rights to a share of proceeds from a legal case (that has not yet been decided), of revenues of some specific product line, of your future revenues (after graduation).
- Ownership rights and (commercial-)usage rights to intellectual property (e.g., patents, trademarks, copyrights), or to digital data.

---

20 Technological advances (automation, AI) have substantially reduced the costs of publicly issuing investable assets, see footnote 12.

21 Take AirBnB, which has helped people better monetize their apartment and individual rooms by giving them access to the global market of home seekers — enabling home owners to issue/offer 'usage rights to their apartment' to a global market.

22 See Chapter 3 for a detailed definition and list of examples of 'digital assets'.

23 For a more extensive list, see the discussion on 'explosion in digital assets' in the most likely scenario of SFTI, 2019, Future of Financial Institutions.

24 In Switzerland, SIX Terravis is the electronic information portal for land registry data.

25 In 2018, the popular online multi-player game 'Fortnite' made over 2bUSD in revenues from selling in-game items and from selling its virtual money ('V-Bucks'). See e.g. Business Insider, 2019, How much money is 'Fortnite' making? Nearly $2.5 billion in 2018 alone, according to the latest report (16 January 2019).

26 For example, to be used to change the appearance of one's avatar, or to be used as a filter on your digital photos. Indeed, "If your platform of communication is digital, why can't your clothes be? ... But how does one 'wear' the couture? There is a 28-day window for the couture's new owner to provide a photo of the future wearer to the creators in order for them to custom fit the digital garments." (Forbes, 2019, World's First Digital Only Blockchain Clothing Sells For $9,500, 14 May 2019).

27 Crypto-assets are defined as digital assets issued on some permissionless distributed ledger (see the text preceding footnote 168 for the definition). See more generally the alternative scenario 'Crypto-assets everywhere'.

28 Crypto-currencies are a special type of crypto-assets. Examples of crypto-currencies include Bitcoin (BTC), issued on the Bitcoin blockchain, and Ether (ETH), issued on the Ethereum blockchain.

29 This is nothing new: We have all been paying with 'usage rights to our data' for services such as Gmail and Facebook.

30 This is nothing new: Remember that a key component of financial information involves creating, selling, and enforcing 'usage rights to data' in the investment sphere.

31 There is an infinite number of data-based assets because they can be defined very narrowly as 'specific usage right of some specific piece of data for some specific amount of time for some specific purpose'.

32 Think AirBnB.

33 Think Uber, Lyft, Didi Chuxing.

34 For more examples of this 'sublet economy', see Wired, 2019, Welcome to the 'Airbnb for Everything' Age (3 October 2019), "Call it the sublet economy. Everything you own can become a source of extra income, and everything you want to rent can be leased from a friendly stranger."

35 Selling 'usage right to some spot on a website' has been the core business model of some of the best-known big tech companies (read: Google and Facebook). They run mini auctions for the 'usage right to advertising spots' on their digital services/websites.

36 Perhaps most famously: Tesla's pre-order campaigns.

Freedom to Generate, Right to Control, and Ability to Monetize

Investable assets build on one another, acting as springboards for yet other novel investable assets. For example, by combining the investable asset 'usage rights to your roof' with an urban gardening service producing and selling seasonal vegetables. By combining the investable asset 'usage rights to your backyard' with a cottage-style studio apartment. Or by combining 'usage rights to data' with proprietary knowledge/IP to build new data — 'derived data'. All three examples may result in new investable assets (e.g., ownership rights, usage rights).[37]

Shift to the East

The center of economic gravity has continued shifting eastward. Home to more than a third of the world's population, APAC economies have continued to catch up to developed economies. APAC's continued growth has pulled the center of economic gravity toward Asia.

The precise intensity of this shift remains unclear. It remains to be seen how developing economies will be affected by a reduction of global supply chains as countries re-on-shore production thanks to advances in automation and 3D-printing. It is also unclear whether Western countries will shift their electronics supply chains back home for fear of tampering with the devices on which critical national infrastructure runs (cyberattack concerns).[38]

Ib. Data sources

Explosion in Digital Data, but Hidden

Ever more digital data is produced and collected. This has been ongoing for a while, but the **tipping point in the exponential growth curve has finally been reached**. The world produces and collects more data in a day than it produced before the start of the 21st century.[39] A key difference is that whereas **most of the world's produced data used to be ephemeral — it is now digitally collected and stored**. But **the majority of this digital data is hidden/private (e.g., encrypted, edge)**.

The **sources of this digital data are as broad as they are diverse**.[40] Contracts are entered and signed in digital form. People wear sensors in all shapes, forms, and places for self-optimization and self-monitoring. Social interactions take place in the virtual sphere (chat, VR). Real world experiences are augmented with a digital layer (voice interfaces and/or AR) to provide additional information and to interact with the objects themselves. Furthermore, AR devices record, analyze and digitally store their surroundings. Self-driving cars' computer-vision cameras film and store everything and everyone they pass on the street. Clothes tell washing machines how to treat them. Games are played online on mobile devices and fully-immersive environments (VR). Movies are interactive and thus produce even more behavioral data.[41] Cities are riddled with sensors and cameras (smart cities) and internet-connected devices (IoT) to monitor and optimize. Devices in homes have digital capabilities such as voice interfaces and internet connectivity (smart homes). Machines and product lines in factories have exact digital copies to constantly monitor their status and predict maintenance (to minimize downtime). Tractors combine satellite and drone images with on-board cameras to optimally spray fertilizers. The promise of fully tailored services furthermore prompts people to give away even more digital data about themselves. **Whatever we do, we create digital data**. Virtually all customer journeys are embedded in a digital ecosystem.

---

37 The urban gardening service may, for example, issue ownership rights to its business and/or usage rights to its produce. Consider also the start-up Rent the Backyard: It builds cottage-style small houses in people's empty backyards, which it then rents — in other words, it sells 'usage rights to a cottage-style small house in someone's backyard'.

38 Besides crippling critical infrastructure, risks include theft of high-value corporate secrets (intellectual property e.g.) and access to sensitive government networks.

39 The data produced in 2017 and 2018 amounts to 90% of the world's data. See Forbes, 2018, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read (22 August 2018).

40 Some forecasts put the number of internet-connected devices (IoT) by 2035 at one trillion — one hundred per human being. See, for instance, Economist, 2019, Connected Computers: Chips With Everything (14 September 2019).

41 Interactive films give watchers choices during the movie (e.g., 'Bandersnatch' of the Black Mirror series on Netflix). The moments are arguably chosen to maximize behavioral insights from the watcher's choice: "Do we seek chaos? Play it safe?". See Wired, 2019, Netflix and Choose (21 January 2019).

Freedom to Generate, Right to Control, and Ability to Monetize

Data owners **want to keep their data hidden/private** because of privacy concerns[42] and/or because they want to optimally monetize their data.[43] Where companies do offer insufficient data privacy, customers may not only switch to competitors exhibiting privacy preservation as a core value ('privacy by design'),[44] they now also have at their disposal a large arsenal of do-it-yourself privacy-preserving tools.[45] People can, for example, employ one or more of the following strategies. They can keep their data at the edge: The data is collected, stored, and processed solely on the local device.[46] They can generate noise to hide their data ('differential privacy'): The local device generates noise before sending the data out.[47] And they can impose end-to-end encryption of their data: They switch to an end-to-end encrypted communication service, which encrypts the raw data on the local device before any other system can access the data (not even the service provider can see the raw user data).[48]

Companies have strong incentives to build their digital services upon privacy-preserving technologies that keep their users' data hidden/private. Users may shy away from service providers not offering privacy-preserving services despite the aforementioned DIY means of data-privacy protection. Governments may enact consumer-protection laws in the form of strict liability, making companies responsible (even in the absence of negligence or ill intent) for damages caused to data subjects from the data that these companies collected. And governments may impose data-collecting companies with

---

42 Having been lured into the digital sphere by the promise of free services, immediate reward and convenience, people have experienced firsthand the costs of too casually trusting others with their data.
The year 2019 marked a watershed moment for digital data privacy and security. It was the year the iPhone was hacked during a simple visit to a website. Hackers could monitor live GPS data, grab pictures, turn on microphones, grab passwords and access tokens, or read end-to-end encrypted communication (since the data is decrypted on the sender's and receiver's devices). This changed everything: Conventional wisdom was that only high-value targets (e.g., journalists, lawyers, activities) were really at risk because the costs of the high costs of such a hack (1-2mUSD). Now, it was clear that anyone was at risk even on what was considered the safest device. See e.g., Wired, 2019, Mysterious iOS Attack Changes Everything We Know About iPhone Hacking (30 August 2019).
People have seen their data being sold to third parties, at times in non-anonymized form. People have seen their data being used to manipulate their own choices and actions, from purchase decisions to voting. People have seen sensitive personal data being made public and used for blackmailing. People have seen employees analyze their data, from emails to voice. People have seen their data treated with little care, lying around unprotected on company servers for employees to snoop through. And people have seen their data being misused by companies themselves or their employees. Uber employees could easily track users' whereabouts using a so-called 'god mode'. Several former employees of Twitter have been charged in the US with spying for Saudi Arabia, collecting user data and tracking government dissidents. See, for instance, Wired, 2019, Twitter Insiders Allegedly Spied for Saudi Arabia (6 November 2019).
For more details, see the discussion on 'Increased importance of trustworthiness' in the most-likely scenario of SFTI, 2019, Future of Financial Institutions.
Earlier empirical data and experiments suggested that people were mostly unwilling to pay modest amounts for privacy-preserving features, or to take the additional steps of selecting privacy-preserving preferences in digital applications and services (e.g., encrypting their data). See e.g., Leslie K. John, 2019, Uninformed Consent, HBR: The Big Idea (September 2019), noting that people were likely driven by immediate, tangible and specific reward and convenience, coupled with a false sense of control over their data usage/access, as well as with an extreme discounting of possible future abstract costs related to privacy loss (if not unawareness of possible costs).

43 Keeping their data private increases the value they can extract from it by selling ownership/usage rights to third-parties (data-as-digital-assets).

44 Supporting the approach of embedding privacy in the foundation is the inventor of the world wide web, Sir Tim Berners-Lee "We have to imagine a world in which any data you create is under your control … By default you will control your data. By default it will not be shared with anybody." (FT, 2019, The people, not governments, should exercise digital sovereignty, 25 November 2019).
In 2019, Facebook announced it will shift towards an end-to-end encrypted communication model. Its CEO and founder, Mark Zuckerberg, believes that users will increasingly demand such end-to-end encryption "As I think about the future of the internet, I believe a privacy-focused communications platform will become even more important than today's open platforms" noting that signs for this shift were already apparent "we already see that private messaging, ephemeral stories, and small groups are by far the fastest growing areas of online communication" (Mark Zuckerberg, 2019, A Privacy-Focused Vision for Social Networking, Facebook, 6 March 2019).

45 An entire privacy-preserving industry has sprung up to address this need.

46 Think of the time when you used Microsoft Windows before the internet. Think of your touch ID or face ID on the iPhone where the biometric data is only stored and processed locally. Think of some smart-home applications which you don't want to be connected to the internet. This more generally captures what is referred to as 'edge AI'.

47 When asking a question on Google search or to Amazon's Alexa, the local device could randomly generate many alternative questions and send all of them simultaneously out for processing by Google or Amazon. When searching for a product on Amazon, many randomly generated search requests could be sent out, and when clicking on a product, many different product selections could be sent out. The local device would act as an intermediary layer with the random alternatives being generated on the local device itself (i.e., at the edge).

48 In the e-commerce space, this could look as follows: A user could start (possibly in full anonymity, behind a VPN) their journey on Amazon's e-commerce platform to find a product. The user may then seamlessly switch to an end-to-end encrypted communication channel in order to directly contact a seller and bilaterally agree on the terms (without Amazon ever knowing about any of this). The user may finally engage a third-party payment service to transfer the money to the seller. (Insofar as the seller uses Amazon's warehouses and logistics, Amazon would however eventually know about the sale.)

Freedom to Generate, Right to Control, and Ability to Monetize

fiduciary duties, compelling them to behave in a trustworthy manner with people's data.[49]

Data Sovereignty Shifts Toward Data Subjects

Data subjects have extensive rights and control over the data they produce. Individuals can **forbid service providers from using their data** because governments have granted individuals broad rights over their digital data.[50] And individuals can **provide third parties with access to their data (data mobility)** because governments have required service providers to provide APIs for third parties to access their users' data.[51]

Western countries with their history of liberal values, belief in competitive markets, and respect for private property took the lead: They established and enforced strong property rights for data subjects in the digital sphere. Contrary to what had oftentimes been advanced, giving data subjects extensive rights over their data did not put Western countries at a competitive disadvantage — just as slavery was not necessary for economic development, nor was allowing corporations to exploit people's data. Western corporations made less profits because they had to compensate/pay people for the 'usage rights to their data'.[52] But this only amounted to a shift of some of the profits of corporations to data owners, who then funneled those profits back into the economy by investing it back into corporate ventures or by increasing their consumption.

Importantly, **shifting data sovereignty/ownership to data subjects does not imply that all profits flow to data subjects and none to corporate ventures downstream in the supply/value chain**. Corporate ventures relying upon third-party data as input may still generate and capture profits if they combine this data with unique tangible/intangible[53] capabilities.[54] The situation is akin to how oil producers (data tends to be considered the

---

49 Many scholars argue that providing data subjects with 'opt in choice' (e.g., in the EU-GDPR, see footnote 46) is insufficient. See e.g., Leslie K. John, 2019, Uninformed Consent, HBR: The Big Idea (September 2019), "A common approach is to require firms to give consumers information on the relevant costs and benefits of sharing … It's unlikely to solve the problem given that users don't read privacy policies … [resulting in uninformed consent to processing one's data. Instead we should give] firms an incentive to use consumers' personal data only in reasonable ways … Interventions such as these would give firms a sincere interest in responsibly using data and in preempting abuses and failures in the system of data collection and sharing (because otherwise they'd face financial penalties)."

50 Governments are likely to increase the rights/sovereignty of data subjects over the digital data that they produce.
An early-mover was the European Union in 2018 with the entry into force of the EU General Data Protection Regulation (GDPR). It requires service providers to request consent from data subjects for any type of processing of their data ('opt-in'). Europe's actions have global reach: "The big five tech giants, Alphabet, Amazon, Apple, Facebook and Microsoft, make on aver-age a quarter of their sales there. And as the world's biggest economic bloc, the EU's standards are often copied in the emerging world." (Economist, 2019, Europe takes on the tech giants, 23 March 2019).
The California Consumer Privacy Act of 2018 (AB 375) goes even one step further (the law goes into effect on January 1, 2020). It prevents businesses from unfairly penalizing consumers who refuse to opt in, though they will be able to charge a fee that makes up for the lost data usage. The purpose is to prevent businesses from imposing the 'opt-in' by offering a sole alternative to 'opt-out of the service entirely'.

51 Governments are likely to mandate 'data mobility' by requiring service providers to provide APIs. Data subjects will then be able to provide third parties with access to their data.
An early-mover was once again the European Union in 2018 with the entry into force of the EU General Data Protection Regulation (GDPR). It requires service providers to allow data subjects to export their data in standardized ('data portability').
Some regulations in the 2010s already went further than simple 'data portability' by providing data subjects with the right to give third parties access to their data held in third-party systems ('data mobility'). An early-mover was again the European Union in 2018 with the entry into force of the EU Payments Service Directive 2 (PSD2). It requires banks to provide communication interfaces for third parties to access bank account information. A third party has access only if the account owner (data subject) consents to it. The UK Open Banking Regulations (entry into force 2018) go one step further by additionally requiring access to product data (e.g., fees, charges, lending rates to the customer). And the Australia Open Banking Regulation (entry into force 2019) goes even further by requiring access to any customer data they hold. Both regulations again require that the data subject consents to a third party accessing the data.
A bill proposed in 2019 in the US would mandate 'data mobility' for large digital platforms having over 100m monthly active users in the US. See 'Augmenting Compatibility and Competition by Enabling Service Switching' ('ACCESS Act of 2019').

52 Where competition is high from foreign players that have access to free data due to lack of data-sovereignty laws and regulations in their home countries, local companies will not be able to pay a high price to data owners for access to their data. Data owners may even provide usage rights to their data for free in order to enable local companies to compete with foreign players, creating local employment in the process.

53 It has been observed that intangible assets/capabilities have replaced tangible assets (e.g., physical infrastructure) as the primary profit drivers in the twenty-first century. See e.g. Jonathan Haskel and Stian Westlake, 2018, Capital Without Capital: The Rise of the Intangible Economy (Princeton University Press: Princeton, NJ).

54 Unique intangible capabilities/knowhow (or 'unique intellectual property') may take the form of unique skills, data, algorithms, software, design, network, scale, and brand.
Uniqueness may result from, among other things, one's human capital (e.g., culture, talent pool), one's legacy/history, secrecy (e.g., Coca-Cola formula), and legal exclusivity in the form of intellectual property rights (e.g., patents providing temporary exclusive rights in exchange for public disclosure of an invention, copyrights providing temporary exclusive rights to a creative work, trademarks, or database rights).

Freedom to Generate, Right to Control, and Ability to Monetize

'new oil')[55] do not capture all the profits of the supply/value chains including oil as inputs.[56] How much profits accruing throughout supply/value chains that data owners can extract will depend on their bargaining power: If their data is truly unique,[57] then they may extract more of those profits (e.g., by fixing the price of usage rights as a share of the profits accruing throughout the supply/value chain).[58]

Contrary to what is oftentimes (implicitly) assumed in discussions about the ongoing shift toward a 'data economy', we do not expect the raw data by itself to be the main value driver in this future economy. Instead, we expect most value creation to be driven by the players that invent on top of this data, combining and expanding the data with their unique capabilities.

Crowd-Sourced Data

The crowd itself has increasingly become an important data source. Everyone can control access to, and usage of, their data: Data subjects can forbid service providers from using their data and can provide third parties with access to their data.[59] Services providers themselves might not even see the (anonymized) aggregated activity data of their services.[60] Digital UIs furthermore enable anyone to collect and distribute data in real time, anytime, and anywhere.[61] In parallel, the advent of privacy-preserving data distribution systems has increased people's willingness to provide access to their data.[62]

Increase in Publicly and Freely Accessible Data

Besides giving data subjects more rights and control over the usage of their data, **governments have concurrently required opening up ever more data to the public in privacy-preserving machine-readable form ('open data policies')**. Anyone can query the data. Where the data contains personally identifiable information, data-distribution systems allow data to be processed while ensuring data security and privacy.[63]

This development most notably includes *government data*, from commercial register, to legal identifiers, country statistics, decisions by tribunals, weather and pollution data, data from cameras and satellites, and the many other sensors that pervade our world.

In addition to the data they produce themselves, *governments have also mandated private corporations to make some of their data publicly accessible*. Early examples of such practices are trading venues' trading data,[64] and large German

55 Others have instead compared data to labor — 'data as labor', see Jaron Lanier, E. Glen Weyl, 2018, A Blueprint for a Better Digital Society, HBR: The Big Idea (September 2019).

56 Or take steel: 1kg of steel may cost 5USD, while a horseshoe may be sold at 50USD and a watch spring out of steel even at 500USD.§

57 Most individual data points are unlikely to be unique from the data users' point of view because data users need vast data sets as inputs. The effect of one data subject holding out by refusing to share their data is thus marginal. The situation would, however, be different if data subjects join forces, for example mandating a third party to negotiate the 'usage rights to the aggregate data' on behalf of the group (advocating for such third parties are e.g. Jaron Lanier, E. Glen Weyl, 2018, A Blueprint for a Better Digital Society, HBR: The Big Idea, September 2019, "we need an additional layer of organizations of intermediate size to bridge the gap. We call these organizations 'mediators of individual data,' or MIDs. A MID is a group of volunteers with its own rules that represents its members in a wide range of ways. It will negotiate data royalties or wages, to bring the power of collective bargaining to the people who are the sources of valuable data").
In any event, most data points are unlikely to be truly unique: There is likely an (imperfect) substitute which contains similar informational content. Aggregate geo-location data from smartphones may, for example, be substituted by data from a satellite and/or street camera.

58 Increased transparency and traceability throughout supply/value chains may allow following an input throughout the supply/value chain.

59 See footnotes 46 and 47, and the text surrounding them.

60 See footnote 38 and the text surrounding it.

61 A picture taken with a smartphone from a burning building during the holidays may contain valuable information.
Consider also Thomson Reuters' specifically built crowd-sourcing data app: It devised a solution that allows farmers to upload data on the crops they planted and to provide updates on the condition of their crops. Farmers are paid with access to aggregate data combined with trends and weather reports. See Thomson Reuters, 2016, New Thomson Reuters Mobile App Uses Crowdsourcing to Deliver Commodities Insight (30 August 2016), "The ['Data Share'] app is designed to aggregate unbiased, raw data to generate more accurate crop forecasting and supply chain evaluation, helping the farmers to make more informed decisions."

62 See Section 'IIc. Delivering issuing and investment decision support'.

63 See the discussion on 'Secure and privacy-preserving data distribution' in Section 'IIb. Helping monetize data'.

64 The European Union's Markets in Financial Instruments Directive II' (EU-MiFID II), which entered into force in 2018, required such free public availability in machine-readable form within 15 minutes for certain financial instruments.

Freedom to Generate, Right to Control, and Ability to Monetize

insurers' data.[65] Governments were mainly driven by consumer-protection and anti-competition considerations (levelling the playing field). To not destroy innovation and competition by taking away the incentive to invest in the first place,[66] governments are likely to adopt a case-by-case approach that considers the size, maturity, service-operation duration, and market position of the service provider.

Explosion in Theme-Related Information

There is data allowing investors to evaluate investable assets in any dimension, helping them to better tailor their investments to their preferences: They can deploy their capital in alignment with themes that capture their preferences, and evaluate their invested capital based thereon (theme-based investment). Investors have considered (or avoided) exposure to themes from blockchain, to quantum computing, cement-based construction, cybersecurity, solar energy, Apple's supply chain, specific ML algorithm development or deployment, video gaming, and to weapons. This type of data has been referred to as theme-related information.

Democratization of Access to Data

The explosion in sensors, ubiquity of digital UIs, and advances in technologies (e.g., AI, robotics, digital platformification) allow collecting and sharing digital data at much lower costs and latency. This has led to a **reduction in the price of access to data**, democratizing the access to data.

As seen before,[67] governments have granted **sovereignty over the data to data subjects**. This has put all data users — including those providing the digital services wherein the data is generated — on equal footing since they all have to buy the rights to use the data from the data subjects.

Additionally, **governments have aimed at ensuring equal access to data for everyone** to further competition by levelling the playing field. Governments have at times prohibited exclusive usage/access to data sets:

- They have required some companies to make their exclusive proprietary data accessible to third parties against compensation, sometimes even requiring free public availability.[68]
- They have prohibited exclusivity agreements between data producers and data users.[69]
- And they have broken up vertical supply/value chains, carving out data-producing entities, to further downstream competition through equal access to data.

Governments may, for instance, prohibit banks from exclusively using their data on payment flows to trade. Or they may require large trading firms to sell off their personal satellites that could give them exclusive access to data.

Ic. Investors

Rise in Investable Capital and in the Number of Investors

The global demand for investable assets continues to increase—global AuM continues to grow.[70] The **proportion of the population investing their capital has increased substantially**. This development was driven by the democratization of the investment space (ETFs, index-tracking funds, robo-advisors, robo-funds, increased financial literacy, zero-trading-fee brokers, direct-access zero-fee online trading platforms, digitalization of investable assets ,[71] democratization of access

65 In Germany, large insurers must provide smaller competitors access to their data to help these smaller companies assess risks, see e.g. Viktor Mayer-Schönberger, Thomas Ramge, 2018, A Big Choice for Big Tech: Share Data or Suffer the Consequences, Foreign Affairs (September-October Issue).

66 The rationale is the same as for intellectual property rights: Players are given an exclusive commercial usage right for a period of time in order to provide enough incentives to them to invest in the first place.

67 See Subsection 'Ib. Data sources'.

68 See footnote 61 and the text surrounding it.

69 FT, 2017, Hedge funds see a gold rush in data mining (28 August 2017), "'exclusivity' agreements with providers, are attracting the interest of regulators and prosecutors concerned that hedge funds are getting an unfair market advantage ... In 2013, under pressure from Mr Schneiderman [the New York Attorney-General], Reuters stopped providing some exclusive content to its premium subscribers."

70 Global AuM has risen from 27tUSD in 2002 to 79tUSD in 2017. See e.g. BCG, 2018, Global Asset Management 2018: The Digital Metamorphosis (July 2018), page 6.

71 See Section 'Ia. Investment universe'.

Freedom to Generate, Right to Control, and Ability to Monetize

to data and information)[72]. Further drivers were an aging population and a *loss in trust in pension funds'* ability to meet their future obligations. Finally, the *reduced wealth prospects from labor*[73] has also driven people into the investment space with the hope of capturing some of the wealth created by the economy — investment has become something of a national pastime.

Changing Demands and Preferences

24/7 availability, instant information access, perfect tailoring, unbundling, digital UIs, mobile, peer ratings and validation (social), augmented reality, virtual reality, voice interface, one-stop shops, and omni-channel have become widely expected by investors. Influenced by their experiences with global tech companies in other areas of life, investors have come to expect the same quality of user experience in the trading area.

Investors demand **traceability** of the underlying data. Investors expect a **high level of transparency** regarding where and how their capital is being used (e.g., how companies use the capital, how funds invest the capital).

Non-listed investment classes[74] are likely to substantially increase in popularity.[75] Investing in younger companies and/or private companies is a more stimulating/interesting experience and is perceived as qualitatively different from investing in large public companies because individual investors can actually have an impact.[76]

Crypto-assets are not dominant but continue to be demanded as an investment class. The permissionless distributed ledgers, whereon crypto-assets are registered, have not become dominant.[77] Crypto-assets have nonetheless kept some popularity as an investment class (e.g., for hedging or speculation).[78]

Alternative Data as Key Input for Investment Decision-Making

All this new data,[79] sometimes referred to as 'alternative data', is increasingly recognized as not only amounting to noise, but as containing **valuable input for investment decision-making**. Social sentiment, social media, internet-of-things data, sensor data, public internet data — they all amount to relevant inputs for investment decision-making. The label 'alternative data' has disappeared as these 'new' data sources have entered mainstream investment input. **Alternative data has established itself alongside traditional financial information** as key input for investment decision.

As new types of assets become investable,[80] further data types and sources may become relevant inputs for investment decision-making.

Societal-impact and sustainability considerations have substantially increased in importance in investment decisions. Investors consider social, environmental, governance, and ethical aspects besides financial returns. Younger generations of investors are reportedly

---

72 See later in this Section for an explanation.

73 See footnote 10.

74 A *listed* financial product describes a product that fulfills the 'listing criteria at an Exchange'. These listings criteria contain additional requirements to what regulators require for a financial product to be issued to the public. Investors may view these 'listing' as a signaling device for higher quality.

75 This describes a world between our most likely scenario ('listed financial products remain dominant') and our second-most likely scenario ('non-listed financial products become dominant') in SIX, 2019, White Paper: Future of the Securities Value Chain (January 2019).

76 FT, 2019, Why the wealthy are investing directly in private companies (16 June 2019), investors "find them a more 'beneficial and stimulating' experience than 'sitting around a table each quarter with investment managers and trustees listening to why a portfolio of equities and bonds have gone up or down in value.' ... [and] an individual can get involved in the business and help shape its strategy".

77 See the alternative scenario 'Crypto-assets everywhere' for an assessment of the conditions under which we can expect permissionless distributed ledgers (e.g., 'Bitcoin blockchain' or 'Ethereum blockchain') and crypto-assets to become dominant.

78 Fidelity, one of the world's largest asset managers, started offering access to crypto-assets to its institutional investors in 2019.

79 See Section 'Ib. Data sources'.

80 See also Section 'Ia. Investment universe'.

Freedom to Generate, Right to Control, and Ability to Monetize

more social and environmentally conscious.[81] As wealth transfers to these younger generations, these considerations become more important in global capital allocation.[82] **Investors thus increasingly demand information on those dimensions**.

Strong Delegation of Investment Decision-Making

Non-professionals have continued to take investment decisions themselves to act on their senses and experiences. They may for instance decide to invest in a new coffee shop in the neighborhood after tasting a fantastic cup of coffee. They may decide to invest in their favorite local bakery, in a friend's new business venture over lunch, or in a real-estate property during a Sunday walk with the family. Nonetheless **most of their investment decisions have been delegated to professional asset managers** (e.g., funds, collective, or individual mandates).

Tailored robo-funds have substantially increased in popularity as asset managers. These robo-funds[83] are fully tailored to investors' preferences and risk profile in real-time (i.e., they continuously adjust/update their positions) — these fully-individualized funds have been referred to as **'funds of one'**.[84] Depending on an investor's preferences, these robo-funds invest indirectly via passively managed funds (e.g., ETFs) or actively managed funds (e.g., VC funds), or invest directly into individual assets.

Funds may no longer issue shares. Investors may directly own the underlying investment assets rather than owning shares in an intermediary fund.[85] This could occur if transaction costs fall to zero[86] and if investable assets are partitioned into small pieces (fractionalization).[87] If so, it becomes economical and viable to buy the individual underlying investable assets — rather than shares in an intermediary fund — irrespective of an investor's portfolio size. Such a development would somewhat reduce the number of investable assets.

Machines Permeate Asset Management

Active management of assets[88] has survived because humans continue to create added value.[89] We identify two such instances: when humans have access to data that machines have not integrated (yet);[90] and/or when

81 See e.g. US Trust, 2014, Annual survey of high-net-worth and ultra-high-net-worth Americans, page 12, "Four in 10 [wealthy US millennials] agree that investing is a way to express their social, political, and environmental values" and page 13, "75% of [wealthy] Millennials … consider the social and environmental impact of the companies they invest in to be an important part of investment decision-making"; Bloomberg, 2018. Sustainable investing grows on pensions, millennials.

82 BCG, 2017, Global Asset Management 2017: The Innovator's Advantage (July 2017), page 24, "Responsible investing grows from niche to mainstream".

83 We define robo-funds as funds wherein an algorithm takes the final investment decision (i.e., automated algorithmic trading). Historically, the most notable types have been: high-frequency traders (HFT); index-tracking funds. Notice that both types are not tailored.

84 See e.g., WEF, 2018, The New Physics of Financial Services (August 2018), page 147.
Robo-funds can be both, actively-managed or passively managed (see footnote 84 for the definitions). Examples of passively managed robot-funds: 'Index-tracking funds' simply copy an index and therefore involve no 'human investment decision-making'; 'Machine-designed funds' are funds wherein machines themselves design the trading algorithms (e.g., neural nets, deep learning) without any human involvement.

85 This model of direct ownership is similar to what used to be referred to as 'social trading' or 'copy trading': against a fee, investors could copy the buy/sell orders of a lead trader.

86 Reduction in transaction costs is driven by increased competition: Higher transparency and lower switching costs allow issuers and investors to easily join different issuing and trading venues; and new competitors offering zero-trading-fee services.

87 Fractionalization was always technically feasible — regulations made fractionalization in many instances too costly. Technological advances have reduced the costs for compliance with issuing regulations by automating virtually all processes (e.g., issuing prospectus for public offerings of securities).

88 We define *actively managed funds* (as opposed to 'passively managed') when humans are involved in the investment decision-making. This captures (i) *funds wherein humans make the final investment decision and/or* (ii) *funds wherein humans are involved in defining the investment strategy or in selecting individual assets*. In (ii), human-chosen rules may then be coded by humans in the form of trading algorithms — referred to as *machine teaching*. Most notably, trading algorithms that decide what to buy and sell based on what are known as 'factors' such as momentum (recent price rise) or yield (high dividends).
Passively managed funds started out as simple index-tracking funds, and are currently expanding into algorithms that design their own investment strategies by analyzing the data without any human guidance. Notable players in this field are the quant funds Two Sigma and Renaissance Technologies (see e.g., Economist, 2019, March of the Machines, 5 October 2019). Note that human involvement is still possible in passively managed funds, just not in the investment decision-making: Humans may be involved in defining the algorithms for assessing investors' individual preferences and risk profiles, and they may be involved in defining/selecting the data inputs.

89 Non-specialty actively managed funds (or 'plain-vanilla actively managed funds') had already seen their share of global AuM plummet from 57% in 2003 to 33% in 2017, while all other classes of funds were constant or increasing. See e.g. BCG, 2018, Global Asset Management 2018: The Digital Metamorphosis (July 2018), page 11.

90 For instance, data out of direct (non-digital) human interactions. Note that for a (creative) interpretation of some digital data to be beyond robo-advisors, the interpretation process must itself rely on data that robo-advisors have not integrated.

Freedom to Generate, Right to Control, and Ability to Monetize

uniquely human factors impact the performance of the assets under management.[91]

Where algorithms take the final investment decision ('robo-funds', 'systematic trading', 'quant funds'),[92] humans may be involved in devising the trading algorithms ('machine teaching'). And where humans take the final investment decisions, machines are always involved in devising the trading algorithms ('quantamental investing', 'non-automated algorithmic trading').

Specifically, active management is likely to survive where digital data sets are of limited size, where funds exert some control over their investments (e.g., PE funds, activist funds),[93] and where funds are operationally active in their investments (e.g., VC and PE funds).[94]

Survival of Non-Index-Tracking Funds

It has become widely known that only a small minority of non-index-tracking funds outperform market benchmarks.[95] The 2000s and 2010s saw a shift toward passively managed funds in the form of index-tracking funds.[96] This shift was primarily driven by the higher costs of non-index-tracking funds.[97] It is therefore **difficult to say how the share of AuM in index-tracking funds will evolve** if the cost advantage of these funds become marginal as asset managers deploy new technologies at scale. It will depend on the number of human investors believing in their own asset-manager-picking abilities (i.e., in their ability to pick the winners, whether humans or machines).

Non-index-tracking funds — whether actively or passively managed — will survive because index-tracking funds arguably overinvest in unattractive companies and underinvest in attractive companies, creating opportunities for active managers to take advantage of.

Increasing Outsourcing of Activities and Processes

Ever more activities and processes within investment decision-making are outsourced to benefit from economies of scale (**cost mutualization**) and to **source the necessary capabilities in new technologies**.[98]

Regulatory costs have remained substantial. Investors have **strongly outsourced activities in the regulatory space**: to counter the rising costs of regulatory compliance;[99] and to reduce the likelihood of non-compliance (avoid fines).[100] Regulatory solutions (e.g., RegTech), among others, automate processes, reduce the time/effort to understand new regulations, and deploy new technologies to avoid fines.[101]

---

91 For example, a start-up background — assessing the founder team, evaluating the strategy, evaluating the problem-to-be-solved, interpreting the results of experiments toward a product-market fit, gauging necessity and opportunities to pivot — combined with a broad network increases the chances of start-ups (e.g., venture-capital funds). Operational expertise with turn-around-management experience creates value for corporations (e.g., private-equity funds).

92 Economist, 2019, Masters of the Universe: Forget Gordon Gekko. Computers increasingly call the shorts in financial markets (5 October 2019), "Funds run by computers that follow rules set by humans account for … 60% of trading activity."

93 Seat on the board, substantial voting rights, etc

94 See footnote 87.

95 Between 2009 and 2019, only 24 percent of actively managed funds outperformed their benchmarks. See e.g. Bloomberg, 2019, Passive Funds Overtake Stock-Pickers in the U.S. Large-Cap Market (12 February 2019)

96 Passively invested AuM's share of global AuM increased from 9% in 2003 to 20% in 2017. BCG, 2018, Global Asset Management 2018: The Digital Metamorphosis (July 2018), page 11.

97 RFS, 2018, Nine Trends Shaping the Future of Managing Assets (November 2018), page 5, the primary driver is cost, but actively managed funds' performance (or lack thereof) is also a driver.

98 For a more detailed discussion, see the alternative scenario 'Middle- and back-office consolidation in finance'. Although the discussion there focuses on middle- and back-office activities, the arguments/rationales apply more generally.

99 The costs of keeping on top of regulations are exploding as the number of new regulations in the financial sector is constantly increasingly. Thomson Reuters reports that since 2004, regulatory updates have increased from about 10 to over 185 per day — one regulatory change every 12 minutes. Economist, 2019, The past decade has brought a compliance boom in banking (2 May 2019), "56,321 [relevant regulatory changes] were issued by 900 bodies in 2017 … At the end of 2018, some 30,000 (or 15%) of the 204,000 employees of Citigroup, an American bank, worked in compliance, risk, and other control functions … At the end of 2008 it was just over 4% of employees." Chris Skinner, 2016, America's regulatory issue is 'too many cooks', BankNXT (15 June 2016), "When Dodd-Frank first appeared in July 2010, it was already 850 pages. Three years later, this had ballooned to 13,789 pages and more than 15 million words."

100 "Regulators have fined financial firms at least $28.4bn for money-laundering and sanctions violations since 2008" (Economist, 2019, The past decade has brought a compliance boom in banking, 2 May 2019).

101 The global revenues of RegTech solutions is expected to growth from $1.4bn in 2019 to $6.4bn by 2025; see e.g. Economist, 2019, The past decade has brought a compliance boom in banking, 2 May 2019.

Freedom to Generate, Right to Control, and Ability to Monetize

At Scale Adoption of Secure and Privacy-Preserving Cloud Solutions

The cloud has become a viable end-to-end alternative to on-prem infrastructure. Cloud infrastructure is mature and stable; multi-cloud solutions are convenient and seamless;[102] and privacy-preserving systems have experienced substantial advances — most importantly in the form of **privacy-preserving advanced-analytics environments**.[103]

Investors have deployed cloud-based solutions at scale to **reduce costs, improve cybersecurity,[104] and to access new technologies**.[105] The fixed costs of operating an on-prem infrastructure have skyrocketed: Processing the explosion in digital data necessitates an advanced big-data analytics environment and vast processing power. Extreme spikes in usage of these assets mean they lie idle for most of the time.

Shift to the East

Investors have increased their investments in APAC economies. Attracted by the rapid growth of APAC economies, global investors have increasingly rebalanced their portfolio eastward. This growth has also meant that the **rapidly rising investable capital from APAC has mostly remained there**.

I. Financial Information Infrastructure

IIa. Making Assets Findable and Describing Them

Explosion in Uniquely-To-Be-Identified Entities

The explosion in investable assets[106] necessitates identifi**ability and description of an increasing number/ variety of assets and issuers**.

Even though everything that is needed to describe and define any asset is available in digital form at the press of a button,[107] this information may still need to be structured, aggregated, synthesized, interpreted and/or verified/certified.

IIb. Helping monetize data

The Rise of Decentralized Data Storage

The explosion in data volume makes complete central storage at data-distribution intermediaries or investors virtually impossible and arguably too expensive. Data privacy furthermore also calls for decentralized storage where the data is produced (see below).

Ever more data is stored decentrally on local devices (edge) and in cloud infrastructures, and sourced when queried. **Only the meta data model is centrally stored in its entirety** at data-distribution intermediaries to map all the centrally- and decentrally-stored data.

Decentralized storage was rapidly adopted by data-distribution intermediaries in the area of new (alternative) data,[108] with traditional financial information lagging behind because of incumbents' legacy data-distribution and data-access systems.

Technological limitations may (temporarily) necessitate central storage of some data at a trusted intermediary. Decentralized data storage is, for instance, infeasible if the communication network cannot handle the high volume of simultaneous data queries, or if it is unable to provide sufficiently-low latency (e.g., for high-frequency traders). Decentralized data storage is also prevented if infrastructure where the data is pro-

102 Due to interoperability and micro-services-based IT architectures.

103 Investors demand privacy-preserving analytics systems and algorithms to query data (knowledge of data usage may provide insights over their trading strategies) and to devise, calibrate, and update their trading algorithms

104 Increasingly sophisticated cyber threats.

105 Which could mean access to a quantum computer.

106 See Section 'Ia. Investment universe'.

107 See again Section 'Ia. Investment universe'.

108 See Section 'Ib. Data sources'.

Freedom to Generate, Right to Control, and Ability to Monetize

duced/stored does not exhibit a (sufficiently performant) data-analytics computing unit.[109]

New data created/derived (among others) from decentrally stored data sources may be produced on the fly, or may be stored with the creator of this new data. In both cases, the **derived data is stored decentrally** unless it is duplicated at a data-distribution intermediary or investor.

Secure and Privacy-Preserving Data Distribution[110]

Data owners/sources (people and corporations) have increasingly **demanded that data distribution systems ensure that their data be kept private/hidden**.[111] They are driven by privacy concerns and by a desire to optimally monetize their data.

Data privacy requires *'data to always be encrypted'*,[112] and *'data to never move'*[113] beyond what is required by the application/service generating that data. As such, data privacy not only mandates decentralized data storage, it states that **the 'raw data' itself should never be distributed, not even in encrypted form**.[114]

Data monetization, however, necessitates access to and processing of this data. Data-distribution systems crucially **build upon secure multi-party computation and federated AI to enable data processing while ensuring security and preserving privacy**.

- *Secure multi-party computation* ensures '(raw) data is always encrypted': It allows evaluating statistical functions while keeping the underlying data encrypted/private throughout the computation.[115]
- *Federated statistical algorithms*[116] ensure '(raw) data never moves': It allows data to be processed where it is stored — and only the result of the processing (e.g. aggregated insights, trained model parameters) is 'moved/distributed'.

Data-distribution systems even allow secure and privacy-preserving data processing even when the raw data

109 The volume of simultaneous data processing queries may be enormous. Without such a unit, processing of the raw data where it is stored is not possible. This instance is likely to reduce as computational units become cheaper and smaller, as analytics models become less computation intensive, and as evermore data is being produced and stored directly in clouds (which exhibit large computational units).
Note that in many instances, users will themselves already choose to have an encrypted backup of their local data to be stored in a centralized unit. Take the data on our smartphones: Most of us have elected to have it backed up in a public cloud.

110 Note that 'data distribution' is somewhat misleading. As we shall see, the 'raw data' is never distributed: The raw data is processed where it is stored, and only the results of this processing are distributed.

111 See Section 'Ib. Data sources' for a more extensive discussion.

112 Data transformation/manipulation techniques (e.g., data anonymization, data perturbation, data swapping, and data synthetization) cannot guarantee data privacy because of inference attacks.

113 See more generally: Thomas Hardjono, David Shier, Alex Pentland, 2016, Trust::Data: A New Framework for Identity and Data sharing (Visionary Future: Cambridge, MA), page 42, 'never decrypted data' and 'share answers not data'.

114 Data privacy goes beyond decentralized data storage because decentralized data storage does not prevent the (encrypted) raw data to be distributed — to move — in real-time when it is queried.

115 Homomorphic encryption is a strict subset of secure multi-party computation. There is a long tradition in homomorphic-encryption research, but only recent advances in computing power have made this technique possible/viable.
If the statistical function itself would reveal the underlying (raw) data, then it is for the data owner to decide whether they allow the processing — and (risk to) forego their privacy.

116 Federated statistical algorithms (aka: federated AI, federated machine learning) describes a machine-learning approach not requiring the data to be centralized in one place. It trains separate models in each location where the data is held (at the edge on a mobile phone, in some on-premise database, or in some public cloud), then sends all these trained models (i.e., the calibrated parameters) to a central server, and finally combines all these models into a master model. The raw data does not move and cannot be reverse-engineered from the trained models. See e.g., The Algorithm, 2019, A little-known AI method can train on your health data without threatening your privacy, MIT Technology Review (11 March 2019).
The start-up OWKIN (backed by Google Ventures) is deploying such an approach in the health-care space: the highly-sensitive data never leaves the hospitals premises.

Freedom to Generate, Right to Control, and Ability to Monetize

contains ex ante non-attributable personally-identifiable information,[117] when the raw data is not encrypted,[118] when the raw data' infrastructure is not connected to the internet,[119] or when the infrastructure of the raw data' infrastructure cannot itself check whether the querier owns the proper rights (see below).

Digitalization of Rights to Data

The creation of (ownership/usage) rights to data is fully digital and user-friendly.[120] The ownership of these 'rights to data' is stored in some **digital ledger**.[121]

Enforcement of rights to data is increasingly automated. When an investor sends a query to some data, the data-distribution system checks with the ledger where the 'rights to data' are stored to determine whether this investor has the rights for such a query.[122] Where the right to data is *purpose-specific*, humans are likely to continue being involved in monitoring enforcement.[123] Where the data contains ex ante non-attributable personally identifiable information, enforcement of rights requires blocking queries that would reveal PII, and may even require anonymization of the data at recording.[124]

Note that 'rights to data' amount to digital assets, more specifically to **data-as-digital-asset**. Whoever owns the 'digital asset' owns the 'rights to data' contained in the asset. Rights to data are therefore a subset of the broader set of digital assets.[125] **Creation, sale, and management of 'rights to data' can therefore run on the same digital-assets infrastructure as other digital assets**.

Digital Platformification

Do-it-yourself rights-to-data digital marketplaces allow data owners/sources to easily create and sell 'rights to their data' (digitally tradable rights to data). Data owners and data users interact directly with each other, disintermediating hitherto middlemen.

Crowd-Focused Solutions

The crowd itself has increasingly become a data source (crowd-sourced data) for investment decisions.[126] People have increasingly been granted sovereignty over their data, grasped the value of the data they are carrying or that surrounds them, and become willing to provide third parties with access to their data due to advances in privacy-preserving systems. People have in turn started demanding ways to monetize this data.

---

117 An enormous amount of data with personally identifiable information cannot be attributed to data subjects without first processing the data to identify these individuals. Think of data from satellites, surveillance cameras, self-driving cars' cameras, smartphone pictures, or AR glasses. Since the necessary consent from data subjects (see footnote 46) cannot be obtained ex ante, these systems are required to act as gatekeepers by checking whether a query (statistical analysis) would reveal personally identifiable information and block those that do.
These systems may even be required to anonymize the data at recording. For example by running an algorithm which recognizes people in the images — but which cannot identify these people — and then replaces the pixels. AI may even replace faces with anonymized computer-generated faces that reflect the facial expressions and emotions of the underlying real face; see e.g., Artificial Intelligence, Deepfakes could anonymized people in videos while keeping their personality, MIT Technology Review (17 September 2019), "The algorithm extracts information about the person's facial expression by finding the position of the eyes, ears, shoulders, and nose. It then uses a GAN, trained on a database of 1.5 million face images, to create an entirely new face with the same expression and blends it into the original photo, retaining the same background."

118 This is especially important during the transition period from 'non-encrypted' to 'encrypted' data. Digital service providers might need to substantially review the architecture of their software.

119 Namely, when the data is held at the 'edge'; see footnote 42.

120 See Section 'Ia. Investment universe' for a discussion of the digitalization of rights creation more generally.

121 The ledger may be a central ledger (with partial replication) or a (permissioned) distributed ledger. The type of ledger that is adopted depends on the incentives and preferences of the participants/stakeholders. The underlying ledger type may therefore vary for different types of data, for different types of rights, and/or for different types of data owners/subjects.

122 If the encrypted data moves, for example because it is sent to an investor, then the encryption protocol would limit queries to what this investor's rights allow.

123 If the 'right to data' is purpose-specific, then a human may still be involved to check whether the usage is indeed within the scope of that purpose (e.g., improving the matchmaking algorithm).
Note that the European Union's General Data Protection Regulation (EU-GDPR), which entered into force in 2018, requires service providers to request consent from data subjects to process their data by indicating the purpose of the data processing. The consent to data processing is therefore restricted to the specific purpose.

124 See footnote 113.

125 See Section 'Ia. Investment universe'.

126 See Section 'Ib. Data sources'.

Freedom to Generate, Right to Control, and Ability to Monetize

Rights-to-data digital marketplaces catering to individual data subjects have seen the light.

Western corporations are the leaders in this space. Western countries were first movers in giving data subjects extensive rights over their data,[127] which allowed Western businesses to lead the way in establishing right-to-data marketplaces.

IIc. Delivering Issuing and Investment Decision Support

Data Veracity Becomes Exponentially More Difficult
Checking the veracity of data has become much more challenging. Data veracity used to be much simpler: The data was directly sourced from non-digital official/recognized entities such as governmental agencies, non-governmental organizations, companies (official documents), or trading venues.

The increasing usage of new data sources that may be less reliable/trustworthy (e.g., crowd-sourced data), the increasing sophistication of fake facts (read: deepfakes), and the rising risk of hacking have increased the demand for data veracity assessment — but have also rendered such assessment significantly more challenging. How to verify that a picture taken from a smartphone is real? How to verify that the person writing on social media is really that person? How to verify that data accessed through the API or website of an official/recognized entity has not been tampered?

Data Cleaning/Preparing Is Exponentially More Difficult
Data cleaning and data preparation **must be performed on decentrally-stored always-encrypted not-to-be-distributed raw data**. Several possible setups are imaginable:

- Data cleaning and preparation may need to be performed on the fly, in real time, when the data is being queried.
- If this is not possible, data cleaning and preparation may need to be performed on the encrypted raw data and stored at the source — distribution of the encrypted cleaned/prepared raw data is not recommended for data privacy reasons.[128] If storage of the encrypted cleaned/prepared raw data at the source is not possible, then centralized storage at a trusted intermediary is necessary.
- If data cleaning and preparation on encrypted raw data is not possible, cleaning and preparation may need to be performed at the origin, when the data is first collected and not yet encrypted.

In the latter two cases, data cleaning and preparation must be performed in partnership with the data owner and/or storage-infrastructure operator.

Real-Time Privacy-Preserving Data Access
Remember that the (encrypted) raw data is no longer distributed — only access is provided, and the results of the data processing are distributed.[129] **Access to the encrypted raw data is in real time via APIs**, and no longer in batches.

Investors **send data queries and receive answers in real time, while both are kept private/hidden**.[130] The data-distribution and data-access systems must thus ensure 24/7 availability and must handle an enormous volume of simultaneous data processing queries.

Zero *Technical* Switching Costs Between Data Sources
Customers can readily switch between providers of data. They can **seamlessly connect, integrate, and switch between different data sources**. Data-access intermediaries in particular have witnessed the **disappearance of technical lock-ins of customers into their proprietary data models.**

We foresee two non-mutually-exclusive paths through which zero technical switching costs could arise: *API standards* (or 'data-model standards'); and *automated API matching* (or 'automated data-model translation').

127 See the text preceding footnote 47.
128 See the discussion on 'Secure and privacy-preserving data distribution' in Section 'IIb. Helping monetize data'.
129 See the discussion about 'Secure and privacy-preserving data distribution' in Section 'IIb. Helping monetize data'.
130 See also the discussion about cloud-based secure and privacy-preserving advanced-analytics environments in Section 'Ic. Investors'.

Freedom to Generate, Right to Control, and Ability to Monetize

API standards have emerged and enable investors to seamlessly connect and switch between providers of the same data types. Governments may impose API standards on FI-infrastructure intermediaries and/or on data owners themselves to reduce lock-ins and support competition.[131] Market participants may self-organize and agree/adopt a standard themselves.[132] A market participant may act as API-aggregating intermediary by translating different APIs for a given data type into one standardized API.[133]

API-matching algorithms automatically translate one API into another, and thus enable investors to seamlessly connect to and switch between data providers. AI algorithms have been trained on a labelled training data set (supervised learning) containing data on how different data models have been matched. Over time, these AI algorithms were able to match ever more data fields until they became fully autonomous.[134]

Non-unique data sources have seen their profits erode as issuers and investors can readily switch between them. **Data-access intermediaries have seen their profits shrink substantially on non-unique data**. Profits might, however, not fall to zero as differentiation may still be possible on the quality of the data (i.e., data veracity, data cleaning and preparation, unified data model).[135] Trustworthiness would likely play a key role in such differentiation.

Since investors can readily connect to and switch between multiple data-access intermediaries, they may compare prices and choose the intermediary for each query *('Pay-as-you-Query')*.

Multiplying Open Data Policies

As seen above,[136] **governments have required opening up ever more data to the public for free in privacy-preserving machine-readable form**. The scope of these open data policies has included both data produced by the government itself, as well as data produced by private service providers (e.g., trading venues' trading data).

The effect on the profitability of data-access intermediaries is unclear. On the one hand, profits fall because data cleaning and preparation services are no longer needed from intermediaries: Governments have required data sources to clean, prepare, and publish the data in a standardized data model. On the other hand, profits may increase because more data may become accessible to intermediaries, enabling them to expand their data veracity services and their data aggregation services (consistently linking data sets into a unified data model).

Digital Platformification

Customers demand convenience (incl. findability), comparability of services (best conditions), perfect tailoring (choice).[137] Similarly to how digital platforms have taken hold in other markets as digital UIs became ubiquitous,[138] **issuers and investors seek issuing-and-investment-decision-support solutions via digital marketplaces**. These platforms aggregate across different FI-service providers and include a wide range of FI services, from access to some raw data, to cleaned data, to rights to data, to regulatory solutions (e.g., regulation monitoring, issuing-document generation), to ratings (e.g., credit ratings, sustainability ratings), to data playgrounds, to cloud-based privacy-preserving advanced-analytics environments, to digital UIs (e.g., desktop, smartphone, AR, VR).

131 In the banking space, the UK created an independent agency ('Open Banking Implementation Entity', OBIE) to develop a mandatory API standard to implement its Open Banking Regulation.

132 Several areas have already seen market participants voluntarily join forces to develop standards. In the banking space, consider 'NextGenPSD2' (driven by The Berlin Group, which represents over 40 banks, associations and payment providers in Europe) and 'Swiss Common API' (driven by SFTI). Outside of banking, consider 'Data Transfer Project', which develops open-source data-mobility standards to enable seamless and direct data mobility between social-media platforms (launched in 2017 by Google, Facebook, Microsoft, and Twitter).

133 In the banking space, one such API-aggregating initiative is the 'SIX API Hub'.

134 This process took some time. At first, the AI algorithm was perhaps able to match 50% by itself and required help from a human for the other 50%. The AI algorithm then learned from the human's matching (supervised learning) and thus progressively improved its matching performance.

135 Although investors typically have their own data model, retail investors and new investors may prefer using (or starting from) an internally-consistent unified data model.

136 See the discussion on 'Crowd-sourced data' in Section 'Ib. Data sources'.

137 See Section 'Ic. Investors'.

138 For a more general discussion, see the Section 'Ubiquity of digital user interfaces' in the most likely scenario of SFTI, 2019, Future of Financial Institutions.

Freedom to Generate, Right to Control, and Ability to Monetize

These digital marketplaces help investors easily compare services and easily find relevant content — they offer the same search-result quality everyone has become used to from the likes of Amazon and Google. With the explosion in diversity and volume of digital data,[139] **findability** is an increasingly important aspect of digital marketplaces. **Competition between FI-service providers has substantially increased**.

Selected services are seamlessly integrated into the investor's existing digital applications and systems, irrespective of whether they are hosted on-prem or in some third-party cloud.[140] A new data source is, for example, readily integrated into one's analytics environment and into one's digital UIs. This **plug-and-play** world (interoperability, zero technical switching costs) provides customers with a greater choice, better tailoring, and a seamless UX (convenience).

It is **unclear whether a solely FI-services marketplace can own the customer interface**. Investors may prefer a one-stop-shop marketplace that covers all their needs (e.g. trade-execution software). The existence of widely accepted digital identities[141] allows investors to seamlessly switch between platforms and thus suggests a co-existence of several marketplaces, each focusing on different needs (and tailored to meeting these needs).

Complete Unbundling of FI Services

Customers demand **perfect tailoring to their needs**.[142] FI services are fully unbundled: Services are unbundled into their constituents (sub-services) and offered as separate services. Investors can, for instance, choose different providers for access to raw data, cleaned data, verified data (data veracity), and a unified data model. They can choose between different providers down to the individual data field. Buyers can, of course, choose to continue sourcing all FI services from the same provider.

Regulatory Crosshair

After regulators focused on banks, asset managers, and rating agencies as the main culprits of the financial crisis of 2008, **regulators turned their attention to FI-infrastructure providers** more generally.

FI-infrastructure providers may amount to a **source of systemic risk** because data amounts to a key input for critical activities/processes of financial institutions, and machines increasingly process this data without human intervention or oversight.

IId. New Players

Big Tech Companies

Big tech companies (Google, Amazon, Microsoft, Facebook, Alibaba, Tencent, etc.) have become **clients of FI-services providers**. Ever more big tech companies have entered the payment space with digital wallets, from Amazon Pay, to Google Pay, to Apple Pay, to Facebook's planned digital wallet ('Calibra') and digital coin ('Libra'). The functionality of these digital wallets **expanded into offering wealth-management and investment services**. This move already happened in China in the early 2010s. Both Alibaba and Tencent's digital wallets started out as a mobile-payment service (peer-to-peer, merchant payments via QR codes) and then expanded into WM to allow their users to invest the money they had lying around in their wallets.[143]

Big tech companies' **core capabilities and technologies can be leveraged for expanding into FI infrastructure**:

- *They have been mapping and categorizing assets:* Amazon is indexing everything that can be sold (it wants to be the 'store of everything'); Google wants to digitally index/map the world, including its assets.[144]

139 See Section 'Ib. Data sources'.

140 Recall that investors have shifted their digital infrastructure into the cloud. See Section 'Ic. Investors'.

141 The government and/or private parties may provide digital identities. Multiple digital-identity providers may be trusted and co-exist – a given person would by uniquely identifiable by different providers.

142 See Section 'Ic. Investors'.

143 Alibaba's digital wallet is called 'Alipay'. Tencent's digital wallet 'Tenpay' is integrated in its message app 'WeChat'. See e.g. CB Insights, 2018, Ant Financial: Unpacking the fintech giant (September 2018).

144 Google's corporate mission is 'to organize the world's information and make it universally accessible and useful.'

Freedom to Generate, Right to Control, and Ability to Monetize

- *They have been building privacy-preserving data-distribution systems:* Google is a first-mover in the federated AI space;[145] Google and Facebook have both released open-source libraries for federated AI on encrypted data.[146]
- *They have been creating and selling rights:* Google and Facebook's revenues come from creating and selling advertising rights.
- *They have been enforcing rights to data:* Rights management (DRM) underpin their stores for digital music, books, and videos.
- *They have been sourcing and aggregating data:* Google and Facebook are notorious for sourcing enormous amounts of data to support their advertising businesses by allowing for more-tailored advertising.[147]
- *They have been operating digital marketplaces:* Amazon and Alibaba have been operating and expanding such platforms for two decades. Amazon was recently awarded a patent for a peer-to-peer 'right to data' marketplace.[148]
- *They have operated search engines to find information:* the word 'Google' has become synonymous for 'search'.

Despite these overlaps, **it is far from certain that big tech companies will become FI-infrastructure providers themselves** because of the increased regulatory scrutiny looming over the FI-infrastructure space and because of increasing concerns over the power of big tech companies. Note that when the regulatory focus increased in Asia, Alibaba and Tencent rapidly retreated from offering financial services themselves. They instead shifted to becoming financial-infrastructure providers offering technology to financial services providers (TechFin).[149] With the regulatory crosshair likely moving toward FI-infrastructure providers, **big tech companies may opt to provide technology to FI-infrastructure providers** rather than entering the space themselves.

Exchanges and Trading Venues

Exchanges and trading venues more generally are likely to continue seeing an erosion in their traditional sources of profits (trading fees, trading data).[150] Searching for new profit pools, operators of secondary markets are likely to continue expanding into data services and thus directly competing with FI-services providers.

145 Google invented federated AI in 2017, see Google, 2017, Federated Learning: Collaborative Machine Learning without Centralized Training Data, Google AI Blog (6 April 2017). Google is furthermore invested in a start-up applying this approach in the health-care space (see footnote 112).

146 They have released these open-source libraries in their ML frameworks (TensorFlow respectively PyTorch). See e.g. VentureBeat, 2019, How federated learning could shape the future of AI in a privacy-obsessed world (3 June 2019).

147 Better, more fine-grained data increases the value of an 'advertising right' by increasing the likelihood of a match/click.

148 CoinDesk, 2018, Amazon Sees Bitcoin Use Case Marketplace (17 April 2018), "The patent describes a system in which individuals and organizations can put streaming data feeds up for sale, to which customers can then subscribe."

149 See e.g., Economist, 2018, Ant and Tencent: As regulators circle, China's fintech giants put the emphasis on tech (13 September 2018).

150 Trading fees are likely to fall because digitalization enables investors to easily connect simultaneously to multiple digital trading venues and place the order where the price is best. Market-makers will also connect to multiple digital trading venues. Revenues on trading data are likely to fall because trading data is no longer a unique asset. Two drivers underlie this development: Regulators are likely to require public availability of trading data at ever lower latency; and new laws are likely to give investors/traders rights over their trading data, allowing them to sell their trading data to third parties. See more generally: SIX, 2019, Future of the Securities Value Chain (January 2019), pages 24 and 44.

Middle - and Back-Office Consolidation in Finance

Medium-Likelihood Scenario

Early-detection signals: adoption of challenger banks; increased outsourcing of IT systems to cloud by legacy financial institutions; modernization of legacy IT systems; adoption of micro-services-based IT infrastructure; increasingly cost-sensitive clients; increasing interoperability; advances in privacy-preserving systems.

Context

From banks, to insurances, to asset managers, all financial services providers **outsource virtually all their middle- and back-office activities to utilities**.

Activities are split between global and local utilities. Local utilities have, for example, successfully captured niches where local circumstances preclude global scaling (e.g., regulatory services), where local regulators demand jurisdiction over the service provider (e.g., for critical processes carrying system risks), or where clients demand a local anchoring.

This process of outsourcing has been ongoing for some time because **middle- and back-office activities have increasingly been assessed as non-differentiating**.[151] But three factors have accelerated this transformation.

First, **middle- and back-office activities increasingly exhibit economies of scale**. Technological advances in automation[152] have increased the scope for cost mutualization: Replacing humans with machines creates scale-based cost reductions in ever more activities.[153] Digitalization has furthermore increased the potential for cost reductions through cost mutualization. Take the building and execution of trading strategies, which necessitates increasingly costly non-differentiating assets such as storage, computing, and big-data analytics.

Second, technological advances (e.g., interoperability, micro-services-based IT architectures, secure and privacy-preserving systems) have **facilitated outsourcing non-differentiating activities by reducing transaction costs**.[154] Ever more activities and processes can thus benefit from cost mutualization.

Third, **new technologies improve ever more services, but the necessary capabilities and skills are rare** and need to be sourced. AI, most notably, enhances everything, but the skills are in short supply. Service providers having those capabilities have increasingly monetized them by offering their activities to other businesses.

FI Infrastructure

Profits on differentiating services (unique services) serving the middle- and back-office are likely to decrease because a single middle- and back-office buyer (the utility) weakens the bargaining power of the supply side.[155] A utility holding out hits the FI-service provider more strongly than one middle- and back-office out of many holding out. And a utility holding out does not risk losing its clients to another middle- and back-office. **By how much profits reduce is unclear** and will depend on, among other things, the second-best alternative to accessing a unique FI service; how much each side loses from holding out; and on negotiation skills.

151 Non-differentiation is less prevalent in the middle office with its range of proprietary/unique analytics (intellectual property).

152 From robotic processing automation (RPA) to artificial intelligence (AI). Algorithms have automated optimal trade execution: JP Morgan's LOXM is an algorithm that automatically executes trade orders at the best price (which most notably includes: how to execute a large order that cannot be executed at once).

153 Thus, replacing variable costs (humans) with fixed costs (an algorithm).

154 Interoperability and micro-service-based IT architecture allows users to seamlessly connect systems from different providers, reducing lock-in risks (by allowing users to easily switch from one service provider to another) and counterparty risks (by allowing users to work with different providers for different services). They have furthermore allowed a gradual outsourcing of activities/systems.

155 To facilitate the description, we use the extreme case of a 'single middle- and -back-office'.

Extreme Consolidation in FI Infrastructure

Medium-Low-Likelihood Scenario

Early-detection signals: little protectionism; no fear of companies being too powerful; lack of government action aimed at enforcing competition in the digital sphere; no fear of foreign operators of key local infrastructure.

Context

Global players dominate most markets. Digitalization has turned most markets into **winner-takes-it-all** by yielding scale-based quality improvements (network effects, data sets)[156] and scale-based cost reductions (economies of scale). A local identity through a long-standing local presence or local origin may compensate for a lack of global scale. And so could trustworthiness and understanding of a client's internal dynamics through long-term personal relationship and collaboration. These soft factors have, however, been of lower importance in the global FI space because data is sourced through technical interfaces and trustworthiness gained through data quality. And even where these soft factors have not been of lower importance, global players have acquired local companies, and with it, their long-lasting personal connections.

The most likely path is lack of government action[157] aimed at enforcing competition in the digital sphere.[158] Waves of consolidation used to characterize the FI space. The market consolidated and, when concentration posed too high a risk of market-power abuse, governments jumped in, mandating carve outs and preventing further mergers. This isn't happening anymore. The waves have given way to a monster wave with seemingly no breaking point.

Governments have also not required these global companies to make their services interoperable, have not broken up vertical supply chains, and have not provided data sovereignty to users. Non-global companies have therefore not been able to source scale,[159] and to source data held at those companies.[160] Non-global companies cannot compete against these global behemoths.

Product manufacturers have scaled up in both B2C and B2B spaces.[161] Services are offered at global scale wherever scale provides an advantage.

FI Infrastructure

All platforms in the FI space have global scale. There is a *single global digital marketplace in the FI-services space*: data owners/sources can create and sell 'rights to their data'; and issuers/investors can find all the FI services they may need.[162] There is also a *single data-distribution and data-access intermediary*.[163]

(Niche) FI-service providers around these platforms have global scale wherever scale provides an advantage. Local niche FI-service providers co-exist with these global players — where scale provides no advantage, and/or where scale benefits alone do not allow offering a strictly superior value proposition.

156 Larger data sets may improve insights and allow better-quality services (e.g., faster service, better tailoring, better findability).

157 Which includes 'ineffective government action'.

158 Governments enforcing property rights and competition would, for instance, aim at reducing user lock-ins, unbundling services, breaking up vertical supply/value chains, and allocating rights to data.

159 Interoperability and breaking up vertical supply chains would allow local companies, which do not own the entire vertical supply chain and which do not have global scale, to benefit from the economies of scale and networks of global upstream companies. These smaller local companies would thus have a chance to compete with global players on costs and on network effects.

160 Data sovereignty to data subjects would allow local companies to source data from a global set of data subjects without themselves having a global user base. These smaller local companies would thus have a chance to compete with global players on data insights.

161 B2C describes businesses doing commercial transactions with private persons (business-to-consumers); B2B describes businesses doing commercial transactions with legal persons (business-to-business).

162 See Sections 'IIb. Helping monetize data' and 'IIc. Delivering issuing and investment decision support' in the most likely scenario.

163 In the most likely scenario, see Section 'IIb. Helping monetize data' for data-distribution systems, and Section 'IIc. Delivering issuing and investment decision support' for data-access systems.

Extreme Protectionism

Medium-Low-Likelihood Scenario

Early-detection signals: *increasing global tensions; increasing fear of China; rising populism; rising nationalism; rising inequality; squeezed middle-class; lagging economic development in developed countries; increasing flows of refugees.*

Context

Sustained globalization discontent, growing nationalistic sentiments, and increasing weaponization of economic tools[164] have led to a world with **cross-border investment and trade restrictions**. Brexit was only the beginning. The trade barriers between the US and China[165] spread to other countries. Governments have imposed **market-access restrictions and restricted domestic companies** from doing business with specific foreign countries/companies out of national-security concerns and to advance national interests.[166]

Governments have furthermore restricted the cross-border flow of data **(data protectionism)** by requiring that their citizens' data stays within the country's borders, sometimes even prohibiting the data from leaving the country at all.[167] Countries have justified these laws on the grounds of national security (spying risks, data-accessibility risks), data colonialization,[168] data monetization,[169] or privacy risks.

Governments have **forbidden AIs trained on foreign data from entering their country**. Governments have, for example, argued for the necessity to support the development of a domestic AI industry by shielding it from foreign competition (digital industrial policy), citing AI's foundational nature for future industries and innovations. Sometimes governments also cited abuses of human-rights to explain market-access restrictions on foreign-data-trained AIs.[170]

FI Infrastructure

Governments want a **locally operated FI infrastructure** to ensure a functioning local market that efficiently allocates capital. FI is considered critical infrastructure and thus of national security relevance.
Domestic FI-infrastructure providers **operate local secure and privacy-preserving data-distribution systems**. These systems also allow the selling of 'rights to data' abroad while ensuring that the raw data never leaves the country.[171] And they allow local investors to access and process worldwide data by connecting to foreign secure and privacy-preserving systems. Fear of foreign governments spying and/or interrupting services led countries to **natively develop these secure and privacy-preserving data distribution systems**.

FI-infrastructure providers have been **forced to sell the systems they operated in foreign countries**.

---

164 Economist, Weapons of Mass Disruption (8 June 2019), noting that such weaponization is a hallmark of the Trump administration.

165 For an overview of the timeline, see FT, 2019, Timeline: No end in sight for US-China trade war (1 June 2019).

166 Perhaps most notably, the US governments added Huawei in 2019 to the list of companies for which US companies need government approval before selling them something — which the US government is unlikely to provide under its 'policy of presumption of denial'. The rationale was 'significant risk for national security'; see e.g. FT, 2019, Google suspends Huawei from Android services (20 May 2019).

167 These laws require that the data be stored within the country, and at times forbid the data from leaving the country at all. By 2019, 'data localization laws' (aka 'data protectionism') had been passed in over 45 countries, including authoritarian as well as democratic countries. Even the EU had de facto passed such laws: The EU-GDPR de facto yields data localization because it substantially raises the compliance costs for companies to store data on EU citizens abroad. See e.g., WSJ, 2019, The Rising Threat of Digital Nationalism: As the internet turns 50, the global vision that animated it is under attack. What can be done? (1 November 2019).
A notable example is Russia: "Russia has blocked LinkedIn from operating there after it refused to transfer data on Russian users to local servers" (FT, 2018, Data protectionism: the growing menace to global business, 13 May 2018).

168 Developing countries have argued that such laws are necessary to combat the plundering of yet another one of their natural resources.

169 Namely, to protect one of a country's key natural resource in the 21st century ('data as the new oil').

170 Governments running a surveillance state may track their citizens everywhere and collect all their digital data. This arguably violates fundamental rights to privacy and to private property.

171 Even if foreign investors are forbidden from investing in local assets, local data may help investors evaluate foreign assets.

Crypto-Assets Everywhere

Low-Likelihood Scenario

Early-detection signals: *loss of trust in governments; rising trust in code; substantial advances in permissionless distributed ledger technologies (DLTs); strong adoption with younger generations (e.g., generation Z).*

Context

The world runs on permissionless distributed ledgers.[172] *Crypto-assets*[173] are the dominant form of digital assets and therewith of investable assets. *Decentralized crypto-currencies* (e.g., Bitcoin, Ether) have replaced central-bank-issued currency as the dominant medium of exchange.[174] *Crypto-contracts*[175] are a widespread form of contracts. Digital services take the form of open-source code stored on these permissionless distributed ledgers and decentrally executed by participants to these ledgers. These are known as 'decentralized applications' *(DApps).*

For permissionless distributed ledgers to be everywhere, however, *a set of conditions must be fulfilled*. We view the probability of all these conditions being *jointly* fulfilled to be low. The following will walk you through some of these necessary conditions.

First and foremost, permissionless DLTs need to solve an actual problem that people have in order for them to adopt/trust this novel technology. The unique feature of permissionless DLTs is that they (promise to) allow running a digital ledger[176] without having to trust some centralized party[177] to operate it. So, if people have trust in some centralized entity, permissionless DLTs would be a solution without a problem.

More specifically, we believe that for people to demand a system that promises to work without a trusted centralized entity, ***people must lose trust that the rule of law will be respected and enforced, they must fear that their government will not uphold their private property rights (fear of expropriation), and/or they must fear that the government will not enforce their contractual rights***.[178] In other words, they must completely lose trust that political institutions aim to act in the interest of the public.[179] Some degree of skepticism that political institutions serve the interests of the people is unlikely to be sufficient for people to switch to permissionless DLTs: Familiarity,[180] recent experiences in no governmental oversight,[181] incomprehension and uncertainty,[182] as well as inertia are likely to

172 Permissionless distributed ledgers (e.g., Bitcoin blockchain, Ethereum blockchain) are defined as ledgers wherein anyone can be part of the consensus protocol. See also Cambridge Centre for Alternative Finance, 2018, Distributed Ledger Technology Systems: A Conceptual Framework (August 2018).
A ledger serves as a registry of ownership of rights to assets. These ledgers may be digital or not. Banks, for instance, used to rely on a piece of paper to register which of their clients owned which of the assets (lying in the bank's physical vault).

173 Crypto-assets are defined as digital assets issued on some permissionless distributed ledger.

174 For the definitions and distinctions between decentralized and centralized crypto-currencies, see the appendix 'Definitions' in SIX, 2019, Future of Money (November 2019).

175 Crypto-contracts are defined as digital contracts that are (i) written in code and automatically run/execute the code when the conditions in the contract are met (aka 'smart contract'), and (ii) whose code is registered on some permissionless distributed ledger. These contracts are either self-enforcing or decentrally-enforced, and thus require no trusted centralized entity for enforcement.

176 A digital ledger, most notably, allows the registration of ownership of rights to (digital and non-digital) assets.

177 This 'centralized party' may amount to a 'single entity' or a 'defined group of entities'.

178 Note that when people trust that contractual rights and obligations are being enforced, they are also willing to rely upon untrustworthy private companies because they trust that the government will enforce the companies' contractual obligations.

179 A loss of trust in governments' capabilities to orchestrate society and the economy is unlikely to be enough for people to turn to fully decentralized systems. There are too many alternatives that rely on existing structures and ways of doing so. Government incompetence is instead likely to lead people to rely on private parties. Incompetence of public judges is likely to lead them to instead rely on private arbitrators to resolve legal disputes. Incompetence of countries' central banks (e.g., hyper-inflation) is likely to lead them to instead rely on an alternative centrally issued currency (e.g., WIR, mobile-phone credits).
A loss of trust in individual politicians' benevolence, even if they amount to presidents, will generally not suffice in democratic countries. The political institutions entail checks and balances (executive, legislative, judiciary branches), requires re-elections, and exhibits term limits in order to reign in malevolent politicians. An exception would be if a malevolent politician is expected to take control over the army, refusing to abide by these laws and regulations, and shifting the country from a democracy to an authoritarian regime.

180 If it's not broken don't fix it.

181 People still remember the last large-scale social experiment in no government laws and regulations — the Internet. It too was led by (digital) technologists. The Internet and the Internet-based economy were built on beliefs in libertarianism, unfettered markets, laissez-faire, and permissionless innovation. It did not result in the promised equal and fair world: The result was a centralized, winner-takes-it-all digital sphere, ruled by a handful of global behemoths, undermining competition and innovation.

182 The functioning and game-theoretic foundations of permissionless DLTs are complex and difficult to understand. There are also considerable uncertainties regarding the long-term functioning of a system that runs on permissionless DLTs. These uncertainties will be discussed later in the text.

Crypto-Assets Everywhere

drive people to continue relying upon the centrally enforced legal framework — and not experiment with such a fundamental fabric of modern societies.

Second, ***reliance on a trusted centralized third-party entity must be impractical***. If a third-party government is trustworthy, then a fully decentralized system may not be needed — even when the local government is untrustworthy. People may, for example, have bank accounts in Switzerland to securely keep their (digital) assets outside of their government's reach. Or people may use the US dollar or Swiss franc instead of their local currency as a medium of exchange. Also, if a local private company is perceived as trustworthy, a decentralized system may also not be needed. If the untrustworthy local government cannot undermine these trusted centralized third parties, familiarity, incomprehension and uncertainty, as well as inertia are likely to drive people to rely upon these (centralized) third parties instead of permissionless DLTs.

But even if there exists a problem — absence of a reliable trusted centralized entity — that permissionless DLTs could solve, their adoption is still not certain.

Third, ***people must want to stay in the digital sphere***. Perhaps because it allows them to deal with foreign service providers. Perhaps because it allows them to subscribe to and instantly consume a digital service such as Netflix. Or simply because it is more convenient to carry digital money than physical cash. If they don't, then they may, for example, return to using precious metals such as gold as a medium of exchange.

Fourth, ***people must trust the functioning of permissionless distributed ledgers***. Although permissionless DLTs tend to be advocated as 'trustless', quite a bit of trust is still needed. People must, for instance, trust that there are no bugs in the code,[183] that the consensus protocol can scale, that the system is resilient against cyberattacks,[184] or that a fully open-source economic system can work.[185] They must also trust that the system remains decentralized:[186] If a minority can take control over the system and set the rules so as to serve its personal interests, then the promised world will at best be as good as the one it is trying to escape from. Finally, they must also trust that the system can properly handle the situation wherein a violent criminal forces you to transfer your rights on the permissionless DLT.

Fifth, ***people must trust that a presumed-malevolent government cannot interfere with these ledgers and their execution***. Governments might be able to overpower the consensus protocol or to prevent internet access to the ledger (e.g., by monitoring/controlling internet traffic).[187] And even if they cannot interfere with the ledgers themselves, they may interfere with the execution of the rights and obligations included in crypto-assets and crypto-contracts. Execution may require a real-world person to take an action; or execution may be linked to a non-digital asset such as a car or a piece of art. A government may be able throw this person in jail, confiscate the car, or intercept the piece of art when it is shipped to its new owner.

If so, then people may shift to fully-decentralized digital systems to serve as a registry for the ownership of their (digital) assets ('crypto-assets').

---

183 It has been reported that 1,000 lines of code exhibit on average 15–20 bugs. "Good programmers working under careful supervision average about one bug per 2,000 lines of code." (Economist, 2019, Cyber Security: Hack The Plant, 14 September 2019).

184 Cyber-attackers might otherwise steal the crypto-assets registered thereon.

185 Any participant must be able to verify all the codes for the system to remain trustless, which requires that all code be open source. An incentive model is therefore needed to reward those developing new code since anyone can readily copy the code once it is published in the system — such an incentive model must be built directly into the system's core code base.

186 It has, for example, been reported that the most famous permissionless distributed ledger, the Bitcoin blockchain, is no longer really decentralized: 60% of the computing power in the Bitcoin blockchain resides in China. Recall that one controls the Bitcoin blockchain (since its consensus protocol is proof-of-work) if one owns 50% or more of the entire computing power in the system. For the data, see Bryan Ford, 2018, Clubs, Coins, and Crowds: Fairness and Decentralization in Blockchains and Cryptocurrencies, Presentation at IEEE Security & Privacy on the Blockchain (23 April 2018).

187 Iran, for instance, shut down the Internet to disrupt protests that erupted in November 2019 following an oil price spike of over 50%; see The Download, 2019, Iran has shut off Internet access for its citizens amid fuel price protests, MIT Technology Review (18 November 2019). More generally, Internet shutdowns have become a widely used tool of authoritarian regimes to control its people, "Africa and Asia are the two continents most affected by internet shutdowns, and India is by far the greatest perpetrator" (The scary trend of internet shutdowns, 1 August 2019).

Crypto-Assets Everywhere

FI Infrastructure

All digital assets (i.e., crypto-assets) are by construction uniquely-identifiable on these permissionless distributed ledgers. Issuers and parties to a digital contract are anonymous but uniquely identifiable with their 'public signature'.[188] **Reference data includes additional descriptive information**, such as information about activities that are linked to this (anonymous) public signature.

'Rights to data' take the form of crypto-tokens that are registered on these permissionless distributed ledgers. FI-services take the form of **open-source DApps**.

188 They may want to remain anonymous because governments could track them otherwise. A given person may have multiple 'public signatures'. Some people may prefer a single signature to build a reputation over time.

3 Definitions and Concepts

Financial information: describes all information that is used by financial entities or market participants for investment decision-making, from trading, to clearing & settlement, asset servicing, investment valuation, risk management, and regulatory and tax compliance.

Relations: Data Model | Data Dictionary | Glossary
- ***Model:*** An abstract and formal representation of something.
- ***Data Model:*** An abstract and formal collection of data elements/fields and their relationships, with the purpose of representing/mapping a real-world domain of interest.[189]
- ***Data Dictionary:*** A repository of information about data elements/fields such as: identifying term *(data notation)*; definition *(data semantics; glossary)*, relationships to other data *(data relationships)*; usage and format *(data constraints)*.
- ***Glossary (semantic layer):*** An alphabetical list of terms with their definitions, including explanations of their relationship to some real-world properties *(real-world mapping)*.
- ***Database:*** Describes a collection of data, organized according to some data model, stored, and electronically accessible.

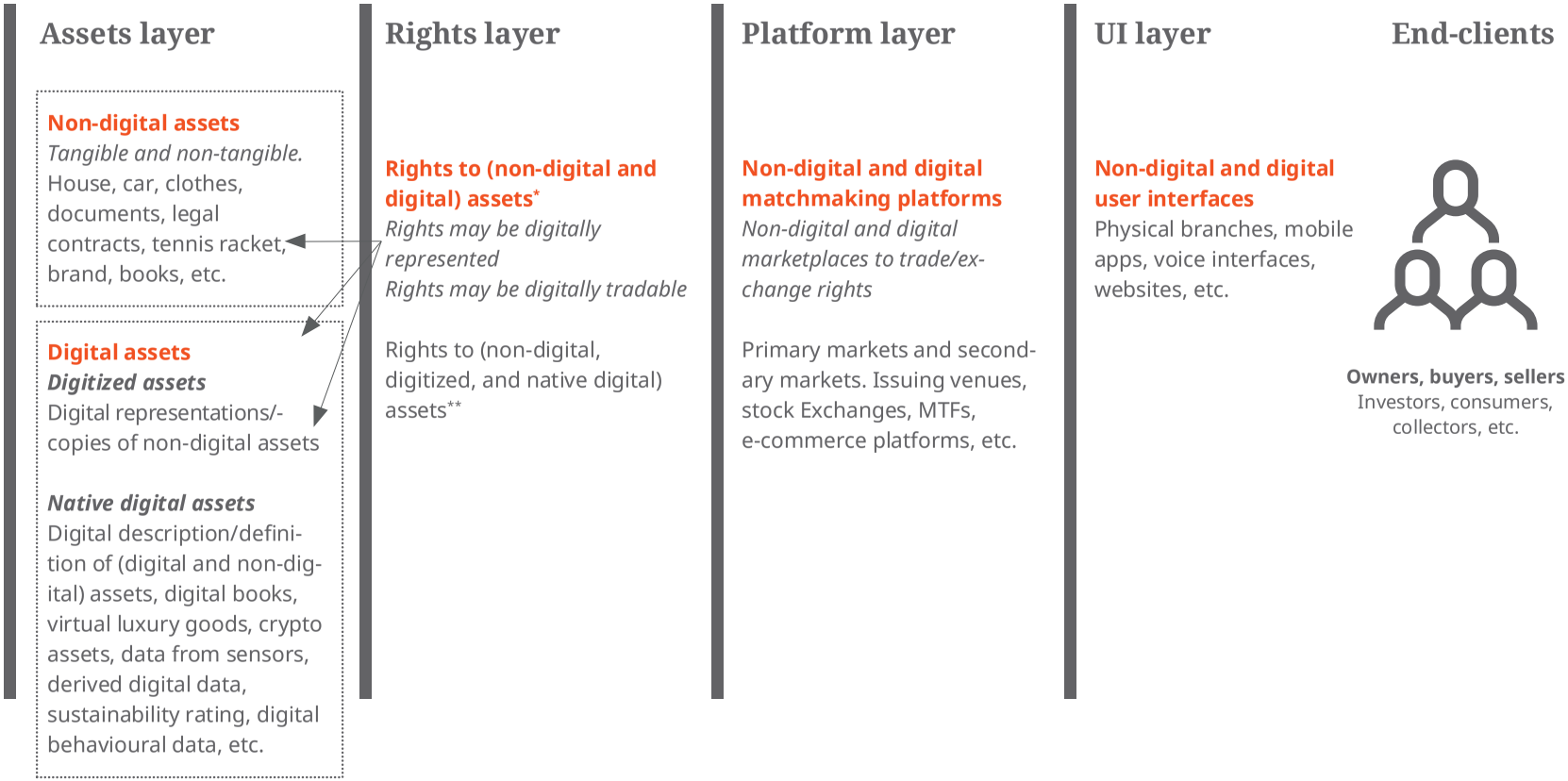
Types of data sources:
- **Reference data:** Describes data which refers directly to the financial products and/or its issuer. Notable examples include: International Securities Identification Number (ISIN); terms and conditions of financial product; legal-entity identifier of issuer; corporate structure and hierarchies of issuer; capital structure of issuer; corporate actions (e.g., stock splits, dividends, spin-offs, meetings); ratings (e.g., credit, risk, sustainability); tax implications.
- **Live data:** Describes dynamic data which helps price financial products. Notable examples include: trading/market data (from exchanges and trading venues); sentiment data; social media data; satellite data; news data.

Digital assets: describe 'something' that can be owned and has a digital presence. Digital assets are a *subset of intangible assets (Immaterialgüter)*.

- We distinguish between two types: ***digitized assets***, which capture digital representations of tangible and intangible non-digital assets/things, and ***native digital assets***, which have no existence in the non-digital realm.
- Digital assets take many different forms. The following list is not exhaustive, but gives a sense of its breadth: *digital description/definition* of a (digital or non-digital) asset; *digitally recorded knowledge* (e.g., digital documents, books, websites, media, news, trade secrets, patents); *digitally recorded non-digital raw data* (e.g., digital representations of mountains, trees, houses, people); *derived digital data*[190] (e.g., calibrated/trained analytics and matching algorithms, results from statistical queries, interpretation of regulatory data, news data, calculated prices for illiquid assets, rating data); *digital behavioural data* (e.g., social media data, trading data on digital trading venues, clicks and website visits, digital payment data); *software* (e.g., analytic algorithms, optimization algorithms, video games, chat applications); *digital art* (e.g., digital photographs, movies, music); *digital properties* (e.g., virtual in-game objects, virtual pets, virtual luxury goods, native crypto-assets); *digital currencies* (e.g., bank money, central bank digital currency, Libra, crypto-currencies).
- **Rights to digital assets** — from ownership rights to intellectual property, to usage rights — are a key source of value creation in the digital and intangible economy. Note that *rights to digitized assets* only provide a legal claim to the digital representation of a non-digital object (e.g., digital map of the world, digital twin of a factory machine), not to the underlying non-digital asset/object.

189 For instance, a data model whose purpose is to represent the price formation of a bond would have as data elements the drivers of the bond's price. Their relationship would be determined by how these drivers interact, etc.

190 Derived data describes new data that has been built on top of existing digital data through combination with further inputs.



* The recording/registration of ownership of rights to (non-digital and digital) assets may be digital — in a so-called 'digital ledger'. Such digital ledger may run as a central ledger, permissioned distributed ledger, or permissionless distributed ledger (e.g., Bitcoin blockchain, Ethereum blockchain). If rights are registered on a distributed ledger, rights are referred to as 'digital tokens' and the process of creating rights to assets as 'asset tokenization'. If rights are registered on a permissionless distributed ledger, rights are referred to as 'crypto-tokens'.

** Rights to any asset always necessitate a definition/description of the assets it is referring/linked to. For example, a digitally represented right to a house ('non-digital asset') may build upon a digital description of this house ('native digital asset'), which may itself build upon digital sensors in the house's walls ('native digital asset'), upon digital legal contracts relating to the house ('native digital assets'), and upon the house's digital representation/copy ('digitized asset'). If we rely upon the 'digital description of this house' generated by a third party, then we will need to acquire the usage rights to this native digital asset.

Note to the Reader

Authors

The views expressed in this paper are those of the authors, and do not necessarily reflect those of SIX or other contributors. For more information about this report, please contact us at: research@six-group.com.

Stefanie Gaiser
Senior Program Manager, SIX

Dr. Tobias Lehmann
Future Scenarios Lead, SIX

Acknowledgments

The authors would like to thank the many colleagues who contributed via discussions, interviews, document reviews, and workshop participation. They would especially like to acknowledge the contribution of those below.

Core Team

Tommy Andorff
Co-founder Trust Anchor Group

Martin Berger
Senior Architect, SIX

Alexander Dorfmann
Senior Product Manager, SIX

Pascal Fuld
Head Capabilities, SIX

Christophe Lapaire
Head Advanced Tax Services, SIX

David Lecompte
Head Marketing Financial Information, SIX

Frédéric Messein
Head Product Proposition, SIX

Dominique Tanner
Head Content Management, SIX

Further Contributors

Brad Bailey
Research Director, Celent

Dr. Jeremy Callner
Chief Product Officer, Gokong AG

Joséphine de Chazournes
Senior Analyst, Celent

Dr. Remo Frey
Senior Open Innovator, SIX

Sven Hubschmid
Head Regulatory Services & VAS, SIX

Phillip Lynch
Head Markets, Partners and Products, SIX

Antonio Maggio
Senior Experience Designer, SIX

Stephan Schaub
Senior Architect, SIX

Dr. Marcel Schöngens
Senior Data Scientist, SIX

Dr. Andreas Sprock
Head Innovation Management, SIX

Michele Vuerich
Head Data Processing, SIX

Visualizations: Kilian Wilde (wilde-grafik)
Copyediting: Rob Scott (Robin Scott Translations)

SIX
Pfingstweidstrasse 110
Postfach
CH-8021 Zürich
www.six-group.com