CHAPTER 2 Digital Space and Its Aspects

Kilnam Chon 2021.4.12/5.12

Digital Space and some of its aspects will be described in this chapter. Please refer Figure 2.1 for diagrammatical description of the digital space, digital subspaces, aspects, and infrastructure. We may use the words, digital space and cyberspace alternatively even though their coverages are slightly different. The digital space tends to have technological perspective, and the cyberspace tends to have application perspective.

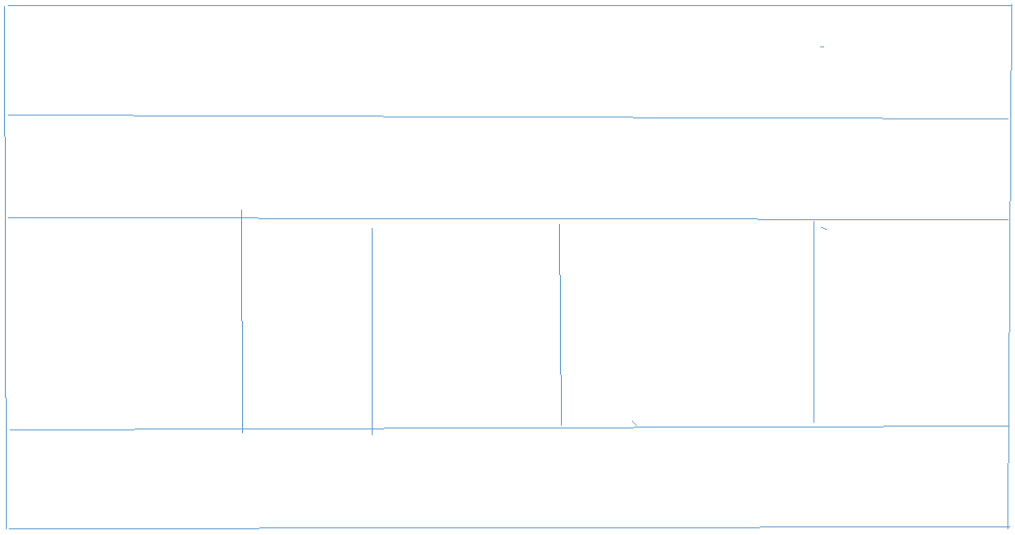


Figure 2.1 Digital Space, Subspaces, Aspects, and Infrastructure

We will cover the digital space and some of its aspects in this chapter as follows;

2.1 Digital Space
2.2 Data
2.3 Artificial Intelligence
2.4 Blockchain

Section 2.1 Digital Space is the revised version of "Cyberspace – What is it?", which was published in 2013 [Chon 2013d]. The Data aspect is covered in Section 2.2 Data. The AI aspect is covered in Section 2.3 Artificial Intelligence. The Blockchain aspect is covered in Section 2.4 Blockchain. The cybersecurity aspect and the social media aspect were covered in Chapter 5 Cybersecurity and Chapter 3 Social Media of Asia Internet History, Third Decade (2000s) in the limited scopes, respectively.

The High-Level Panel on Digital Cooperation convened by the UN Secretary-General with The Terms of Reference, *"1. The Panel will advance proposals to strengthen cooperation in the digital space among Governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders...(snip)"* [UN 2019]. Its report, "The age of digital interdependence" was published in 2019. Its road map for digital cooperation was approved by UN General Assembly in 2020 [UN 2020].

References

[Chon 2013d] Kilnam Chon, "Cyberspace – What is it?", 2013.
[UN 2019] UN Secretary-General's High-level Panel on Digital Cooperation, The age of digital interdependence, 2019.
[UN 2020] UN General Assembly, Secretary-General's Report: Road map for digital cooperation, 2020.

2.1 Digital Space

Kilnam Chon

(1) Introduction

The Internet turned fifty-years old in 2019, with more than half of the global population as its users [Internet 2020]. There are various application systems based on digital technologies with the Internet and other networks as their infrastructure. We refer to these application systems as aspects of digital space. The aspects include artificial intelligence, data, social media, cybersecurity, and Internet of things (IoT) among others. Digital space and cyberspace have drawn a great deal of attention in this century, with various conferences and organizations devoted to them [Cyber 2013; Seoul 2013; ECIR 2013; Black 2010; Cyberspace 2013; Chon 2013b]. This section explores digital space, and its subspaces; digital economy and digital society as well as aspects of the digital space. We will then explore governance of digital space and its aspects in the next chapter.

In this chapter and the next chapter, we use "cyberspace" and "digital space" interchangeably except for cases where it is necessary to separate them. Wikipedia defines cyberspace as "a concept describing a widespread, interconnected digital technology" [Cyberspace 2020]. This definition could also be used for digital space. Other similar terms such as digital world, cyber world, virtual space, and virtual world can be considered as well. Cyberspace has been discussed since the mid-1990s when the word was coined by several people including William Gibson. The word cyberspace was given prominence in his book, Neuromancer [Gibson 1984]. "Digital" was elaborated by many people including Nicholas Negroponte. He wrote the book, Being Digital in 1995 [Negroponte 1995]. Digital space is a more neutral term than cyberspace. Digital space is more harmonized with digital economy and digital society than cyberspace, too. Cyberspace tends to imply cybersecurity and cyber warfare, especially in the USA and Europe. In 2010, the US White House issued a report entitled "International Strategy for Cyberspace" [White House

2012]. The US government designated a ‘Cyber Command’ as the fifth domain after land, sea, air, and space. The European Union as well as the UK government followed suit by forming similar organizations. These initiatives brought worldwide attention to the ideas of cyberspace as well as cyber warfare.

(2) Digital Space

Digital Space, Real Space, and Mixed Space

Digital space is a virtual space that is typically based on the Internet whereas real space is based on the physical world we live in. Additionally, there is mixed space consisting of both digital space and real space. Figure 1 shows a representation of these spaces.

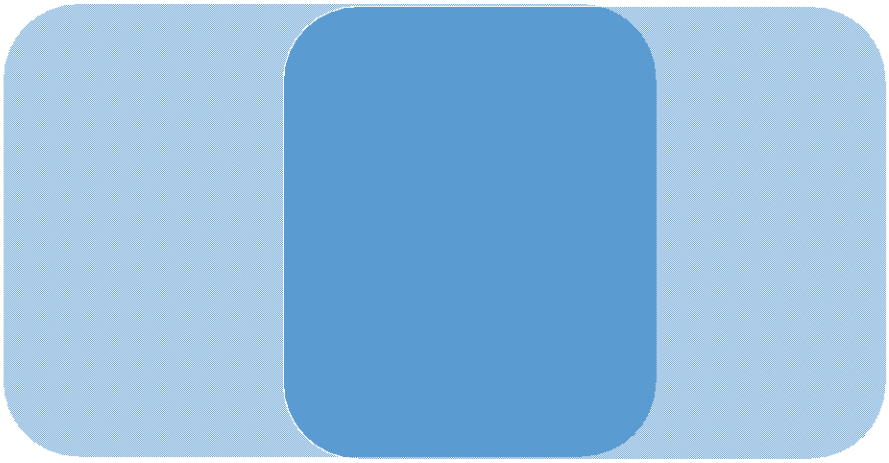


Figure 1 Digital Space, Mixed Space, and Real Space

Some mixed spaces are called cyber-physical systems, such as a sensor-based network system where the Internet and other networks are used [Cyber-Physical 2020]. Many Internet-based systems tend to be mixed spaces rather than pure digital spaces without any real space component.

Digital Space and the Internet

Digital space, when referring to digital society and digital economy, has the Internet as its infrastructure in most cases. But some digital spaces have other network infrastructures – for example, a telephone system without the Internet, a television system without the Internet, or a

sensor-based network system [Claffy 2013]. Digital space has various aspects including cybersecurity, artificial intelligence, data, social media and Internet of things (IoT) among others. See Figure 2 for a diagrammatic representation of digital space, its subspaces, its aspects, and infrastructure.

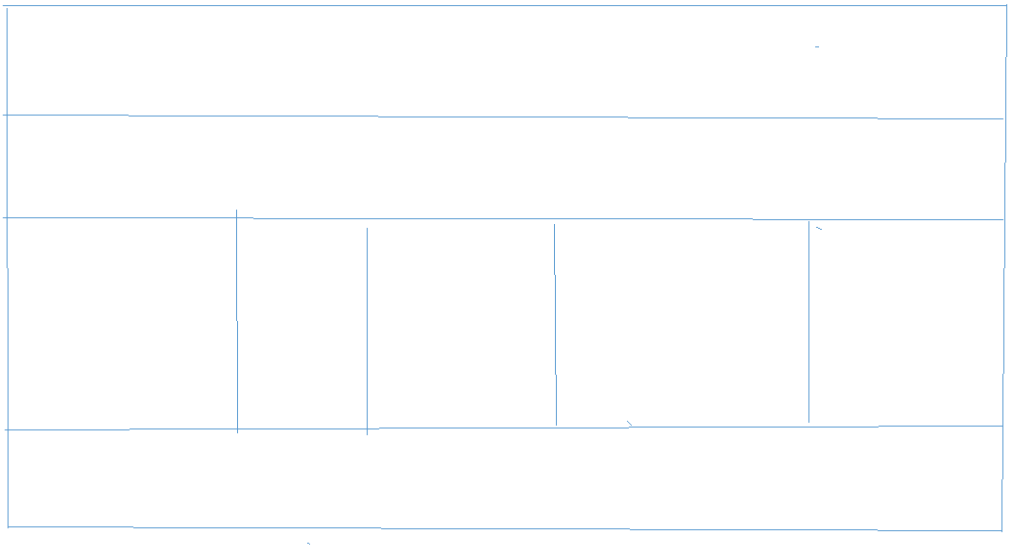


Figure 2 Digital space, Subspace, Aspects and Infrastructure

(3) Subspaces of Digital Space; Digital Economy and Digital Society

David Clark, in his paper "Three Views of Cyberspace", emphasized three facets [Clark 2011]:

Cyber Security
Cyber Economics
Cyber Society

Anthony Giddens, in his paper "Four Dimensions of Globalization", proposed four dimensions of globalization to which Gabriela Tejada added culture as the fifth dimension [Tejada 2007, Giddens 1991]:

World Capitalist Economy
Nation-State System
World Military Order
(International) Division of Labor
Culture

Kilnam Chon proposed the following major aspects in his paper [Chon 2013]:

CyberSociety
CyberSecurity
CyberEconomy
CyberNation-State
Cyber Environment

Digital Society

Digital society, including digital culture and digital life, is closest in meaning to 'the Internet' as they cover a similar semantic domain. With this understanding, digital society governance would be similar to Internet governance [IGF 2020]. Both digital society governance and Internet governance cover multiple social issues such as privacy, security, abuse, addiction, and violence, among others. The concepts of digital society and digital culture cover a range of contents, but the term 'the Internet' tends to cover this same range in a more partial fashion. The Web Index by the Web Foundation covers various aspects of digital society as well as digital economy, as many indexes on digital space tend to consider only the digital economy [Web 2012].

Digital Economy

Digital economy is one of two subspaces of the digital space that has been developed extensively in this century. UNCTAD's Digital Economy Report 2019 stated:

"In 2016, the Digital Economy represented $11.5 trillion, or 15.5 percent of global GDP – 18.4 percent of GDP in developed economies and 10 per cent in developing economies, on average. It found that the digital economy had grown two and a half times faster than global GDP over the previous 15 years, almost doubling in size since 2000."

There are other indexes on the digital economy including Internet Matters by McKinsey, and the Network Readiness Index by the World Economic Forum [UNCTAD 2019; McKinsey 2012; World 2019; Boston 2011].

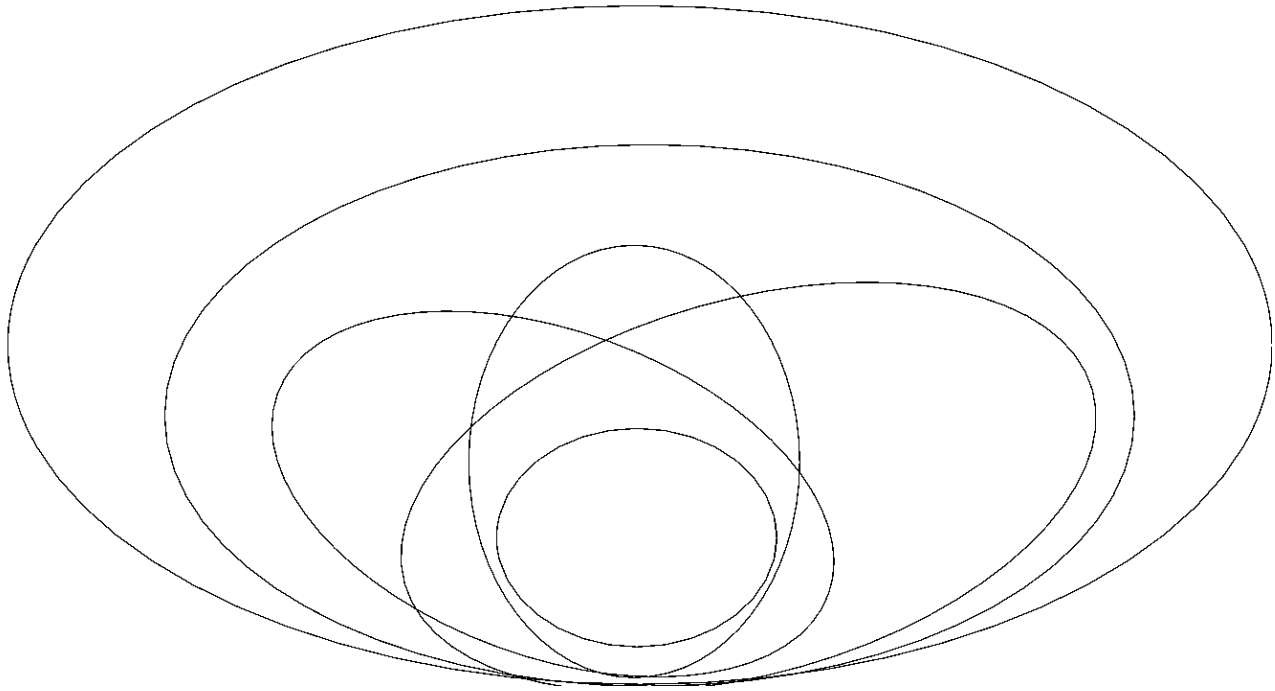


Figure 3 Digital Economy and Other Economies

(4) Aspects of Digital Space

There are the following six aspects of digital space which are covered in this chapter;

Artificial Intelligence (AI)
Data
Internet of Things (IoT)
Cybersecurity
Social Media
Blockchain

These aspects were covered at Asia Pacific School on Internet Governance (APSIG) in its annual schools in 2010s [APSIG 2020]. Governances of these aspects were also covered in the APSIG annual schools in 2010s.

In this chapter, we will cover these six aspects. We would like to see a "complete" set of the aspects sometime in future.

Artificial Intelligence (AI)

Artificial intelligence (AI) with the Internet and other technologies had the major development in this century [Lee 2018; Chon 2018b; McKinsey 2018; PwC 2017; Stanford 2015; Russell 2019]. Most of the current AI development is closely coupled with the Internet along with data and

high-performance computing which is typically based on cloud computing as well as AI algorithms. Kai-Fu Lee calls this development the first wave of AI, which is taking place in the first decades of the twentieth century.

Almost all major companies working on AI are also the major Internet companies. They include Amazon, Apple, Facebook, Google and Microsoft in the USA, and Alibaba, Tencent, and Baidu in China among others. We expect the close symbiotic relationship between AI and the Internet to be kept for a long time to come.

Consulting companies such as McKinsey and PwC forecasted AI's contribution to the global economy at around $15 to 20 trillion in 2030 [McKinsey 2018; PwC 2017]. This is roughly 15-20% of the global economy. AI is expected to impact almost every aspect of the economy and society in the coming years. AI governance is an important issue for the digital society, too, and will be described in the next chapter along governances of other aspects.

Data

Data, in particular big data, also has a symbiotic relationship with the Internet. We had one zettabyte in the world in 2009. The growth of data in the digital space was 33 zettabytes in 2018 and is expected to be 175 zettabytes in 2025 with an exponential growth curve in the foreseeable future [IDC 2018]. The big data is also a necessary component of AI growth. Handling of these data raises many issues including privacy, ownership of the data, and abuse of the data among others. Data governance in the next chapter explores on these issues including General Data Protection Regulation (GDPR), which was developed in the EU recently [Park 2018; EU 2016; AccessNow 2020].

Internet of Things (IoT)

Internet of Things (IoT) is developed to serve devices rather than people through the Internet. IoT development started in the last century, and grew substantially in this century and surpassed the human users in this decade [Chon 2017; Gartner 2017; Kondepudi 2015]. We expect the number of devices to be connected to the Internet to grow from around 10 billion in 2015 to 100 billion or more in the next decade. We also had Mirai, the first case of malware through IoT in 2016. IoT governance including IoT security and standardization are important issues now [IETF 2019; Kondepudi 2015].

Cybersecurity

Cybersecurity has been one of the most visible aspects of digital space in this decade, partly due to the addition in 2011 of the cyber domain to the four previously recognized domains – land, sea, air, and space – in the military conceptualization by the USA, EU, and UK governments. Specifically, the organizations charged with preparing for cybersecurity and cyber warfare are as follows:

USA: Cyber Command
EU: European Network and Information Security Agency
UK: Government Communications Headquarters

Many conferences on cybersecurity were held in the twenty-first century. Some worthy of mention include the following:

Black Hat Conference
International Conference on Cyberspace
Cyber Dialogue
DEF CON
ECIR Workshop
Global Cyberspace Cooperation Summit
USENIX Security Symposium

The Stuxnet incident in 2011 as well as the cyber attack in Estonia changed the cybersecurity landscape by bringing the concepts of cyber warfare and cyber weaponry into currency [Sanger 2012; Clarke 2010].

Cooperation on cybersecurity incident responses have been coordinated nationally, regionally and globally with establishment of organizations after the first worm, called Morris Worm in 1988 [Morris 2020]. The cooperation started with Computer Emergency Response Team Coordination Center (CERT/CC) in 1988 and Forum of Incident Response and Security Team (FIRST) in 1990 [CERT 2020; FIRST 2020]. Please refer Chapter 5 Cybersecurity of Asia Internet History, Third Decade (2000s) on these organizations. Please also refer APSIG on its classes on cybersecurity and cybersecurity governance [APSIG 2020].

Social Media

Social media is another important aspect in this century. Please refer Chapter 3 Social Media of Asia Internet History, Third Decade (2000s) for detail description. People tend to access social media for interacting in the digital space rather than the traditional Internet applications. Notable social networking service websites include Facebook, Twitter, Instagram, Weibo, and LinkedIn. Messaging services are also very popular, and they include WhatsApp, Facebook Message, WeChat, Line, and Kakao Talk. Social media is replacing the traditional Internet applications, particularly in East Asia where the messaging service and e-commerce as well as video are dominant applications now. Please also refer Section 3.5 Social Media Governance of Asia Internet History, Fourth Decade (2010s) for additional information.

Blockchain

Blockchain technology was invented by Nakamoto as he published his paper, “Bitcoin: A peer-to-peer electronic cash system” in 2009 [Nakamoto 2009]. The blockchain is “a growing list of records, called blocks, that are linked using cryptography”, and it is used for digital currencies as well as other distributed ledgers that record transactions in a verifiable and permanently recorded manner with no central administrator [Blockchain 2020; Distributed Ledger 2020]. Please refer Section 2.3 Blockchain for further description.

Other Candidate Aspects

Digital Nation State may cover legal systems for digital space as well as the international relations in digital space, which may be substantially different from those of real space. Explorations on Cyber International Relations (ECIR) covers the cyber nation state extensively – in particular, the facet of international relations [ECIR 2012]. The International Conference on Cyberspace also covers the international relations aspect of the cyber nation state [Cyber 2011].

Digital Environment is a new aspect candidate that needs to be studied thoroughly. The digital environment on its own is very important including both the (sustainable) digital environment itself, as well as the requirements of the cyber environment needed to support a sustainable physical environment [Chon 2012e]. While we work on a sustainable digital environment, we also need to work on mixed environments that consist of digital and physical environments including cyber-physical systems.

Names and Numbers are managed by Internet and other organizations globally. IP addresses in both their IPv4 and IPv6 formats as well as other numbers including the Autonomous System Number are managed by the Number Resource Organization (NRO) with the close cooperation of the Internet Assigned Numbers Authority (IANA) of the Internet Corporation on Assigned Names and Numbers (ICANN) now. Media Access and Control (MAC) address is a unique identifier assigned to a network interface for communications. It is typically used with Ethernet with MAC address allocation being handled by IEEE through its 802 Committee. Domain names are managed by ICANN including Top Level Domain Names (TLDs) in English alphabets and other characters. International Organization for Standardization (ISO) handles the standardization of information technology including country codes, which are used for the domain name and others.

Some of the following areas may be considered as digital space aspects, too.

Digital Education
Digital Labor
Digital Health

Please refer Chapter 8 Online Education of Asia Internet History, Third Decade (2000s) on digital education.

(5) Global Standards

Global standards for digital space are handled by various organizations with the close collaboration of national, regional and global standards bodies, which include the following:

- Institute of Electrical and Electronics Engineers (IEEE)
  IEEE is a technical professional organization for advancement of technology. IEEE Standard Association works on industry standards through 802 Committee and the related registration authority on MAC address.

- Internet Engineering Task Force (IETF)
  IETF is the standards body for Internet protocols, and it was founded in 1986, taking over the

work of the Network Working Group of the ARPANET Project which begun in1969. This includes Request for Comments (RFC), the Internet standard documents.

- International Organization for Standardization (ISO)
  ISO handles variety of standards including information processing. Many of them are relevant to Digital Space.

- International Telecommunication Union (ITU)
  ITU handles standardization and allocation on telecommunication including spectrum allocation [Restrepo 2019].

- World Wide Web Consortium (W3C)
  W3C is the standards body for WWW-related technologies such as HTML and HTTP.

- The 3rd Generation Partnership Project (3GPP)
  The 3GPP is a collaboration among the telecommunications associations of the USA, Europe, East Asia (China, Japan and South Korea) to develop standards for the third-generation mobile phone system and next generation mobile phone systems.

(6) Governance of Digital Space and Its Aspects

The Working Group on Internet Governance (WGIG) of the United Nations defined Internet governance as follows [WGIG 2005];

> "*Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*"

The Internet governance principles was revised at NETmundial Meeting in 2014 [NETmundial 2014].

For digital space, we may look into broadening the concept of the governance now. Many aspects of digital space are in their early stages, and their governances may be substantially different from the Internet governance. The concept of the governance in the Internet governance may not work well in some aspects as we are discovering in cybersecurity governance and artificial intelligence governance. The ECIR workshop on "Who controls cyberspace?" is of great interest since we still do not know how digital space will be governed [ECIR 2012].

Some aspects of the digital space governance may be appropriate to consider now. On the other hand, cybersecurity governance may be premature, which is somewhat similar to the state of nuclear technology governance in the 1950s [Nye 2011]. We may eventually need cybersecurity governance in a similar way to nuclear technology governance, which requires treaties and inspection protocols.

The IGF Workshop on "Cyberspace Governance – Exploration," was held in 2013 to discuss digital governance [Chon 2013b]. Asia Pacific School on Internet Governance offered classes on

governances of various aspects in 2016-2019 including Data Governance, IoT Governance, Cybesecurity Governance, AI Governance, and Social Media Governance [APSIG 2020].

Artificial Intelligence Governance

Artificial intelligence governance has finally attracted much attention globally with various conferences and meetings, and various publications [Chon 2019; Russell 2019; FLI 2017]. AI governance may be substantially different from Internet governance in many ways. First of all, we are unable to develop any consensus on the AI principles to start with, and we have many versions of the AI principles at present. We may also need regulations by governments since human safety is at stake such as autonomous driving. AI was included in the existential risk list issued at Cambridge University and others [Cambridge 2020; BERI 2020]. Industry is playing a major role in AI governance in this century, too.

Data Governance

Data governance is closely related to AI governance as well as privacy governance [Park 2017]. The European Union (EU) came up with General Data Regulation Policy (GDPR) in 2016, which was accepted by many countries and regions in addition to Europe [EU 2016]. We expect GDPR to take a lead on the data governance development in the coming years [AccessNow 2020].

IoT Governance

IoT governance may be developed similarly to the Internet governance, and we may consider the IoT governance as an extension of the Internet governance [Chon 2017]. The differences in these two governances may include standardization and users. The IoT standards are mostly developed by industry consortia rather than global non-profit organizations such as IETF [Kondepudi 2015]. The number of "users" in IoT exceeded human users of the Internet in this decade already, and we expect to have more than 100 billion devices connected to the Internet in the coming decades.

Cybersecurity Governance

Cybersecurity governance has been addressed actively in this decade [Tikk 2018; Chon 2016; Komiyama 2019; Cyberspace 2011]. There was much effort on developing the global norms on cybersecurity through UN and other organizations. 2015 UN GGE Report endorsed the Cyber Norms of Behavior in Peace Time as follows [UN 2015];

- *states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;*
- *states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure;*
- *states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity.*

But a consensus among state governments has not been developed. It may take much effort and time before we could come up with a good cybersecurity governance model for the world. Meantime, there is reasonably good governance on the operational level through national and regional computer security incident response teams (CSIRT) with the global organization called Forum of Incident Response and Security Team (FIRST) [CERT 2020; FIRST 2020].

Social Media Governance

Social media governance is attracting much attention lately [Park 2019; Park 2020]. We are having many important issues on the social media governance including misinformation, abuse, and ownership on social media data among others. The social media governance is becoming closely related to the AI governance now as AI technologies are applied to the social media now. This makes the social media governance much more complex.

Other Governances

Governance of other aspects such as privacy and other human rights issues as well as social issues such as education and work may need to be addressed. The governances on these aspects may take much different formats than the governance of other aspects, and they would be the major challenges in the coming years and decades.

(7) Issues

Global forums on governance of digital space

A few global forums currently exist that deal with digital space, including the following:

RightsCon
Internet Governance Forum (IGF)

RightsCon covers almost all areas of digital space with its over twenty program categories [RightsCon 2019]. Internet Governance Forum also covers many areas with four tracks; data, environment, inclusion and trust in its 2020 meeting [IGF 2020]. The global forums on digital space are still in their infancy as many of them were founded recently or their coverages have been expanded to cover digital space. We need to look into what we need in this area globally, regionally, and nationally.

Globalization vs Fragmentation

The digital space is being globalized including aspects and subspaces as well as its infrastructure; the Internet and the telecommunication networks. We may be facing fragmentation of the digital space includiing the Internet in the coming decades [Drake 2016; Mueller 2017].

(8) Concluding Remarks

The digital space, including its various aspects, is still in its early conceptual stages, as explained in this section. We examined definitions of digital space along its subspace: the digital society and the digital economy. Then, we explored five aspects of the digital space. We would like to

see further studies on the digital space, its subspaces, and its aspects as well as their governances in the coming years.

The digital space is being developed at a rapid pace in this century. AI, data, and IoT are playing major roles in the development of the digital space now. All of the trillion-dollar companies are from the digital space now. These trends would continue in the coming decades. The current coronavirus-19 (COVID-19) crisis is also contributing to the development of the digital space.

I wrote the article, "Cyberspace – What is it?" and organized the workshop, "Cyberspace – Exploration" in 2013. We would like to revisit the digital space within the coming decade to find out if we have to go through another major revision on the digital space.

References

[AAAI 2018] AAAI and ACM, AI, Ethics and Society Summit, Honolulu, 2018.
[AccessNow 2020] AccessNow, Two years under the EU GDPR; An implementation progress report, 2020.
[Almeida2016] Virgilio Almeida, Cyberspace Governance, Harvard University, 2016.
[APSIG 2020] Asia Pacific School on Internet Governance, APSIG.asia, 2020.
[Asia 2020] Asia Internet History Project, Third Decade (2000s), 2020.
[Attali 2008] Jacques Attali, After the Crisis, 2008.
[Baig 2020] Aamer Baig, et al., The COVID-19 recovery will be digital: a plan for the first 90 days, McKinsey, 2020.
[Behrens 2019] A. Behrens, Positive and negative effects of digital life, 2019, Positive Negative Impact, 2019.
[Bell 2020] We need mass surveillance to fight COVID-19, but it needs not have to be creepy, MIT Tech Review, 2020.
[Berkeley 2020] Berkeley Existential Risk Initiative, 2020.
[Black 2010] Black Hat Computer Security Conference, July 2010.
[Bonvanie 2017] Rene Bonvanie, Sharing of data, algorithm, Global Cyberspace Summit, 2017.3.17.
[Boson 2011] Boston Consulting Group, e-Intensity, 2011.
[Brookings 2020] Brookings, How the EU plans to rewrite the rules for the internet (DSA), 2020.
[Brooks 2020] Joseph Brooks, An extraordinary period in internet history: Akamai data shows 30% surge in internet traffic, 2020.
[Bruegel 2020] Bruegel Annual Meeting, EU digital strategy at a time of geopolitical stress, 2020.9.2.
[Cambridge 2020] The Center for The Study of Existential Risk (CSER), Cambridge, 2020.
[Cerf 2020] Vint Cerf, Internet lessons from COVIT19, COVID19 and Internet Openness, 2020.
[CE 2011] Council of Europe, The (Budapest) Convention on Cyber Crime, 2011.
[CERT 2020] CERT, Wikipedia, 2020.
[Choi 2019] Yang Hee Choi, Future of ICT, Computer History Workshop, Jeju, 2019.
[Chon 2012e] Kilnam Chon, Ecological Internet, NORDUNET, 2012.
[Chon 2013] Kilnam Chon, "Cyberspace – What is it?", Cyber Commons. 2013.
[Chon 2013b] Kilnam Chon, et al., Workshop on Cyberspace Governance – Exploration, IGF,

Bali, October 2013.
[Chon 2013c] Kilnam Chon, Cyberspace – “What is it?”, 2013.
[Chon2014] Kilnam Chon, Cyberspace Governance, 2014.
[Chon2016] Kilnam Chon, Cybersecurity Governance, 2016.
[Chon2017] Kilnam Chon, IoT Governance, 2017.
[Chon2018] Kilnam Chon, Digital Governance, 2018.
[Chon 2018b] Kilnam Chon, AI: Past and Present, 2018.
[Chon2019] Kilnam Chon, AI Governance, 2019.
[Chon2019b] Kilnam Chon, Internet Governance and AI Governance, 2019.
[Chon 2019c] Kilnam Chon, Internet Governance History, 2019.
[Chon 2020] Kilnam Chon, Digital Space - Introduction, 2020.
[Chon 2020b] Kilnam Chon, Coronavirus and Internet, 2020.
[Choucri 2012] Nazli Choucri, Cyberpolitics in International Relations, MIT Press, 2012d.
[CFR 2018] Council of Foreign Relations, “What is the digital society we want to build together?”, 2018.
[Claffy 2013] KC Claffy and David Clark, Platform Models for Sustainable Internet Regulation, TPRC 41, 2013.
[Clark 2011] David Clark, Three Views of Cyberspace, ECIR, Harvard-MIT, 2011.
[Clarke 2010] Richard Clarke, Cyber War, 2010.
[CyberCommons 2012] CyberCommons.net, 2012.
[CyberDialogue 2013] Cyber Dialogue Conference, 2013.
[Cyber-Physical 2020] Cyber-Physical System, Wikipedia, 2020.
[Cyberspace 2011] Global Conference on Cyberspace, 2011.
[Cyberspace 2020] Digital Space, Wikipedia, 2020.
[Dafoe2018] Allan Dafoe, AI Governance: Research Agenda, Oxford University, 2018.
[Dafoe2019] Allan Dafoe, AI, Strategy, Policy and Governance, Beneficial AI, 2019.
[DistribtuedLedger 2020] Distributed Ledger, Wikipedia, 2020.
[DocFilm 2019] DocFilm, Omnipotent Amazon, DW, 2019.05.11.
[Drake 2016] William Drake, et al., Internet Fragmentation – Overview, World Economic Forum, 2016.
[DW 2018] DW, Cleaners: Social media’s shadow industry, Part 1 and 2, 2018.
[EastWest 2015] East West Institute, Promoting international cyber norms, 2015.
[Economist 2010] Cyberwar, Economist, 2010.7.1.
[EC 2020] European Commission, Shaping Europe's digital future, 2020.02.19.
[ECIR 2012] ECIR Workshop: “Who Controls Cyberspace?”, 2012.
[ECIR 2013] Explorations in Cyber International Relations, ECIR.MIT.edu.
[ESCAP 2020] ESCAP/APCICIT, How Korea turned tide on COVIT-19 using ICT, 2020.4.28.
[EU 2016] EU, General Data Protection Regulation (GDPR), 2016.
[European 2020] European Central Bank, Payments in a digital world, 2020.
[Facebook 2020] Mike Schroepfer, Social Spaces, Emtech MIT, October 2020.
[Farrell 2019] H. Farrell and A. Newman, Weaponized interdependence: how global economic networks shape state coercion, International Security, MIT Press, 2019.
[FIRST 2020] FIRST.org, 2020.
[FLI 2017] Future of Life Institute (FLI), Asilomar AI Principles, 2017.

[Gartner 2017] Gartner says 8.4 billion connected things will be in use in 2017, 2017.
[Gibson 1984] William Gibson, Neuromancer, Ace Books, 1984.
[GlobalCommons 2020] Tokyo Forum 2020, Center for Global Commons, Tokyo University, 2020.12.
[Grey 2020] John Grey, Why this crisis is a turning point in history, New Statesman, 2020.3.
[Heaven 2020] Will Heaven, Why the coronavirus lockdown is making the internet stronger than ever, MIT Tech Review, 2020.
[ICANN 2020] ICANN, ICANN's Early Days, ICANN History Project, 2020.
[IDC 2018] IDC, Data Age 2025: Digitization of the World, 2018.
[IEEE 2015] IEEE, IoT Ecosystem Study – Executive Summary, 2015.
[IETF 2019] IETF, Internet of Things (IoT) Security, RFC 8576, 2019.
[IGF 2020] Internet Governance Forum.
[Internet 2020] Internet World Stats, 2020.
[Kagermann 2020] H. Kagermann & U. Wilhelm, European Public Sphere-toward digital sovereignty for Europe, 2020.
[Komiyama2019] Koichiro Komiyama, Cybersecurity Governance, APSIG, 2019.
[Kondepudi 2015] Sekhar Kondepudi, IoT Standard War, Forum on IoT, ITU, 2015.
[Korean 2020] Korean Government, Flattening the curve on COVID-19, UNDP, 2020.4.16.
[Larik 2015] Joris Larik, Cyber Governance: challenges, solutions and lessons for effective global governance, 2015.
[Liaropoulos 2016] A. Liaropoulos, Exploring the complexity of digital space governance, J. of Information Warfare, 2016.
[McKenzie 2011] Alex McKenzie, INWG and the conception of the Internet: An eyewitness account, IEEE Annals of the History of Computing, Vol 33, No1, 2011.
[McKinsey 2011] McKinsey, Internet matters, 2011.
[McKinsey 2018] McKinsey, Promise and challenge of the age of AI, 2018.
[McKinsey 2020] McKinsey, COVID-19 recovery will be digital: A plan for the first 90 days, 2020.5.14.
[McKinsey 2020b] McKinsey, Digital strategy in a time of crisis, 2020.4.22.
[Morris 2020] Morris Worm, Wikipedia, 2020.
[Mueller 2017] Milton Mueller, Will the Internet fragment?, 2017.
[Munich 2011] Munich Cybersecurity Conference, 2011.
[Nakamoto 2009] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009.
[Negroponte 1995] Nicholas Negroponte, Being Digital, 1995.
[Netmundial 2014] Netmundial, 2014.
[NSCAI 2021] National Security Commission on AI, Final Report, NSCAI.gov, 2021.
[Nye 2011] Nuclear lessons for cybersecurity, 2011.
[Nye 2014] Joseph Nye, Regime complex for managing global cyber activities, GCIG, 2014.
[Ochiai 2018] Yoichi Ochiai, From Ubiquitous to Digital Nature: art, entertainment, design, YouTube, 2018.(Japanese)
[OECD 2017] OECD, Digital Economy Outlook, 2017.
[Park2018] KS Park, Data Governance, APSIG, 2018.
[Park 2019] KS Park, Social Media Governance, APSIG, 2019.
[Park 2020] KS Park, Social Media Governance, 2020.

[PwC 2017] PwC, Global Artificial Intelligence Study: Sizing the Prize, 2017.
[Restrepo 2019] Joaquin Restrepo, Spectrum allocation for 5G international framework, 2019.
[Russell 2019] Stuart Russell, Human Compatible, 2019.
[Sanger 2012] David Sanger, Confront and Conceal, 2012.
[Security 2018] Security Today, Cyber Ecosystem, 2018.
[Seoul 2013] International Conference on Cyberspace, Seoul, 2013.
[Stanford 2015] Stanford University, Stanford AI 100 Report, 2015.
[Stevens 2018] Tim Stevens, Cyberweapons: Power and governance of the invisible, Journal of International Politics, 2018.
[Taparin 2020] Hans Taparin, Future of college is online, and it's cheaper, New York Times, 2020.
[Tejada 2007] Gabriela Tejada, The four dimensions of globalization according to Anthony Giddens, GLOPP, 2007.
[Tikk 2018] Eneken Tikk, Cybersecurity Governance, APSIG, 2018.
[UN 2015] UN GGE Report, Major players recommending norms of behavior, 2015.
[UN 2019] Report of UN Sec. General's High Level Panel on Digital Cooperation, Age of Digital Interdependence, 2019.
[UN 2020] Report of Secretary-General: Roadmap for digital cooperation, June 2020.
[UN 2019] UNCTAD, Digital Economy Report 2019.
[UNDP 2020] UNDP Flattening the curve on COVID-19, 2020.4.16.
[Victoria 2019] A. Victoria, Cybersecurity and Artificial Intelligence, 2019.
[Web 2012] Web Foundation, Web Index.
[Web 2017] Web Foundation, White Paper on AI: Road ahead in low and middle-income countries.
[WGIG 2005] Working Group on Internet Governance, WGIG Report, 2005.
[White House 2011] Whitehouse, International Strategy for Digital space, 2011.
[World 2019] World Economic Forum, Network Readiness Index, 2019.
[Worldometers 2020] Worldometers.info, 2020.
[WSIS 2005c] World Summit on Information Society (WSIS), Tunis Agenda, 2005.
[Wu 2003] Tim Wu, Net Neutrality, 2003.
[Xiang 2020] N. Xiang, Why China has so few options to hit back over US ban on TikTok, Nikkei Asian Review, 2020.
[Zuboff 2019] Shoshana Zuboff, The age of surveillance capitalism, 2019.

Appendix Coronavirus and Digital Space

Coronavirus 19 (or SARS-CoV-2, or COVID-19) is taking over the world since it was announced as pandemic by the World Health Organization in March 2020. There are a total confirmed infection cases of 4,721,828 and total confirmed deaths of 313,260 affecting 213 countries and territories as of 2020.05.17 [Worldometers 2020]. This pandemic is an extraordinary case in modern human history.

John Grey wrote an article, "Why this crisis is a turning point in history" in 2020 with the following quote [Grey 2020];

"….There will be celebrations as the pandemic recedes, but there may be no clear point when the threat of infection is over. Many people may migrate to online environments like those in Second Life, a virtual world where people meet, trade and interact in bodies and worlds of their choosing….."

Brian Chen wrote the following in the New York Times on 2020.04.15:

"A computer with a good internet connection, communication apps and entertainment are the only tech we really need, ever."

Many people around the world really live in the digital space much of time lately due to the COVID-19 pandemic. A recent study indicated a 30% sudden increase of Internet traffic in East Asia according to Akamai [Brooks 2020]. Many could not go out for work, school, and so on due to nation-wide lockdowns. Moreover, they are afraid of infection by meeting people physically, but feel comfortable to meet them in the digital space with computers, smartphones, television, and other audio-visual equipment since they offer non-contact meetings.

In many countries with lockdowns, regular K12 education as well as college education is now being done in the digital space rather than the physical world. Online education used to be a complementary tool. This is no longer the case [Taparin 2020]. Much of daily work is also done in the digital space rather than by commuting to offices. Much of shopping is similarly done in the digital space through e-commerce. This sudden change is due to the risk of infection in the real world through physical contacts.

The digital space with the current reasonable matured technologies is providing a very important alternative now. But it also has drawbacks, however, including the following.

- Handicapped people, physically or economically may have a similar or worse handicap in digital space.
- Governments tend to use digital space technologies for surveillance and other privacy infringement to fight against the pandemic, and may not give up these technologies when the pandemic is over.

What will happen to the world after this pandemic is over? We may not be able to go back to the pre-COVID-19 world, and the digital space of the post-COVID-19 will be different from the digital space of the pre-COVID-19 [McKinsey 2020]. We need to carefully look into issues on the digital space and the mixed space for the post-COVID-19 world.

Section 2.2 Data

Kilnam Chon

Introduction

Data is one of the major aspects of the digital space along AI, IoT, cybersecurity and social media. Please refer Figure 2.4.1 on the digital space, and data and other aspects.

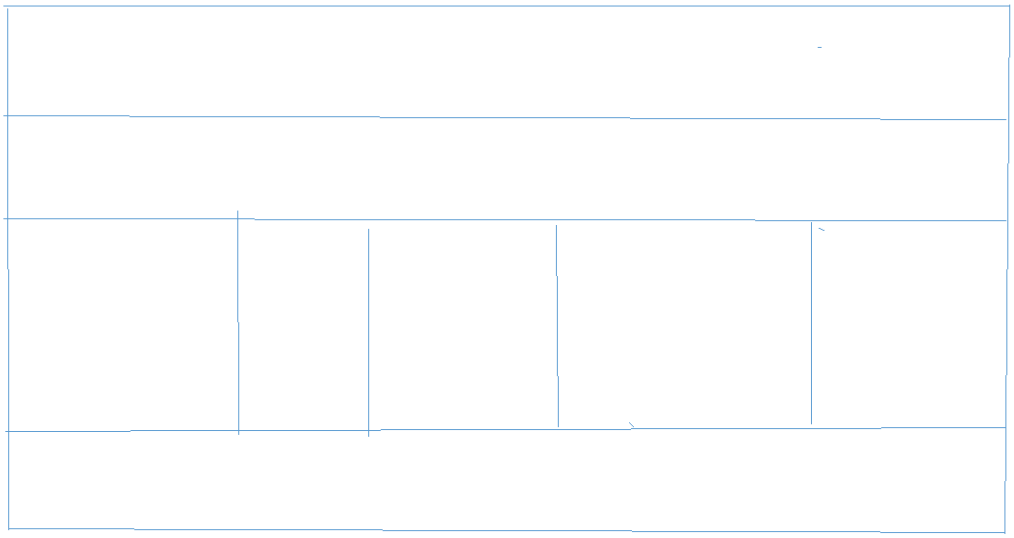


Figure 1 Digital Space, Digital Subspaces, Aspects and Infrastructure

There are several kinds of data; video, images, graphics and text. The video dominates the total data volume generated in the Internet. The data volume has been growing exponential growth since the Internet became popular in the last century.

"***Data science*** *is an inter-disciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from many structural and unstructured data*" [DataScience 2020]. **Data engineering** may be considered as part of the data science handling engineering aspect of data science. ***"Data Management*** comprises all disciplines related to managing data as a valuable resource" [DataManagement 2020].

In this section, we cover the following topics;

Exponential Growth of Data and Big Data

Data Center

Privacy and Data

Artificial Intelligence and Data

Data Archive

Open Data

Exponential Growth of Data and Big Data

Data generated in the Internet has been growing exponentially. The annual sizes of the global datasphere were less than one Zettabytes in 2010, and around 25 Zettabytes in 2017. It is expected 175 Zettabytes in 2025 [ISC 2017; EC 2020].

The exponential growth started with the birth of digital technologies including digital storages and digital computers as well as the Internet in the twentieth century. We expect this exponential growth will be sustained in foreseeable future in the twenty-first century.

Big data in petabytes, exabytes, and zettabytes is "*a new field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data processing application software"* [BigData 2020]. It may be considered as a special branch of data science and data managemente. The big data is also a critical component of artificial intelligence study.

Data Center

Data were used to be stored in computer systems in the twentieth century. The data have been increasingly stored in data centers which are dedicated to handle data for in-house usage or for commercial and public services. Many major Internet companies such as Google, Amazon and Microsoft among others have dedicated data centers around the world with their networks in addition to other networks to serve their data centers as well as their users. These companies also host web services. Many large organizations have the dedicated data centers even though they also use public data centers.

Data centers as well as the Internet consume much electricity lately. "*One study in 2018 indicates the world's data centers consumed 205 terawatthours of electricity, or about one percent of all electricity consumed that year worldwide"* [DataCenter 2018]. Thus, saving on the electricity and other environmental consciousness are becoming very important among the Internet companies. For example, Google and Facebook announced their plans to make them carbon neutral within a decade or two, similarly to Amazon, Apple and Microsoft [Guardian 2020].

Privacy and Data

Privacy became increasingly important as computing and networking became pervasive. Many Internet companies, in particular social networking service companies such as Facebook and Google have extensive data on their users. State governments around the world also have extensive data on their citizens, too. These data became serious issues on privacy protection around the world. This is particularly true with recent development of AI technologies related to data and privacy. Many governments enacted privacy laws to protect their citizens. European Union came up with the General Data Protection Regulation (GDPR) in 2016 on data protection and privacy [GDPR 2016]. GDPR is becoming a leading regulation on the privacy and data

protection globally. Additionally, European Union came up with Digital Market Acts and Digital Service Acts in 2020.

Please refer further information on privacy and data in Section 3.2 Data Governance and Section 3.5 Social Media Governance [EC 2020].

Artificial Intelligence and Data

Artificial intelligence (AI) and data, in particular big data are working together since they need each other. AI needs data, in particular big data and good quality data. On the other hand, handling of big data tends to require AI technologies, too. Data science and AI research are also working together. Many conferences on AI and data science cover each other. This is particularly true on machine learning which depends on big data on its performance.

Data Archive

Data archive attracts much attention lately. There are many non-profit and governmental archives including many libraries around the world. Their efforts are related to "open data" which is explained in the next subsection. Traditional libraries such as national libraries increasingly cover digital libraries. Many museums as well as universities are also working on digital archives. There are also commercial archive companies in particular among the Internet companies, too.

Internet Archive may be one of the first major non-profit data archive organizations [Archive 2020]. It was founded in 1996 with "*the stated mission of universal access to all knowledge. It provides free public access to collections of digitized materials, including websites, software applications/games, music, movies/videos, moving images, and millions of books. In addition to its archiving function, the Archive is an activist organization, advocating a free and open Internet. The Internet Archive currently holds over 20 million books and texts, 3 million movies and videos, 400,000 software programs, 7 million audio files, and 463 billion web pages in the Wayback Machine"*.

YouTube is another notable case with one of the largest video archives, if not the largest video archive, in the world with "some Exabytes"[Quora 2020]. Anybody can upload their video to YouTube to archive their videos. Google including YouTube has estimated storage size of 10-15 Exabytes [Quora 2018] where many keep their files on video, pictures and text through Google Drive. Other Internet companies offer similar services around the world.

Open Data

"Open data is the idea that some data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control. The goals of the open-source data movement are similar to those of other "open (source)" movements such as open-source software, hardware, open content, open

education, open educational resources, open government, open knowledge, open access, open science, and the open web"[OpenData2020].

Open data is closely related to "Open Government Data (OGD)" as promoted by many governments and civil societies [OECD 2020]. Another important area is science data including non-textual data such as maps, genomes and chemical compounds among others.

References

[Archive 2020] Internet Archive, Wikipedia, 2020.
[BigData 2020] Big Data, Wikipeida, 2020.
[DataCenter 2018] DataCenterKnowledge.com, 2018.
[EC 2020] European Commission, A European strategy for data, 2020.02.19.
[GDPR 2016] EU, General Data Privacy Regulation, 2016.
[Gensler 2018] Gary Gensler, Blockchain and Money, 15.S12, MIT, 2018.
[Guardian 2020] Guardian, Facebook and Google announce plans to become carbon neutral, 2020.9.15.
[IDC 2017] IDC, Digital Ages 2025 study, 2017.
[IDC 2020] IDC, Global datasphere in 2018 reached 18 zettabytes, 2020.
[OECD 2020] Open Government Data (OGD), OECD, 2020.
[OpenData 2019] Tim Davies, et al., The State of Open Data: Histories and Horizons, 2019.
[OpenData 2020] Open Data, Wikipedia, 2020.
[O'Reilly 2021] Tim O'Reilly, Building a better data economy, MIT Tech. Review, 2021.
[Quora 2018] Quora.com, What is storage capacity of Google, 2018.
[Quora 2020] Quora.com, Estimate size of youtube may be in some Exabyte, 2020.
[DataScience 2020] Data Science, Wikipedia, 2020.
[DataManagement 2020] Data Management, Wikipeida, 2020.
[WEF 2019] WEF, How much data is generated each day?, 2019.

2.3 Artificial Intelligence – Overview

Kilnam Chon

Introduction

This section summarizes development of Artificial Intelligence (AI) since its inception in the mid-twentieth century to the present. AI may be classified as narrow AI and general AI [Artificial 2020; Tegmark 2017; Russell 2019; Helsinki 2018]. Narrow AI focuses on a specific task such as a game like Go and chess, language translation and so on. General AI, which we also call Artificial General Intelligence (AGI), can handle any intellectual task like a human. General AI focuses on human-level intelligence and super intelligence. In this article, we use the

phrase general AI to keep symmetricity to narrow AI. Most AI developments focus on narrow AI now. We may call narrow AI as AI lately.

This section covers overviews of the following topics;

AI History
AI Economy
AI Applications
Super Intelligence
Complex Systems
Governance
Conferences

AI History

In the 1940s, there were several important initial developments in information technologies including a bit, digital computers, a hyperlink models, and a neutral network model as well as cybernetics. Shannon defined the concept of the "bit" with 0 and 1 [Shannon 1948; IEC 2008]. Digital computers were developed in Germany, the UK, and the USA in the 1940s [Wikipedia 2019]. Bush proposed the concept of the hyperlink in his essay on Memex [Bush 1945]. However, its realization took 50 years until Tim-Berners Lee developed the World-Wide Web in 1990. A neural network model was developed by McCulloch and Pitts [McCulloch 1943]. Alan Turin wrote an article on intelligence and created the Turing Test [Turing 1950]. Norbert Wiener created the concept of cybernetics, which analyzed minds and machines [Wiener 1948].

The Dartmouth AI Workshop was held in 1956 where the term, "Artificial Intelligence" was used for the first time officially [Dartmouth 2020; Russell 2019].

With the availability of digital computers in the 1950s, the initial AI boom took place in the 1960s. However, AI researchers eventually encountered difficulty to realize AI applications, and the first AI winter came in the 1970s, as the initial optimistic views on AI disappeared. With the developments of neural networks and expert systems, the second AI boom appeared in the 1980s. Many AI researchers in Asia did not participate during the initial AI boom in the 1960s but participated from the second AI boom in the 1980s. Then, a second AI winter occurred in the late 1980s and early 1990s. The second AI winter was particularly damaging to the AI community, and many left AI activities. However, some AI researchers, including Geoffrey Hinton and his group, kept working on the AI research, in particular on the neural network, and came up with the deep neural network model [ACM 2019]. The neural network and related research led to the third AI boom in the 2010s. This was backed up with the availability of big data by Internet AI companies and high-performance computing based on cloud computing as well as various algorithms based on the deep neural network and other AI technologies.

AI Economy

PwC and McKinsey forecast the value addition by AI to the global economy in 2030 would be between 10 and 20 trillion dollars [PwC 2019; McKinsey 2018]. This amounts to 10-20% of the global economy. This gain tends to be taken by a few leading countries and a few leading companies since the nature of gain by the AI and other digital technologies are "winner takes

all". Thus, we will have an issue: How should the economic gain of trillion dollars made by AI be distributed?

AI Applications

Kai-Fu Lee in his 2018 book, *AI Superpowers: China, Silicon Valley, and the New World Order*, categorizes AI applications into four overlapping stages of waves: Internet AI, Business AI, Perception AI, and Autonomous AI [Lee 2018; Lee 2019]. Internet AI handles huge data through the Internet. In Business AI, data are handled as parts of business processes. In Perception AI, various aspects of perceptions such as eyes, ears, and other senses are handled. In Autonomous AI, machines and systems handle sensing and respond. Their examples include autonomous robots, and autonomous driving.

Super Intelligence

Nick Bostrom published a book, *Superintelligence*, in 2014 where he proposed that developing superintelligent AI may be possible in this century" [Bostrom 2014]. He focused on general AI in his book. General AI has progressed only slightly thus far. However, Bostrom argues that it will start to take off soon, reaching human level intelligence in this century, and reaching super intelligence later in this century. Eventually, the AI will taper off later in this century or the next.

Narrow super intelligence based on the development of machine learning systems has been explored by Deep Mind Technologies among other companies and research organizations. Deep Mind developed a series of AI systems in the 2010s: AlphaGo, AlphaZero, and AlphaFold [Deep 2018a; Deep 2018b; Russell 2018; Strogats 2018; Tegmark 2017; Harari 2018].

The initial AI system was AlphaGo Fan in 2015, which was developed to compete against the European Go champion. AlphaGo Fan was based on deep learning systems, and it won a match against a high ranking professional Go player for the first time in the history. The system was upgraded to AlphaGo Lee in 2016, which represented a major breakthrough. AlphaGo Lee competed against Lee Saedol, one of the top Go players in the world, and AlphaGo won the match by 4 games to 1. It was later upgraded to AlphaGo Master in 2017, which competed against other top ranking Go players without a single loss. Deep Mind developed Alpha Zero in 2017, which plays against itself to improve its capability, and it can play several games including Go, chess, and Shogi [Deep 2018a]. It beat AlphaGo Master easily. AlphaGo surpassed human-level intelligence in the game of Go, and it can be considered to have reached narrow super intelligence. In the case of AlphaZero, we may consider it is the first step beyond narrow AI toward general AI since it can cover more than one game.

Strogatz commented on potential issues with the algorithm and explainability of AlphaZero among other types of machine learning. He stated "AlphaZero gives every appearance of having discovered some important principles about chess, but it cannot share the understanding with us" in his article [Strogatz 2018]. Deep Mind also developed AlphaFold, which covers scientific discovery [Deep 2018b]. We may observe whether the Alpha Series of AI systems surpasses narrow AU and leads to general AI.

Complex Systems and Narrow AI

There are many complex systems such as the Internet, electric grids, and nuclear plants that are increasingly being handled by AI due to their complexity. These complex systems include large-scale systems such as the Internet, or real-time system such as financial system. In many cases, we have to delegate to AI systems to handle these complex systems since humans cannot handle them properly anymore, which may lead us to classify these as special cases of super intelligence.

Internet Governance, Digital Governance and AI Governance

Internet governance has gone through several decades of development since the 1970s, and we are increasing focusing on digital (technology) governance, which includes IoT governance, data governance, cybersecurity governance, social media governance, and AI governance among others.

One of the issues with governance is that it raises the following question: Can we apply Internet governance schemes, such as multistakeholderism and governance principles, to other digital governances? For most governances, we developed principles such as Internet Governance Principles and AI Principles as well as cybersecurity norms.

What constitutes AI governance is one of the major issues now. We may consider some of the following issues as the major issues of AI governance [Tegmark 2017; Russell 2019; AAAI 2019; Chon 2019; FLI 2017; FHI 2019];

Principles
Policy
Ethics and Human Rights
Accountability, Explainability, and (Algorithmic) Transparency
Security
Safety
Social and Economic Impact
Data

AI communities are working on the above issues. We have fairly solid results in some issues including the principles and the ethics, but most of the issues are still in their early stages of development [FLI 2017; EU 2019b; EU 2020; Dafoe 2018]

Please refer Chapter 3, “Digital Governance”, for detail descriptions of digital governance, and the governance of its aspects including artificial intelligence governance.

Major Conferences on AI and Machine Learning [Pal 2019]

NeurIPS – Neural Information Processing Systems
ICML – International Conference on Machine Learning
ICLR – International Conference on Learning Representations
AAAI – Association for the Advancement of Artificial Intelligence
CVPR – Computer Vision and Pattern Recognition

ICCV – International Conference on Computer Vision
GECCO – Generic and Evolutionary Computation Conference
COLT – Conference on Learning Theory
IROS – International Conference on Intelligent Robots and Systems
ICIP – International Conference on Image Processing

References

[ACM 2019] ACM, Turing Award, 2019
[Artificial 2020] Artificial general intelligence, Wikipedia, 2020.
[Bostrom 2014] Nick Bostrom, Superintelligence, 2014.
[Bostrom 2018] Nick Bostrom, AI will be the greatest revolution in history, 2018.
[Bush 1945] Vannevar Bush, As we may think, Atlantic, 1945
[Chon 2018] Kilnam Chon, Digital Governance, 2018.
[Chon 2018b] Kilnam Chon, Artificial Intelligence – Past and Present, 2018.
[Chon 2019] Kilnam Chon, AI Governance, 2019.
[Chon 2020] Kilnam Chon, Digital Space, 2020.
[CSER 2020] Cambridge; Center for Study of Existential Risk, Leverhulme Center for Future of Intelligence, 2020.
[CSET 2020] CSET, Mapping US multinationals' global AI R&D activity, 2020.
[Dafoe 2018] Alan Dafoe, AI Governance: Research Agenda, Center for Study on AI Governance, Future of Humanity Institute, Oxford University, 2018.
[Dafoe 2019] Alan Dafoe, AI, Strategy, Policy and Governance, Beneficial AI, 2019.
[Dartmouth 2020] Dartmouth Workshop, Wikipedia, 2020.
[Deep 2018] Deep Mind, AlphaZero, 2018.12.
[Deep 2018b] Deep Mind, AlphaFold: Using AI for scientific discovery, 2018.
[EU 2019b] EU, Ethics guideline for trustworthy AI, European AI Alliance, 2019.
[EU 2020] EU, White Paper on AI – European approach to excellence and trust, 2020.
[Felton 2018] Edward Felton, AI and Explainability, 2018.
[Fridman 2020] Lex Fridman, Lex Fridman Podcast. (100 by 2020.6.5)
[Fortune 2018] Fortune, Special Issue on AI, November 2018.
[FHI 2019] Future of Humanity Institute, Oxford University, 2019.
[FLI 2017] FLI, Beneficial AI with Asilomar AI Principles, 2017.
[GPAI 2021] Global Partnership on AI, 2021.
[Harari 2018] Yuval Harari, 21 lessons for the 21st century, 2018.
[Helsinki 2018] University of Helsinki, Elements of AI, 2018.
[NHK 2018] NHK Special, Money World, #2 Work Will Be Gone!, 2018.10.7.
[IEC 2008] IEC, Information Science and Technology, 800000-13, 2008.
[Jordan 2018] Michael Jordan, AI: revolution has not happened yet, Medium, 2018.4.
[Lee 2018] Kai-Fu Lee, AI Superpowers, 2018.
[Lee 2019] Kai-Fu Lee, Who is winning the AI race, in Stanford University Engineering School, 2019.
[McCulloch 1943] W. McCulloch and W. Pitts, A logical calculus of the ideas immanent in nervous activity, 1943.

[McKinsey 2018] McKinsey, Promise and Challenge of the Age of AI, 2018.
[MIT 2017] MIT, Minds and Machines, 24.09 (by Alex Byrne), 2017.
[MIT 2018] MIT, Artificial General Intelligence, 6.S099 (by Lex Fridman), 2018.
[Ng 2017] Andrew Ng, The state of AI, 2017.
[NSCAI 2021] National Security Commission on AI, NSCAI.gov, 2021.
[Pal 2019] A. Pal, What are the best machine learning conferences across the world, 2019.
[Pinker 2020] S. Pinker and S. Russell, On foundations, benefits, and possible existential threat of AI, 2020.
[PwC 2019] PwC, 2019 AI Predictions, 2019.
[Russell 2009] Stuart Russell and Peter Norvig, AI: A modern approach, 2009.
[Russell 2018] Stuart Russell, Long-term future of AI, 2018.
[Russell 2019] Stuart Russell, Human Compatible, 2019.
[Shannon 1948] Claude Shannon, A mathematical theory of communication, 1948.
[Stanford 2015] Stanford University, Stanford AI 100 Report, 2015.
[Strogatz 2018] Steven Strogatz, One giant step for a check-playing machine, NYT, 2018.12.
[Tegmark 2017] Max Tegmark, Life 3.0, 2017.
[Tegmark 2018] Max Tegmark, "How Far Will AI Go?", 2018.
[Turing 1950] Alan Turing, Computing machinery and intelligence, Mind,1950.
[UN 2017] UN, Final Report of 2017 GGE Meeting on Lethal Autonomous Weapons Systems (LAWS), 2017.
[Wiener 1948] Norbert Wiener, Control and communications in the mind and the machine, 1948.
[Wired 2018] Wired, "How to Teach AI Some Common Sense?", 2018.11.

Section 2.3 Blockchain

Kenji Saito

- **Introduction**

January 2021 marked 12 years since Bitcoin, the first instance of blockchain, went live. During that time, various so-called blockchain technologies have been derived, but confusion persists regarding the original purpose of blockchain. Many of the technologies flooding the market that claim to be blockchain appear to be merely databases that have become somewhat difficult to tamper with. But blockchain is not just about tamper resistance.

As widely known, the origin of the blockchain is the invention of Bitcoin, which is thought to have been created to enable users to transfer their funds without interference from governments or banking institutions. The Bitcoin blockchain, which was invented with the aim of fulfilling this goal, was supposedly designed to make it provable to all participants that a digitally signed

record of a transaction is unshakably positioned in the particular past of occurrence, and therefore the record of the monetary transfer cannot be reversed or altered in any way. Perhaps we need to go back to this point of origin in order to make a fair judgment of what has happened over the past 12 years, because of the confusion about the original purpose of the technology.

This section describes the history, technology, applications of blockchain and how this technology is changing the shape of money, one of the media we are most familiar with in our society.

- **History of Blockchain**

Many of the key events involving blockchain occurred in the 2010s. However, the germination of this technology goes back much earlier than that. In this subsection, we go as far back as the 1980s to review related concepts and inventions, in mostly chronological order, up to the 2010s.

Blind signature [Chaum 1983] is a technique for digitally signing hidden data as if it were signed blindfolded. It was developed to enable anonymous electronic payments and was implemented in the payment system by DigiCash (1989), a company founded by the inventor of this signing scheme. Blind signature is not used in Bitcoin (although it has been used, for example, in a Bitcoin-compatible anonymous payment system [Heilman 2017]) or any of the major blockchain-based digital currencies, but it is a spiritual ancestor of Bitcoin, as it pursues the privacy aspect of the freedom to use money.

State Machine Replication [Lamport 1984; Schneider 1990] is a technique for achieving fault tolerance of a service, in which a server is considered to be a state machine (a machine consisting of a set of states and transitions between the states). By always replicating the state machine (maintaining a set of the same servers), if some of the servers experience a failure, as long as other servers are still intact, the service will not be stopped (Figure 1). To agree on the sequence of events for replicating state transitions, this technique requires a consensus algorithm. In the consensus algorithm, depending on the assumed failure model - *benign* for transmission failures or *Byzantine* for arbitrary failures - correct nodes among n servers agree on the order of the events without being affected by f faulty nodes among n. It is known that benign fault-tolerance (FT) requires $n > 2f$, and Byzantine fault-tolerance (BFT) requires $n > 3f$ unless messages with unforgeable signatures are used.

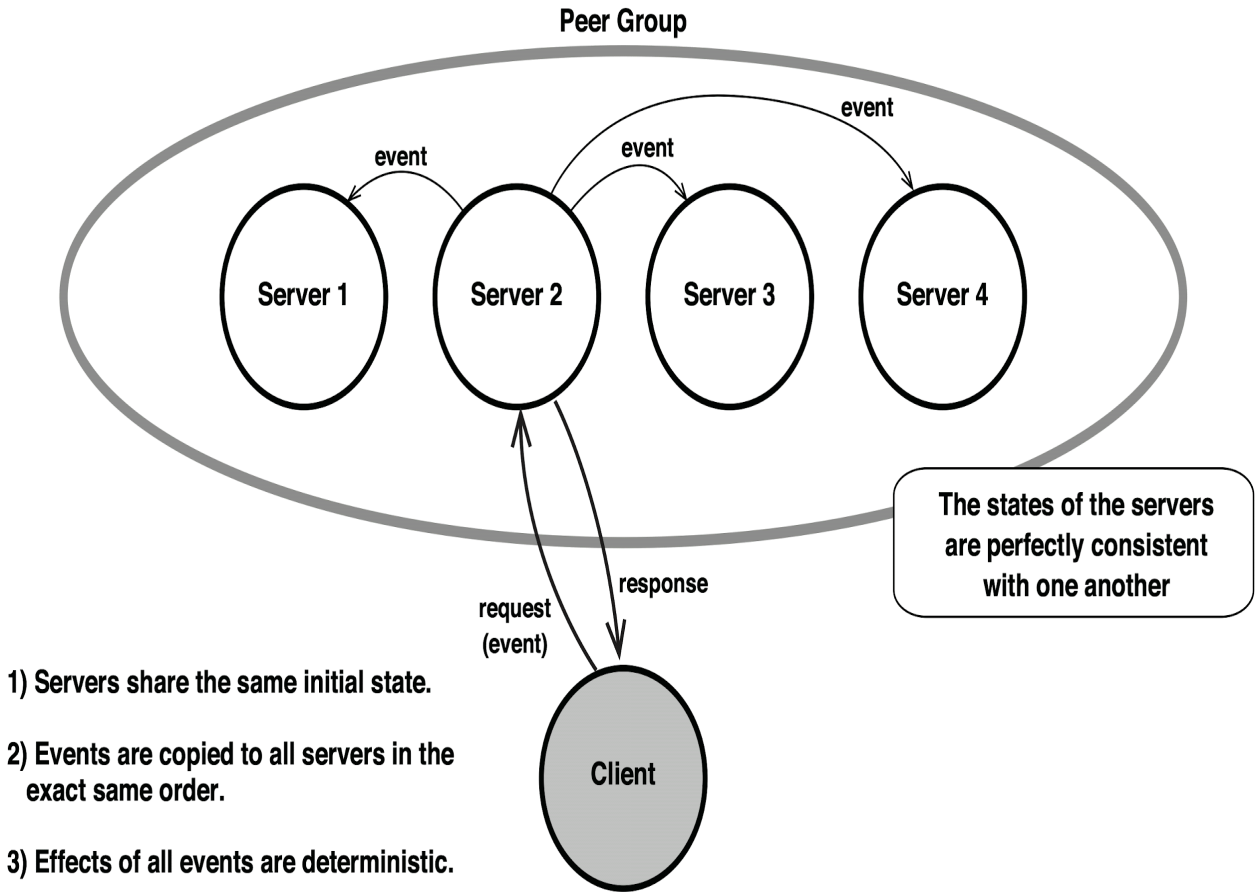


Figure 1: State Machine Replication

Blockchain technology places this technique in a different context. Although fault tolerance remains important, the replication of state machines is rather used to provide participants with a singleton of the sequence of events. When you have a replica of a state machine and know that other participants have the exact same replicas, you can believe that we share the single correct view of history. This allows us to do business, such as transferring financial assets, without any discrepancies.

The problems are that the original state machine replication requires that the number of participants n be predefined, and it should be possible to estimate the maximum number of faulty participants f. This means that the technique can only be used in a managed environment. Since blockchain aims to achieve the singleton of the sequence of events in a non-managed, decentralized environment (as not to let anyone be influential enough to stop or alter transactions), a different technique is used at least for the first generation of blockchain (see Section 2.3.3), which can be described as a *probabilistic state machine* [Saito 2016].

Hashcash (1997) (more formally defined in [Back 2002]) is a spam-prevention mechanism that requests email software to perform a *proof of work* before sending a message. A proof of work in general is an economical mechanism to deter unauthorized use of services such as DoS (Denial of Service), which requires the performance of some computing task before using the service. In Hashcash, a sender of a message needs to prepare a mail header with a random number that is adjusted so that the first 20 bits of the mail header's SHA-1 digest are 0 (that is to say "find data whose cryptographic digest is below a certain number"). It took about one second (as of 1997) to prepare to send a single email with this scheme, but it would be very costly (labor intensive) to send a large number of emails. This idea of proof of work was later applied in the design of Bitcoin.

Hysteresis Signature and **Inter-crossing Histories** [Iwamura 2000] are proposed solutions for the problem of proving the correctness of a digital signature positioned in a certain past point of time, regardless of the expiration of the public key certificate, leakage of the private key, or compromise of the signature algorithm that may have happened after signing. The problem is broken down into two sub-problems: *elapsed-time proof* to prove that a digital signature signed in the past remains correct today, and *alibi proof* to prove that a digital signature claimed to have been signed in the past did not really exist at the time.

Hysteresis signature is a technique to keep signing the accumulated records including past digital signatures with a latest signature algorithm, forming a chain of signatures. This technique has been used in timestamp services. A problem with this is that a whole history of events can still be fabricated by the signing entity. *Inter-crossing histories* is a technique to apply hysteresis signature to communication among multiple autonomous entities, so that the accumulated history to be signed includes (cryptographic digests of) events in other domains of which the signer does not have control. This would enable the verification of history in a paleography-like style (by tracing references), which would in turn make a consistent fabrication of a past history very difficult.

These techniques have been applied to blockchain technology and its applications. Bitcoin, for example, has chains of signatures and a chain of cryptographic digests in the history of transactions (as described in Section 2.3.3) that can be seen as applications of hysteresis signature. The problem of possible counterfeits of hysteresis signature has been covered by proof of work. The well-known technique of *anchoring*, or putting a cryptographic digest of records in a private ledger to a public blockchain in order to enable later verification by the participants or the users of the private ledger, can be seen as an application of inter-crossing histories.

BitTorrent [Cohen 2003] and **Samsara** [Cox 2003] are efforts to barter computational resources in *P2P* (Peer-to-Peer) environments. P2P is a method of configuring a network application by building and providing services through communication among equal partners

(peers) without requiring a fixed set of servers. This provides a high degree of flexibility and has the advantage of allowing services to be started without infrastructure, such as a group of servers, and allowing for plasticity, where the system continues to function even if part of it is lost. After around the year 2000, P2P was often used for file sharing services and so forth.

However, a P2P system will fail if modified software is distributed based on selfish but reasonable demands, such as only wanting to enjoy the benefits of the system without sharing their resources to be used by other peers. The system must also be designed for the existence of *churns*, or migratory peers, who participate in the system only when it is convenient for them to do so and who repeatedly join and leave the system. Through the identification of these issues, the recognition of the importance of economic mechanisms in the design of P2P systems was quickly shared by the researchers of such systems.

In BitTorrent and Samsara, network bandwidth and storage space are respectively bartered with other participants. These programs use a *tit-for-tat* or payback strategy: if a participant does not provide sufficient bandwidth for uploads, the programs reduce the download bandwidth for the peer, or discard data stored for participants who do not provide the same amount of space for other peers to use.

PPay [Yang 2003] and **i-WAT** [Saito 2003; Saito 2010] tackled the problems of P2P systems in a more generalized way by providing a system of exchanging IOUs that can be used as P2P currency. Figure 2 outlines such a digital currency system. What this system does is transfer credits (obligations or IOUs issued by debtors), so that goods and services can go in the opposite direction to promote fair sharing of resources among peers.

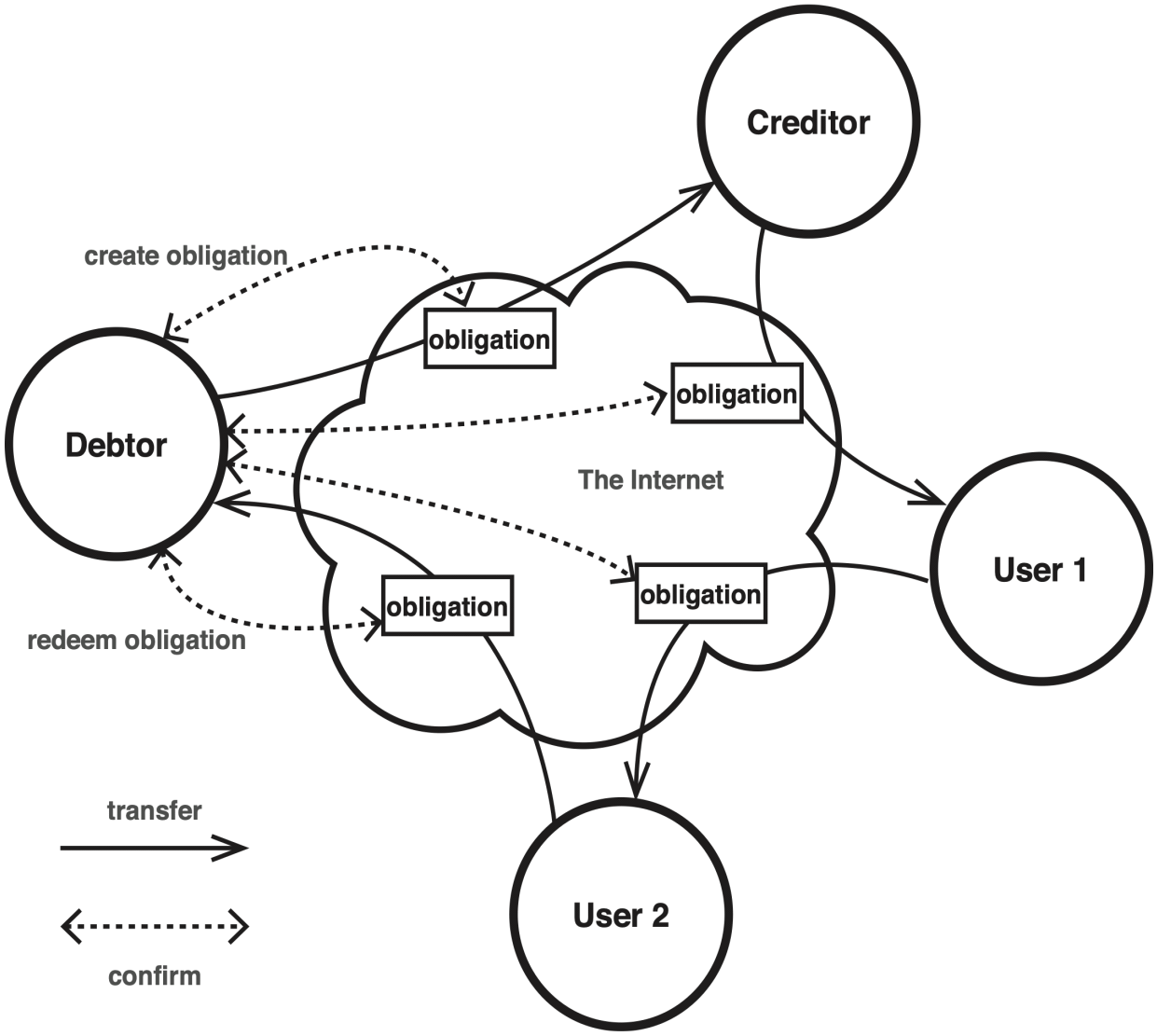


Figure 2: Overview of IOU as Digital Currency

In order to do this digitally, it is necessary to avoid the problem of *double spending*. For example, if user 1 in Figure 2 duplicates the obligation of the debtor and passes the same credit to user 3 (who is not in the figure) as well as user 2, user 1 would receive double the amount of goods or services in return, which would be unfair. In order to detect and invalidate such double spending, someone has to confirm the transfer of the credit and to maintain the correct state of the credit. This is always a problem with electronic money, but it would be simpler if the central mint (or bank, or at the implementation level, a set of servers) controlled the transfer of money. However, this cannot be the case for a P2P system.

PPay and i-WAT solve this problem in the following way: if the credit is duplicated in circulation, the final obligation that the debtor has to satisfy is doubled. Thus, the motivation for

voiding the double spending lies with the debtor, and therefore, the transfers of the credits need to be confirmed by their debtors (or their delegates).

Ripple [Fugger 2004] is a mechanism for two parties without a direct means of payment to discover and use a payment path, called a *Ripple path*, that passes through the common trusted parties. This concept existed back in 2004, but the service has only recently gained popularity since the benefits of digital currencies in international monetary transfers (notably, price destruction of the fees) became clearer with the spread of Bitcoin.

Bitcoin [Nakamoto 2008] is the first blockchain currency system, designed and implemented at the beginning by an anonymous developer who names him/herself *Satoshi Nakamoto*. Details of the blockchain technology will be discussed in Subsection 3 Blockchain Technology, but the currency system itself can be outlined as Figure 3. To prevent double spending, a monetary transfer is validated (confirmed) by the network of validators (often called *miners*).

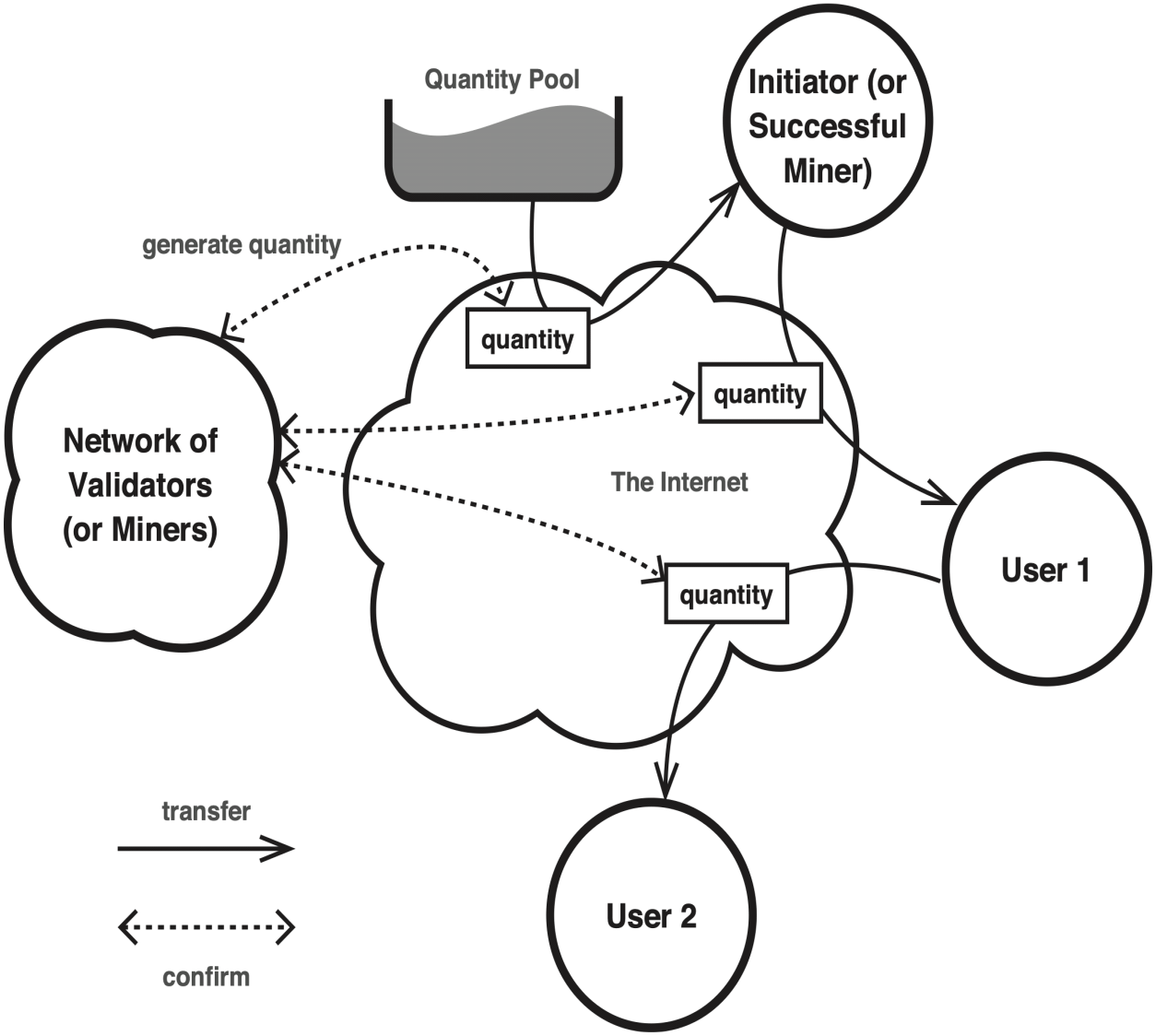


Figure 3: Overview of Blockchain-based Digital Currency

Unlike IOU-based digital currency, a Bitcoin's digital coin (*bitcoin* starting with lowercase letters, or *BTC*) is not a representation of a debt, but that of an abstract value or quantity generated as a reward for validating payment transactions (it is as if *mining* the quantity from the quantity pool, where the validators are called *miners*; readers are referred to the footnote[1] for the problem of this term). A set of transactions, called a *block*, is validated through a competition among validators at a time, which does not need to contain any other transactions than that of paying the reward to the validator themselves. Another difference from IOU-based currency is that destruction of money is not defined as part of the lifecycle of the digital coin, although the coin can be *burnt*, or sent to a non-existing address.

Countless variants, or alternative coins called *altcoins*, have arisen, but many follow the same design as Bitcoin and differ only in parameters. These coins are often called *cryptocurrencies*.

Open Assets Protocol [Charlon 2013] has been specified on top of the Bitcoin data structure and its semantics in order to define, generate and transfer quantities other than bitcoin over the Bitcoin blockchain. Those quantities are called *colored coins*, which denote a general concept of non-native tokens on the (Bitcoin) blockchain. It is said that a colored coin can represent an asset like a bond. However, a bond is a representation of a debt and can be redeemed so that it should be outlined as Figure 2; a colored coin works as shown in Figure 3, being semantically close to bitcoin.

Ethereum [Buterin 2013] is a foundation for general applications by extending the concept of the blockchain. Applications on the Ethereum blockchain are called *smart contracts*, which are not necessarily augmented versions of contracts as we see in our social lives, but automated digital objects with state transitions. In Ethereum, each validator (miner) runs *EVM (Ethereum Virtual Machine)* on which contracts (application programs) are executed. *Ether* (or *ETH*), the native currency of Ethereum, is generated upon validation of a block just as with Bitcoin. Ether is sometimes called *cryptofuel* because it is converted to a unit called *gas* required to execute a virtual CPU cycle on EVM. Metaphorically, EVM must be like an engine in the view of the designers of Ethereum.

Figure 4 outlines how smart contracts run on the Ethereum blockchain. Since the chain of blocks defines an order of events, a blockchain can be seen as a run of a single state machine, or a series of state transitions, which is replicated to all participants. Vitalik Buterin, the inventor of Ethereum, must have thought that this would define a world computer since a computer can be abstracted as a state machine, and a blockchain provides a singleton state machine in the world whose workings can be verified by all.

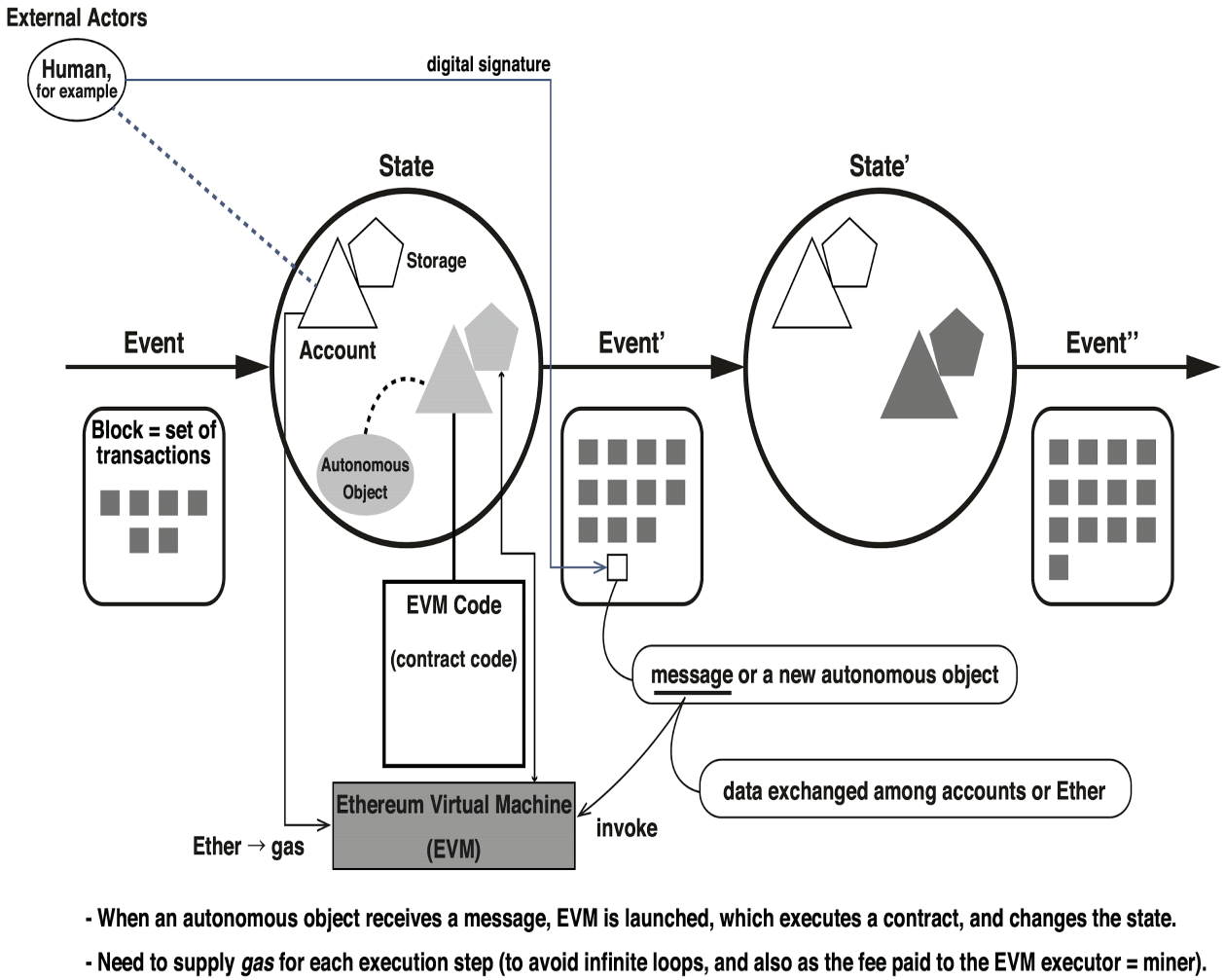


Figure 4: Overview of Ethereum, Its Virtual Machine and State Machine

The so-called *world state* consists of two kinds of accounts: an *EOA (Externally Owned Account)* owned by an external actor like a human being, or a contract (also called an *autonomous object* although it requires a message reception and EVM to run). Each has the balance in Ether. A transaction is signed by an external actor, which is either a message to an account or deployment (writing to the world state) of a new contract. When a contract receives a message, the corresponding contract code is run on EVM. The gas is consumed from the account of the sender of the message.

There are private ledgers that are capable of executing EVM-based smart contracts, such as *Quorum* (2016) [ConsenSys 2019], private version of Ethereum, and *Hyperledger Burrow* (2017) [Linux 2018].

Hyperledger [Linux 2018] is a project started in 2015 by the Linux Foundation with a four-fold mission: 1) prepare a business-ready open source distributed ledger framework and code base; 2) create a technical community for open source development; 3) involve the leaders of the ecosystem including developers, service/solution providers, and customers; and 4) provide a platform for governance.

There has been a great deal of open source software development within Hyperledger. *Hyperledger Fabric* (2016) is probably the most common general-purpose private ledger, whose initial code was a merge between code provided from IBM and Digital Asset Holdings (DAH software was called Hyperledger before this project by the Linux Foundation started). *Hyperledger Sawtooth* (2016) is a blockchain-based ledger whose initial code was provided from Intel. *Hyperledger Iroha* (2016) is another general-purpose private ledger whose initial code was provided from Soramitsu, a startup based in Japan. *Hyperledger Indy* (2017) focuses on decentralized identifier management. *Hyperledger Besu* (2019) is an Ethereum client compatible with public and private networks of Ethereum.

Corda [Hearn 2019] is a ledger by R3 (a consortium of financial institutions) specifically designed for managing agreements between financial institutions, and was first introduced in 2016. Corda has a clear mission of achieving "what I see is what you see, and we both know that, and the audit can confirm that", which is apparently different from Bitcoin's "not to let anyone stop you from transferring your own funds as you see fit", and has been designed accordingly.

Polkadot [Wood 2016] is a framework to host heterogeneous multiple ledgers, which can connect to existing blockchains such as Bitcoin or Ethereum, and can host new ledgers called *parachains*. The multiple ledgers can interwork through the central chain of blocks called *relay-chain*, whose state machine is managed via a BFT algorithm. This can be seen as an application of the inter-crossing histories concept.

BBc-1 (Beyond Blockchain One) [Saito 2017] is a lightweight toolkit for private ledgers that can solve elapsed-time and alibi proof problems of digital signatures through inter-crossing histories. BBc-1 has been developed by a non-profit called Beyond Blockchain, based in Japan.

Libra [Libra 2019] is a payment system based on the Libra Blockchain, a state-machine replicating ledger managed by Libra Association, founded by Facebook. It is said that any interested parties can have a replica of the state machine so that they can verify the recorded transactions. However, whether such a party has a correct replica or not seems not to be verified. This problem is rather apparent for the Libra Blockchain because the documentation is clearly

written. The problem must actually be common among many managed, state-machine replicating private ledgers.

Ethereum 2.0 [Ethereum 2020] is a new version of Ethereum under development to solve the following issues of a probabilistic state machine: lack of finality and lack of scalability. In order to tackle these problems, Ethereum 2.0 will introduce a voting mechanism among self-nominated parties (this voting scheme is often called *proof of stake*) and shards (horizontal partition). In addition, the shards will be able to host ledgers other than those based on EVM (Ethereum Virtual Machine), which would make Ethereum 2.0 semantically close to Polkadot.

- **Blockchain Technology**

As described before, blockchain was first invented in order to realize Bitcoin, which is thought to have been created not to let anyone stop you from transferring your own funds as you see fit. The Bitcoin blockchain had to implement a state machine that satisfies the following three properties (BP: Blockchain Properties) in order to achieve this goal of Bitcoin:

BP-1: Only the authorized user can cause a state transition that is allowed in the state machine.

BP-2: Such a state transition always occurs if the authorized user wants it to happen.

BP-3: Once a state transition occurs, it is virtually irreversible.

These properties have been pursued not only by Bitcoin blockchain, but also by many other ledger systems to work in a non-managed environment (often regarded as *permissionless*, where anyone can be a user). In a managed environment (often regarded as *permissioned*, where one needs to be allowed to join), BP-2 might take another form.

The consequences of these requirements to authentication in a non-managed environment is that we want to use digital signatures, but without public key certificates, because we need to prove the identity of a user without relying on a specific third party (not to let that third party to stop the user, to satisfy BP-1), and without worrying about the expiration of the public key certificates (to satisfy BP-2). Still, we need to be certain about the validity of public keys for verifying digital signatures. The solution in Bitcoin, Ethereum, and many other systems is that a cryptographic digest of a public key is used as the identifier of an account whose balance and other information are operable only by the holder of the corresponding private key. This design is groundbreaking in such a way that it allows a public key to be attached to the transaction data along with a digital signature, and the validity of the public key is verified if the digest calculated from the public key is equal to the address of the authorized user's account, which allows a

completely unrelated third party to verify the legitimacy of the public key and verify the authenticity of the transaction.

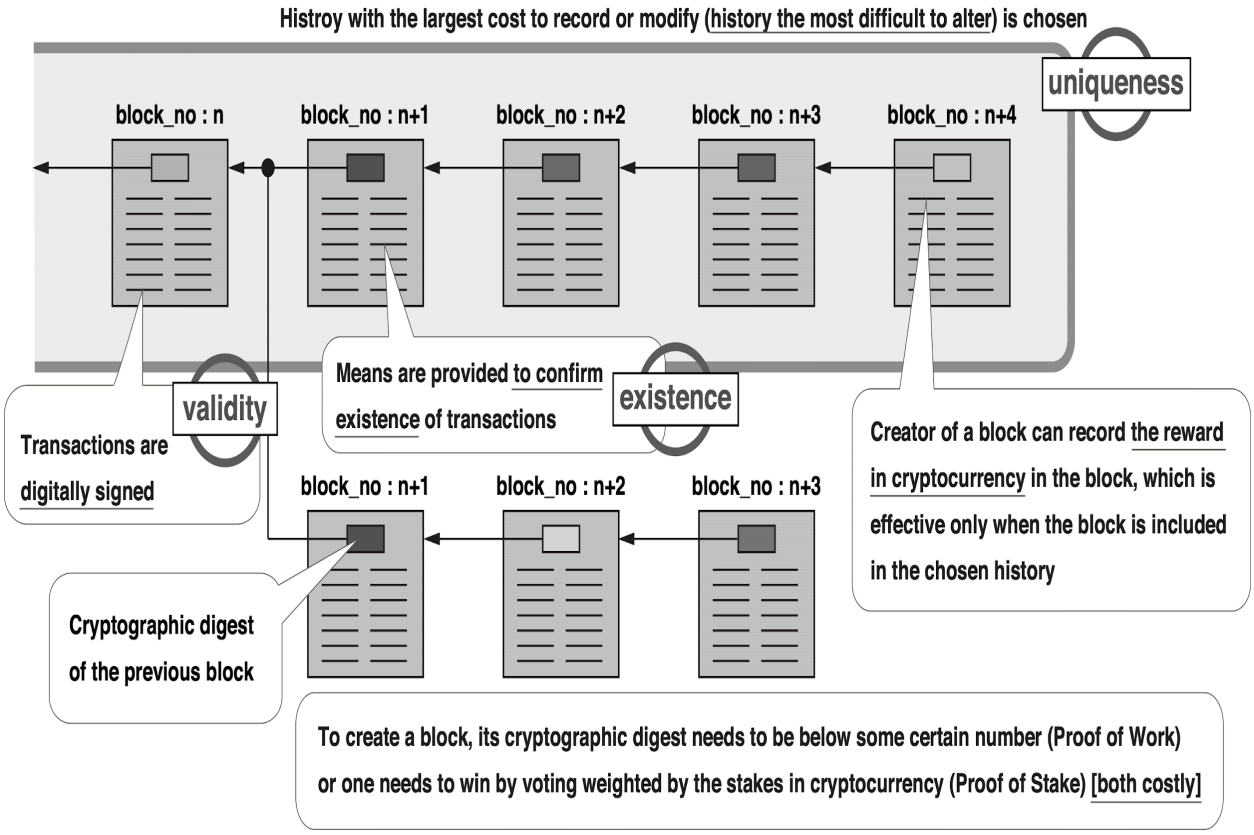


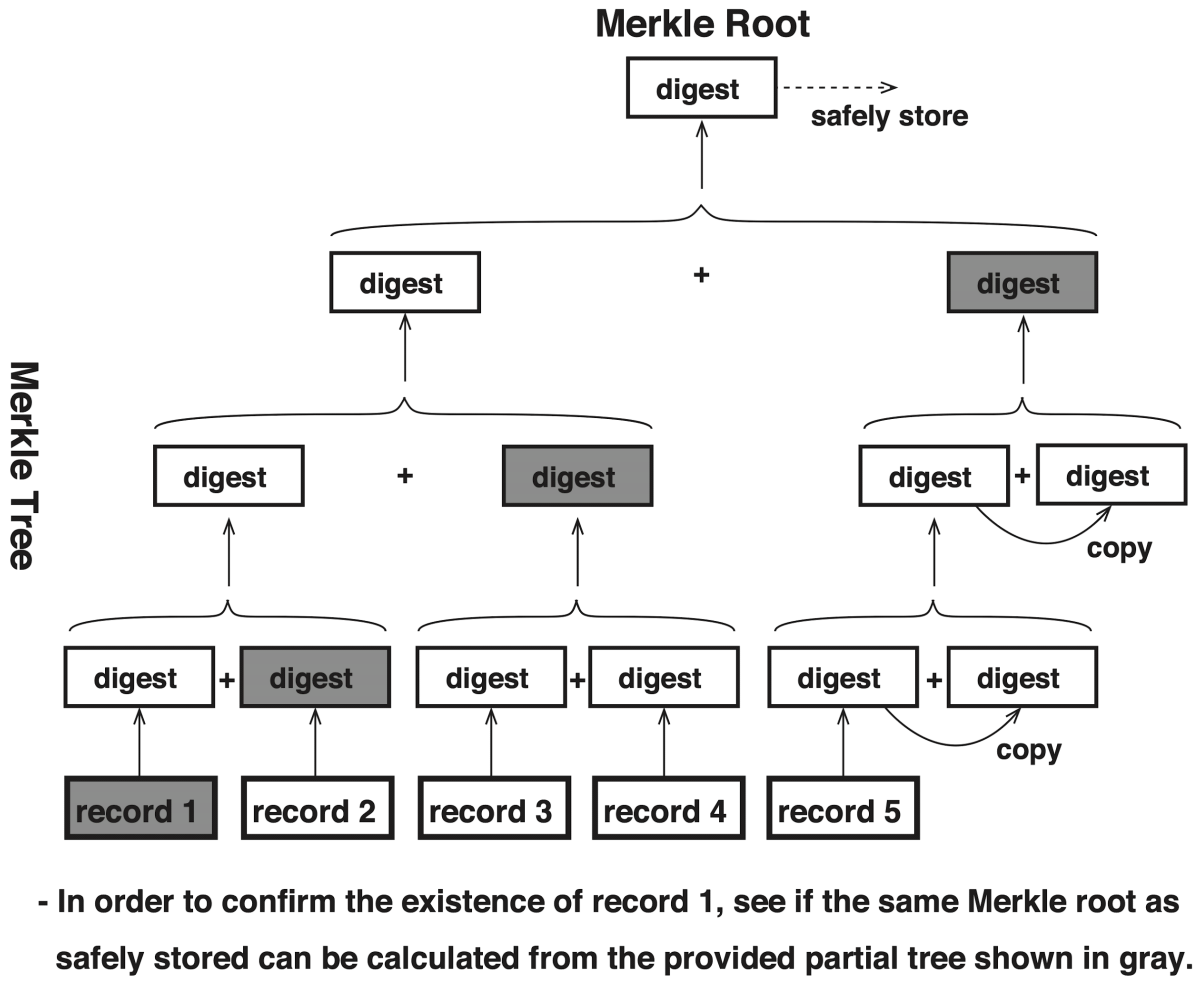
Figure 5: Generalized Blockchain (the 1st Generation)

In addition, since digital signatures need to be correctly verified regardless of compromise of the signature algorithm or private keys (to satisfy BP-2), the elapsed-time proof problem of digital signatures needs to be solved, which means that somehow transactions must be firmly placed in the past (BP-3 needs to be satisfied). Also, high availability needs to be provided (to satisfy BP-2) without any centric forces (that might decide to stop the system) and with redundancy, and therefore, it should work as a P2P system. In Bitcoin, Ethereum, and the like (let us call these the 1st generation blockchains), these are achieved as illustrated in Figure 5.

Each *block* storing a set of transactions has a digest of the previous block in its header. This structure is sometimes called a *hash chain*, because a digest is casually called a hash value. When building a block numbered *n*, the previous block numbered *n-1* must have already existed since it is not possible to compute the digest of a block unless it exists. Therefore, this structure logically represents the relative timings of the creation of blocks. Moreover, the data of the block must be configured so that the digest of the block is less than or equal to the target value

typically inherited from the previous block (in Bitcoin, the target value is adjusted every 2016 blocks in order to maintain the interval between blocks of 10 minutes on average). This forms a proof of work because it requires repetitive calculations (or, for blocks to be valid, it needs to collect the most votes where the right to vote is obtained through stakes in the native tokens, as Ethereum 2.0 is being designed). Creating (or remaking) a block is costly, and the older the block being altered, the greater the number of the subsequent blocks that must be altered one after the other, which results in a cumulative increase in the cost of alteration.

Transactions are stored in a block, but only a single value representing the set of transactions is stored in the block header, and the digest of a block is calculated using its header only. The structure used for obtaining a single representative value of transactions is a *Merkle tree* [Merkle 1987], as illustrated in Figure 6, which provides an inexpensive way for verifying the existence of a transaction in a block.



- In order to confirm the existence of record 1, see if the same Merkle root as safely stored can be calculated from the provided partial tree shown in gray.

Figure 6: Merkle Tree and Merkle Proof (partial tree)

In Bitcoin, a single *Merkle root* of the Merkle tree calculated from a set of transactions is stored in one block header. In Ethereum, three such roots are stored in one block header: the root of a *Merkle-PATRICIA trie* to represent the whole state of the blockchain as a set of key-value pairs, the root of a Merkle tree of transactions, and the root of another Merkle tree of transaction *receipts*, where a receipt contains the results of a transaction such as the consumed amount of gas and the list of logs. These structures provide verifiable records of events and states with respect to the blockchain.

However, these structures and algorithms alone cannot provide a single history of records, because blocks are created in an autonomous and decentralized way in order not to stop the process of recording transactions. As a result, two or more blocks that meet the criteria may be proposed by multiple participants at the same time, and since there must not be a single party responsible to decide which block is to be included in the correct history (because that party may decide to stop the process), each participant will have to choose a block to connect succeeding blocks at its own discretion, resulting in a *fork* of the hash chain. Since the order of blocks must be unique to solve the problem of double-spending, Bitcoin has a consensus mechanism, the *Nakamoto consensus*, where everyone adopts the chain for which the accumulated cost of proof of work is the highest (roughly, the chain with the longest extension). Nakamoto consensus is consistent with the design intent in the sense that it adopts the history that is the most costly to overturn.

These functionalities are classified into functional layers as described in Table 1, where a lower layer functionality is a prerequisite for the higher layer functionality.

Table 1: Functional Layers of Blockchain

Layer	Functional Stack	Description
high ^ ^ ^	Description of Rules e.g. transfer of bitcoins	Application logic to decide what transactions are valid (generalized as smart contracts).
	Consent of Uniqueness e.g. Nakamoto consensus	When two mutually contradicting transactions are cast, (eventually) everyone chooses the same one to place in the correct history.
	Proof of Existence	No one can delete the evidence of an existing transaction in the past, nor fabricate the evidence of a transaction that did not exist.

^ low	e.g. hash chain with proof of work	
	Guarantee of Validity e.g. transaction with a digital signature	The content of a transaction is not contrary to the past history regarding the asset in question, the transaction is cast by a legitimate user, and the transaction cannot be altered.

- **Blockchain Applications**

As described before, blockchain is designed to make it provable to all participants that a digitally signed record of a transaction is unshakably positioned in a particular past, and therefore, the fact of the monetary transfer cannot be reversed or altered in any way, even when the digital signature algorithm or private keys are compromised. After Ethereum, it became easier to conceive an application of blockchain as a general state machine, not only for fund transfers. Then what would be some of the actual applications other than transferring funds?

Let us consider this in the context of digitizing a person's last will and testament as an example. Under the current Japanese law, for instance, a person's last will cannot be treated as official unless it is written and signed in person and approved by a notary. However, if it can be proven that the digital signature to an electronic version of a person's will is genuinely his or her own and that the will has not been altered after the person's death, then it would be possible to legalize a digital version of that person's will.

However, there is generally no guarantee that the private key of someone will be kept secret after their death. Also, even if the will is entrusted to a notary, or someone who preserves the will and vouches for its legitimacy, who can testify that it was signed before the person's death, the heirs and the notary may conspire (e.g., an heir may successfully obtain the dead person's private key, tamper with the will to receive a huge inheritance, and encourage the notary to perjure him or herself in exchange for their share). Therefore, the digital version of a will cannot be actualized simply by having the person digitally sign the document.

But then again, if the digitally signed will or its cryptographic digest is written to a blockchain before the person's death, then the will can be viewed as valid (in a logical sense) insofar as the blockchain continues to fulfill the properties mentioned above (mainly BP-3, but considering the cases of updating the will, BP-1 and BP-2 must also be satisfied).

This logic is applicable to other similar applications, for example, graduation certificates of private academic institutions (that may go bankrupt), or passports of people from a country (that

may cease to exist). In fact, an application of blockchain technology for providing refugees with digital legal identification has been pursued by a joint effort of Accenture, Avanade, and Microsoft, helping the United Nations [Johnson 2018].

In short, blockchain can potentially improve digital certification beyond the limit of digital signatures that suffer from elapsed-time and alibi proof problems. Such potential can be classified into two major categories of applications: 1) tokens and 2) provenance.

Tokens here are digital certificates representing some rights or assets that are purchasable or something with which we can purchase things (object or medium of exchange). Table 2 shows a classification of tokens and examples for each class. Among the examples, *CBDC (Central Bank Digital Currency)* is discussed in detail in Section 2.3.5. *CryptoKitties* [CryptoKitties 2017] are virtual cats users can breed. As Figure 3 shows, non-redeemable tokens may be straightforward extensions of a blockchain-native currency. Redeemable tokens, as illustrated in Figure 2, need to be implemented on top of such a foundation if it is on the 1st generation blockchain.

Table 2: Classification of Tokens and Examples

	Fungible	**Non-fungible**
Redeemable	*CBDC (Central Bank Digital Currency)*, electronic money	tickets, securities
Non-redeemable	bitcoin, Ether, etc. (cryptocurrencies)	*CryptoKitties*

Applications of tokens and their automation range from financial asset management to automation of corporate behaviors such as stock splits, capital reductions and mergers.

Provenance has a wide range of applications for long-term proofs that recorded information is genuine, including certificates (e.g. last wills, grades at schools, identifications, licenses, etc.), logs (e.g. detection of parts or products at a certain point in a supply chain) and even sensory data. In an IoT environment, a sensor with an embedded private key can output digital signatures along with its sensory data to allow for verification of the authenticity of the data. However, once the security of the sensor is compromised, the signatures would become useless. Then again, putting the digests of (a group of) the sensory data into blockchain would virtually guarantee the authenticity of data prior to the incident (the same goes with supply chain management, as it also

uses sensory data in the production and distribution lines). This situation is analogous to the case of the last will and testament, which makes a prototypical case of provenance with blockchain.

A recent notable provenance application was tracking of surgical mask distribution in Taiwan during the COVID-19 pandemic [FiO 2020]. It looks as if the state machine replication approach, where replicas are shared among stakeholders for verification, was used in the application. Such an approach has two problems (SMRP: State Machine Replication Problems):

SMRP-1: Do all stakeholders have replicas (or part of it) for verification?

SMRP-2: Is there a way to verify that the replica one party has is genuine?

In the example of surgical mask distribution, the consumers themselves or parties representing the consumers need to have a replica proven to be genuine in order to monitor the distribution by the government. Otherwise, an existing technique for data management would suffice.

- **Blockchain for Digital Currencies**

Fungible tokens are typical and original cases of blockchain applications. Cryptocurrencies were known to the public through a number of thefts that occurred on exchanges; notable ones in Asia in the 2010s include Mt. GOX (2014), Bitfinex (2016), and Coincheck (2018) incidents, all of which went the similar ways. Such a consequence is deduced in a straightforward way from the properties of blockchain. Because we employ digital signatures to prove our identity on our own (BP-1), the question of whether or not we are the person in question is replaced by whether or not we can use the private key. Once the private key is compromised, no one can stop the stealing and subsequent transfers of funds (BP-2), and since we cannot reverse the transfer (BP-3), we cannot get the money back. However, these properties are important for guaranteeing economic freedom, and the 2016 *hard fork* (non-compatible update) of Ethereum blockchain [Buterin 2016], in which the Ethereum community themselves compromised BP-3 to cancel a stealing transaction, raises an important question of governance vs. freedom.

Another topical contribution by Ethereum is the ERC-20 [Vogelsteller 2015] series of smart contract standards for fungible tokens (ERC stands for Ethereum Request for Comments). This has allowed developers to easily define new currencies by implementing the ERC-20 standard or deriving new classes of contracts from it. However, many ICOs (Initial Coin Offerings – to sell digital coins to be used in new services to fundraise for the development of the services) that allowed for unwarranted funding were executed, which caused a great deal of damage such as unreturned funds, lost trust in the digital currency industry, etc. The reaction to this has led to a

focus on security tokens (redeemable tokens) and stable coins (tokens whose prices are somehow stabilized).

Another movement is to replace national fiat currencies themselves with digital currencies (CBDC: Central Bank Digital Currency). Notable examples include ongoing projects of E-krona [Riksbank 2019] in Sweden and DCEP (Digital Currency Electronic Payment) [Kwan 2020] in China. Bakong [NBC 2020] in Cambodia is the system of payment supported by the national bank, which is almost ready for full deployment. CBDCs are not necessarily blockchain-based, but properties BP-1 and BP-3 would be useful for realizing accountable monetary systems.

However, the potential for digital currencies should also lie in the non-governmental side. A non-profit called *Plastic Bank* continues to experiment with issuing digital tokens in exchange for the collection of ocean plastic waste [IBM 2019], which is ongoing in Haiti, Brazil, Indonesia, the Philippines, and, most recently, Egypt.

The modern monetary system is about 400 years old and has developed along with modern society. Digital technology is changing the shape and meaning of money with blockchain. It may bring about a world in which the weak, not the strong, can issue money.

References

[Back 2002] Adam Back, Hashcash - A Denial of Service Counter-Measure, 2002.
[Buterin 2013] Vitalik Buterin, Ethereum White Paper: A next generation smart contract & decentralized application platform, 2013.
[Buterin 2016] Vitalik Buterin, Hard Fork Completed, Ethereum Blog, 2016.
[Charlon 2013] Flavien Charlon, Open Assets Protocol (OAP/1.0), 2013.
[Chaum 1983] David Chaum. Blind signatures for untraceable payments. In Advances in Cryptology – Crypto ’82. Springer-Verlag, 1983.
[Cohen 2003] Bram Cohen. Incentives Build Robustness in BitTorrent, The First Workshop on Economics of Peer-to-Peer Systems, 2003.
[ConsenSys 2019] ConsenSys. Quorum, 2019.
[Cox 2003] Landon Cox and Brian Noble, Samsara: Honor among thieves in peer-to-peer storage, Proceedings of the ACM Symposium on Operating Systems Principles, 2003.
[CryptoKitties 2017] The CryptoKitties Team, CryptoKitties: Collectible and Breedable Cats Empowered by Blockchain Technology, 2017.
[Ethereum 2020] Ethereum, Ethereum 2.0 Specifications, 2020.
[FiO 2020] FiO, A Mask Inventory System on Blockchain is Being Deployed to Fight Coronavirus in Taiwan. Fintech News Hong Kong, 2020.
[Fugger 2004] Ryan Fugger, Money as IOUs in social trust networks & a proposal for a decentralized currency network protocol, 2004.

[Hearn 2019] Mike Hearn and Richard Gendal Brown, Corda: A distributed ledger, 2019.
[Heilman 2017] Ethan Heilman, Leen AlShenibr, Foteini Baldimtsi, Alessandra Scafuro and Sharon Goldberg, TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, NDSS '17, 2017.
[IBM 2019] IBM, Plastic Bank: Enabling plastic recycling and financial inclusion with Blockchain, 2019.
[Iwamura 2000] Mitsuru Iwamura, The Alibi and Elapsed-Time-Proof Problems in Digital Signatures: Hysteresis Signatures and the Concept of Digital Paleography, bit. 32 (11), pp.42-48, 2000. *(in Japanese)*
[Johnson 2018] Peggy Johnson, Partnering for a path to digital identity, Official Microsoft Blog, 2018.
[Kwan 2020] Chi Hung KWAN, China Aiming to Issue a Central Bank Digital Currency -Expected Macro-Level Effects, Research Institute of Economy, Ministry of Trade and Industry of Japan, 2020.
[Lamport 1984] Leslie Lamport. Using Time Instead of Timeout for Fault-Tolerant Distributed Systems, ACM Transactions on Programming Languages and Systems, pp.254-280, 1984.
[Libra 2019] Libra Association. Libra White Paper, 2019.
[Linux 2018] The Linux Foundation, An Introduction to Hyperledger, 2018.
[Merkle 1987] Ralph C. Merkle, A Digital Signature Based on a Conventional Encryption Function. Advances in Cryptology — CRYPTO '87, pp 369-378, 1987.
[Morrison 1968] Donald R. Morrison, PATRICIA—Practical Algorithm to Retrieve Information Coded in Alphanumeric, Journal of the ACM, 15 (4), 1968.
[Nakamoto 2008] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.
[NBC 2020] National Bank of Cambodia, PROJECT BAKONG: Next Generation Payment System, 2020.
[Riksbank 2019] SVERIGES RIKSBANK, E-krona, 2019.
[Saito 2003] Kenji Saito, Peer-to-Peer Money: Free Currency over the Internet, Proceedings of the Second International Conference on Human.Society@Internet (HSI 2003), Lecture Notes in Computer Science 2713, pp.404-414, 2003.
[Saito 2010] Kenji Saito and Eiichi Morino, The Brighter Side of Risks in Peer-to-peer Barter Relationships, Future Generation Computer Systems, 26 (8), pp.1300-1316, 2010.
[Saito 2016] Kenji Saito and Hiroyuki Yamada, What's So Different about Blockchain? — Blockchain is a Probabilistic State Machine, IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp.168-175, 2016.
[Saito 2017] Kenji Saito, and Takeshi Kubo, BBc-1: Beyond Blockchain One - An Architecture for Promise-Fixation Device in the Air, 2017.
[Schneider 1990] Fred B, Schneider. Implementing Fault-Tolerant Services Using the State Machine Approach: A Tutorial, ACM Computing Surveys, 22 (4), pp.299–319, 1990.
[Vogelsteller 2015] Fabian Vogelsteller, Vitalik Buterin, ERC-20 Token Standard, 2015.
[Wood 2016] Gavin Wood, Polkadot: Vision for a heterogeneous multi-chain framework, 2016.
[Yang 2003] Beverly Yang and Hector Garcia-Molina, PPay: micropayments for peer-to-peer systems, Proceedings of the 10th ACM conference on Computer and communications security (CCS '03), 2003.