# Chapter 3
# Crypto Assets (Cryptocurrencies) and Central Bank Digital Currencies


**Naoyuki Iwashita**

## 1 Rise and Fall of Crypto Assets

Bitcoins, which drew attention worldwide after their price soared in 2017, began to be seen as a high-risk investment after crashing in 2018. But a byproduct of the Bitcoin, blockchain technology, is drawing attention as a leading next-generation technology, and pilot studies for various applications of this technology are being conducted. Having said that, the only examples of the large-scale application and social acceptance of blockchain technology so far are bitcoins and other crypto assets (cryptocurrencies).

Blockchain technology was developed using already existing technologies such as digital signatures based on public key cryptography and hash chains, which are successive applications of hash functions. It has as many as 3.6 million users in Japan alone, even if their use of it is mainly for the purpose of dabbling in crypto assets, because, at its peak, the economic value of crypto assets being traded was tens of trillions of yen. In that sense, this phenomenon represented the social deployment of information security technology on an unprecedented scale.

However, the rise of the Bitcoin is not an unalloyed story of success. Early investors made economic gains from the bitcoins they had purchased for extremely low prices when the price of the currency shot up. However, this rise in the bitcoin's market value was owing to the fact that they were beyond the reach of financial regulators and could be traded anonymously in the international market, and with their rise, they have been used for purposes such as international money laundering and terrorism financing, causing disruption to the global financial order.

Meanwhile, those who invested in the currency in 2017 or later have suffered losses as the price of the currency plummeted following several cases of the hacking of bitcoin exchanges and the theft of bitcoins. From the perspective of information

N. Iwashita (✉)
School of Government, Kyoto University, Tokyo, Japan
e-mail: iwashita.naoyuki.7e@kyoto-u.ac.jp



S. Kaji et al. (eds.), *The Economics of Fintech*,
https://doi.org/10.1007/978-981-33-4913-1_3

security technology, these incidents were fresh reminders of how difficult it is to securely manage the safety of private keys, a security essential when it comes to digital signatures.

The key to the success of the Bitcoin was to use the Proof of Work (PoW) system, a consensus mechanism that increases the safety of a transaction even in the absence of a trusted third party. As the market value of bitcoins soared, it became possible to make enormous profits by mining bitcoins using the PoW function. This resulted in massive investments in Bitcoin mining facilities, enough to distort global resource allocation and intensify global environmental problems.

The creator and developer of the Bitcoin in its early days, Satoshi Nakamoto, designed it as a form of electronic cash that could be used for pseudonymous financial transactions among strangers over the Internet. However, the currency has deviated significantly from what Satoshi seems to have intended, and his original plan never came to fruition. How did this deviation take place, and is it possible to return to the original plan?

## 2 Birth and History of the Bitcoin

There is no evidence to show that a person named Satoshi Nakamoto actually exists. It is not even clear whether this is the name of a specific individual, but if it is, the identity of this person is shrouded in an aura of mystery. However, let us not worry about that for the moment. Going by the paper[1] published under this name, it is hard to imagine that its author had envisaged the Bitcoin to be what it has become today.

The title of this paper is "Bitcoin: A Peer-to-Peer Electronic Cash System." Regarding electronic money (e-money) that can use digital data to function on open networks such as the Internet exactly in the same way as cash does—as a medium of money transfer or payment—and that can also protect the privacy of the participants by ensuring the anonymity of the transaction, various ideas have been proposed since the 1980s.[2,3] The studies behind such ideas are relevant even today in the application of encryption technology, and they have spawned diverse proposals for electronic payment systems around the world, some of which are in actual use. In Japan, e-money is widely used in the transport and retail sectors.

However, most such utilitarian forms of e-money are regulated by the financial authorities as debts of the issuing entities, and the transactions are not anonymous. Satoshi would have seen this as being far from ideal. He proposed the Bitcoin as a system of electronic payment that allowed transactions to remain anonymous and could take place without a trusted third-party intermediary.

---

[1] Nakamoto (2008).

[2] Chaum (1982).

[3] Okamoto and Ohta (1989).

Technologically speaking, the Bitcoin is no more than the merger of two previously existing projects. One was Surety.com's electronic record authentication service,[4,5,6] and the other was the Hashcash[7] project. The Bitcoin was no more than a combination of the latter's PoW concept with the former's system of linking hash functions to make it difficult to falsify data. Based on the fact that it enabled online money transfers without going through a third-party intermediary, the Bitcoin came to be known as a form of electronic cash.

We will not go into the details of the principle behind the Bitcoin, but the important thing to note is that there exists no organization, such as an issuing company, that supports the Bitcoin. What supports the Bitcoin system is, essentially, a computer-generated resource exchanged among individuals who endorse the concept of the Bitcoin or want to profit from it. Bitcoin transactions are not governed by specific contracts or legal frameworks, but merely by a code (a computer program). Even that code is publicly accessible and can be freely modified (subject to peer review and testing) by developers on a voluntary basis.

The code has important economic consequences (such as crypto asset price changes or the settlement of leadership struggles among traders). The emergence of this kind of a world dominated by code was predicted right from the time the Internet was born, but the prediction came true earlier than expected, and the fact that it took the shape of a crypto asset worth tens of trillions of yen was enough to astound people.

## 3 Jolted Awake by the Cyprus Financial Crisis

The Bitcoin system used its own monetary unit, bitcoin (BTC), which did not have a fixed rate of exchange with legal currencies such as dollar (USD) or yen (JPY). Even e-money that comes with a guarantee from issuers that it can be used at the same rate as legal tender for making purchases took time to gain the trust of users and be widely accepted. No wonder, then, that crypto assets, which have unique currency values that make them difficult to use either for purchases or as a means of storing value, were not accepted by the public—until the Bitcoin emerged.

As bitcoins began to be increasingly exchanged among and mined by enthusiasts, BTC's rate of exchange with legal currencies began to rise. In the beginning, it had almost no worth, but by 2012, it had become worth around USD 10. But it was the outbreak of the Cyprus financial crisis on March 28, 2012, that transformed the Bitcoin from a game for enthusiasts to a practical investment option (see Fig. 1). When banks in Cyprus, a small Mediterranean island country, temporarily suspended operations during the financial crisis there, bitcoins were used, and gained widespread

[4] Haber and Stornetta (1991).

[5] Bayer et al. (1993).

[6] Haber and Stornetta (1997).

[7] Back (2002).

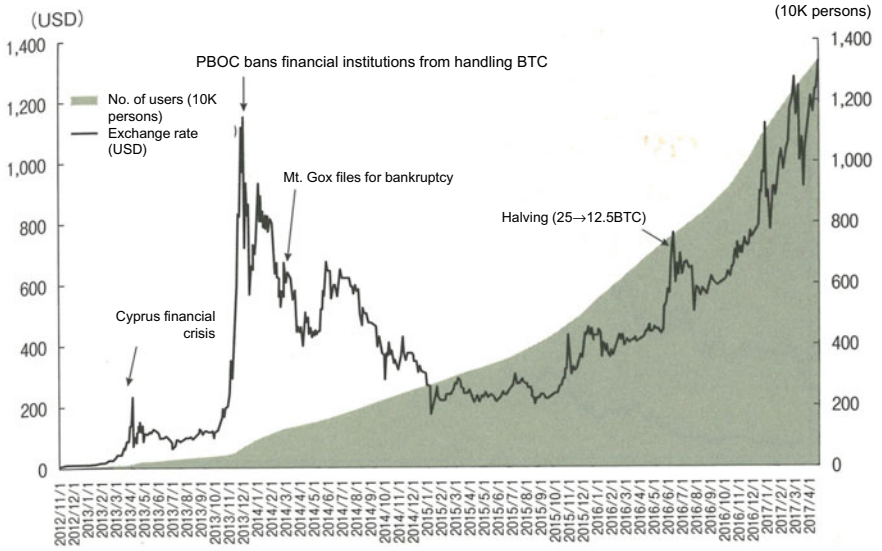



**Fig. 1** Bitcoin price trends and user statistics (2013–16). *Source* blockchain.info

attention, as a means of transferring funds abroad. As a result, the price of BTC, which had been around USD 20 before the crisis, rocketed to nearly USD 200. Of course, the rate went down again once the crisis ended, but the incident highlighted the ability of bitcoins to be used for international fund transfers, causing it to gradually strengthen.

The next wave came toward the end of 2013. When a Chinese e-commerce site enabled payment in bitcoins, it triggered a bitcoin speculation fever in the country. The market overheated and BTC quickly shot up to USD 120.

Concerned about the overheating, the People's Bank of China (PBOC) banned domestic banks from paying out bitcoin purchase funds at the end of 2013. This caused the currency to plummet to half its previous price, to USD 600. Shortly thereafter, the largest bitcoin exchange in the world, Japan-based Mt. Gox, filed for bankruptcy, setting off a downward trend for BTC. By 2015, BTC had returned to its former price in the vicinity of USD 200.

It remained at that level for a while, but began to recover once again in 2016. Several explanations are offered for why this happened, such as that the potential of blockchain technology began to draw attention internationally or that more individual investors were buying BTC for speculation purposes, but it is not clear which of these explanations is correct.

Even if a commodity is not backed by the government or supported by business confidence, it can have value if there is a possibility that somebody might buy it from you for a high price, and this value changes based on people's expectations. In particular, in this era of monetary accommodation around the world, the target policy interest rate of central banks in the major economies has been close to zero.

Undoubtedly, this excessive monetary accommodation has also had a hand in creating an abnormally big market for crypto assets.

## 4 Rise of 2017 and Fall of 2018

The price of BTC began to rise rapidly at the start of 2017. The currency, which was being sold at around USD 1000 in January 2017, had appreciated as much as twenty times by the end of the year, hitting USD 20,000 at one point in December 2017 (see Fig. 2). Every time the price hit a new milestone, there was wide media coverage, and an increasing level of public attention was inevitably directed at the rates.

This soaring of BTC prices was a phenomenon that surpassed the expectations of finance professionals. Economists who place importance on economic fundamentals have been declaring that crypto assets, which are not backed by either government or business confidence, have an intrinsic value of zero and will eventually converge at that price. Professional traders, who place importance on market trends, have also avoided investing in crypto assets, being unable to calculate their theoretical price and not liking that there are no safeguards in place against broker accidents or bankruptcies. Investments in crypto assets, therefore, are entirely the preserve of individual investors, who are amateurs, and they were the only ones who benefited from the soaring of BTC in 2017.

In 2017, the prices of other cryptocurrencies rose even more dramatically than that of BTC, and the total value of all crypto assets in circulation for the entire year

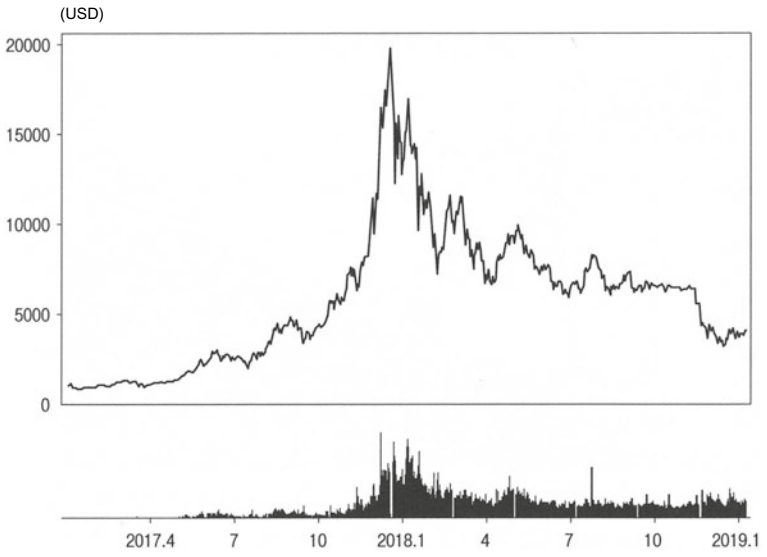



**Fig. 2** Bitcoin price trends (since 2017). *Source* coinmarketcap.com

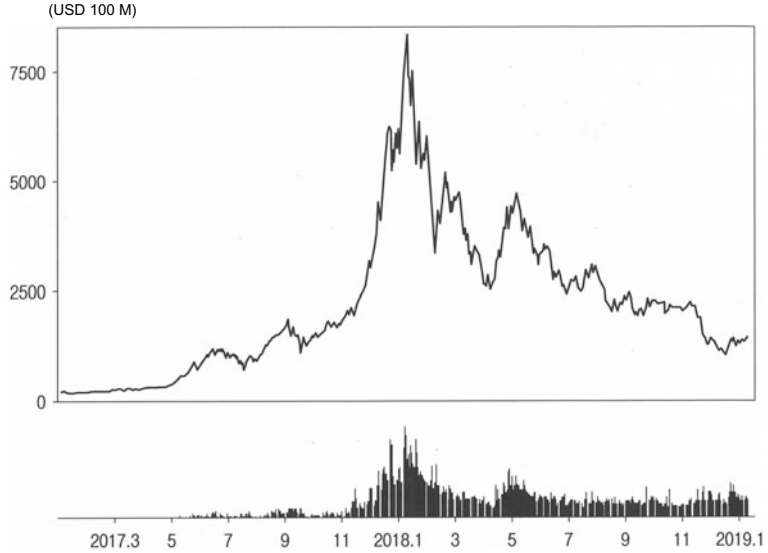



**Fig. 3** Aggregate market value trends of all cryptocurrencies (since 2017). *Source* coinmarketcap.com

was almost 50 times greater than that for the previous year (see Fig. 3), expanding from JPY 2 trillion (USD 1.77 billion) to JPY 90 trillion (USD 83 billion). This is an amount equivalent to the currency in circulation in Japan (JPY 100 trillion) or the aggregate market value of stocks listed on the First Section of the Tokyo Stock Exchange held by individual investors. The rise in the price of cryptocurrencies was so dramatic that many senior central bank and finance ministry officials in major developed economies began to voice extreme concern over it.

And then in January 2018, crypto asset prices entered an adjustment phase. The price of BTC plunged to below 10,000 USD on January 18 and subsequently began to fluctuate wildly. However, this was a natural correction to be expected following a rapid increase in price, and many market participants remained bullish on the currency.

What poured cold water on the enthusiasm was an incident of the theft of crypto assets in Japan. Coincheck, the largest domestic bitcoin exchange, lost the entirety of customers' NEM crypto assets in its custody to theft. The assets were worth a total of JPY 58 billion. Coincheck confessed that its security measures had been inadequate and compensated customers for their losses, but was forced into a long-term suspension of operations and was given two business improvement orders by the Financial Services Agency (FSA). Following wide media coverage of the incident, the price of BTC fell again and has not risen over USD 10,000 since April 2018 (as of the writing of this book).

Having fallen to USD 6000 in June, BTC remained relatively stable between USD 6000–8000 until mid-November, but it fell sharply again between mid-November and

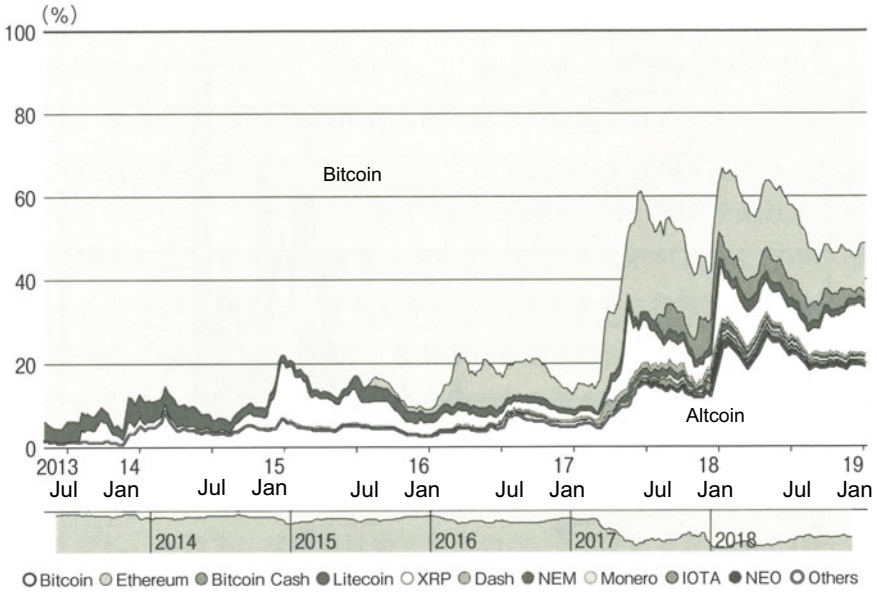



**Fig. 4** Currency-wise composition trends of the distribution value of crypto assets (past five years). *Source* coinmarketcap.com

early December, ending the year at USD 3800, a fifth of the peak price posted barely a year before.

## 5 A Magic Wand Called ICO

The price of BTC soared by 20 times over the course of 2017. Meanwhile, the total value of all crypto assets soared by 50 times during the same period. As a result, the share of BTC in the larger crypto asset market more than halved, from about 85% to under 40% (see Fig. 4). This change took place over an extremely short period of time, having started only in May 2017. Before that, the share of BTC in the crypto asset market had never been lower than 80%. Therefore, in order to understand what happened in the crypto asset market in 2017, it is important to look not just at the Bitcoin, but also at other crypto assets (collectively termed "Altcoin").

It is thought that the driving force behind the expansion of the cryptocurrency market in 2017 was the Initial Coin Offering (ICO). An ICO "collectively means an activity to raise funds from the public using a digital token issued by a company or an individual."[8] The mechanism of an ICO warrants some explanation.

[8] From "Initial Coin Offerings (ICOs)—User and business operator warning about the risks of ICOs," posted on the FSA website dated October 27, 2017.

The total value of ICOs undertaken in 2017 amounted to JPY 400 billion, which is 40 times the amount of the previous year. The total value of ICOs organized in 2018 amounted to JPY 2 trillion.

Most ICOs are based on the crypto asset platform Ethereum and are issued in the form of digital crypto assets called ERC-20 tokens. One needs Ethereum to buy such tokens, so with an increase in ICOs, the demand for Ethereum increases, and so does its rate of exchange. Again, although the money paid toward obtaining ICO tokens is not reimbursed, because these tokens are Ethereum denominated, their dollar value goes up when Ethereum appreciates. As a result, the price of the tokens in the secondary market rises, further invigorating ICO activity. This kind of positive feedback loop is thought to have been behind the rapid rise in the amount of ICO tokens issued and in the price of Ethereum from May 2017 (see Fig. 5).

Let us take a look at the reality behind ICOs, which became the engine driving the rise of crypto assets in 2017, and the various arguments related to their regulation.

ICOs are sometimes characterized as Initial Public Offerings (IPOs) using digital assets, but in fact, there is another difference. The entity planning an ICO need not be a corporation. It could be an individual who comes up with a somewhat attractive plan for a small new business he or she hopes to set up with friends, or a group of people who have gathered together for this purpose over the Internet. The first thing such people create is a business plan called a "white paper."

This document, which is on average several dozen pages long, is sometimes explained as being similar to the prospectus for a stock or bond initial or secondary offering, but in reality, it is much more random. A prospectus is issued for the

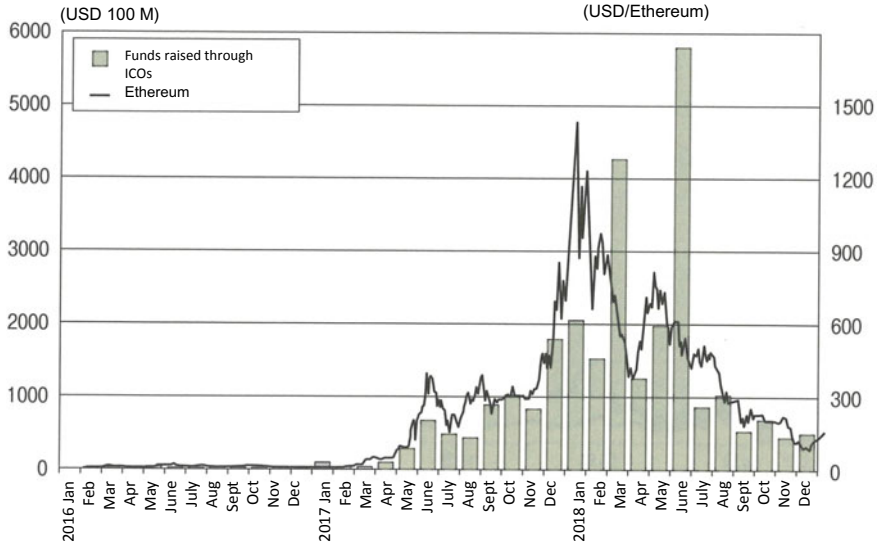



**Fig. 5** ICO-based fundraising and Ethereum price trends. *Source* www.coinschedule.com, www.coingecko.com

purpose of providing information on the basis of which investors can make investment decisions. It covers certain standard topics and is liable for damages if found to have misrepresented the facts. By contrast, ICO white papers are not governed by the law, nor are their contents standardized. They are often rewritten subsequent to the implementation of the ICO.

Tokens issued during ICOs are also different from stocks and bonds. Token owners, unlike shareholders, do not have the right to receive dividends or participate in the management of the company, nor are the tokens, unlike corporate bonds, repayable upon maturity. The tokens merely come with something like discount coupons, called "utility tokens," that can be used to purchase the products or services of the business operated by the token-issuing entity. As a result, the entity making the ICO can raise funds in exchange for tokens with almost no obligations.

Common sense would seem to dictate that, like stocks or bonds, tokens issued for purposes of fundraising would be better received if they bound the issuing entity to paying some form of dividend or repayment of the principal. However, ICO tokens would risk being seen as marketable securities governed by the securities laws of the land if they were to commit to paying out dividends or repaying the principal. And the act of issuing marketable securities to the public would make the issuing entity subject to disclosure requirements and various other behavioral regulations under the securities act. This is why token-issuing entities issue utility tokens, which are a type of "wildcat securities," in an effort to circumvent the aforementioned regulations.

It is surprising enough that anyone would be willing to buy such "worthless" tokens, but the fact is that these ICO tokens were so popular that the websites of issuing companies ended up crashing due to excessive traffic from would-be investors. Why did investors buy these tokens? They did so because they wanted to sell them in the secondary market and make a profit on the sale. In fact, investors who bought ICO tokens issued during January–March and April–June 2017 and held them until the end of the year made profits that were, on average, 18.3 times and 3.5 times the invested amount, respectively.

Although the number of times by which the price increased obviously fell during the second half of the year, the rumor that buying ICO tokens in the primary market and selling them in the secondary market was profitable spread like wildfire among crypto asset investors, resulting in a huge surge in the popularity of ICOs, thereby causing the price of crypto assets also to soar.

If the fundraising entities were to make good use of the craze to develop sterling products or services that contribute to economic growth, then perhaps ICOs could be acknowledged to have some value. However, there is no guarantee that those who raise money through no-obligation utility tokens rather than by taking loans or issuing stocks will put that money to effective use.

In a paper titled "Digital Tulips? Returns to Investors in Initial Coin Offerings" published in May 2018, Boston University research scholars Hugo Benedetti and Leonard Kostovetsky analyzed the behavior of token-issuing entities following an ICO. They did this by counting the number of tweets made from the twitter accounts of projects for which funds had been raised through an ICO and conjecturing that a project had expired when the tweets died down.

| ICO issuer category | Number of issuers | Number remaining after 120 days | Number gone by 120th day | Disappearance rate at 120 days (%) |
|---|---|---|---|---|
| No funds raised, no tokens listed | 694 | 118 | 576 | 83 |
| Funds raised, but no tokens listed | 420 | 200 | 220 | 52 |
| Funds raised and tokens listed | 440 | 369 | 71 | 16 |
| Total of all categories | 1,554 | 687 | 867 | 55.8 |

**Chart 1** ICO issuer disappearance rate by 120th day after the issue. *Source* From Benedetti and Kostovetsky (2018); some figures estimated by author

Since community management through dialog with ICO token buyers is an important business activity, twitter is often used as a means to conduct such dialog, so Benedetti and Kostovetsky's approach is persuasive. Their paper analyzes the official twitter feeds pertaining to as many as 4003 ICOs that were either implemented or planned. Table 1 summarizes the knowledge gleaned through their study (the paper itself presents the data as running text, but I have presented it in a chart here).

It is understandable that 83% of the projects that failed to raise funds would have disappeared by the 120th day. By contrast, only 16% of the projects that had both been able to raise funds and list tokens had disappeared within 120 days. Having said that, companies that list their stocks on the market through an IPO rarely ever disappear (go bankrupt or close down) even if they are venture firms, so a 16% disappearance rate within four months should be seen as quite a high rate.

Entrepreneurs who set up venture firms work very hard for business success so that they can return the borrowed capital and become wealthy. By contrast, if someone can obtain large sums of money simply by writing a white paper, it is unsurprising that their motivation to work hard in pursuit of business success is not too strong. As for those who invest in these ICOs, they are happy so long as they can resell their tokens in the secondary market for a higher price, because whether or not the business ultimately succeeds is no concern of theirs. Consequently, the contents of white papers tended to be vague and sloppy, sometimes not even complete as documents, and yet this did not seem to affect the sale of ICO tokens in 2017. Since the end of 2017, of course, many ICOs have ended unsatisfactorily, without selling many tokens, but the enthusiasm of issuers who hope to procure funds with no strings attached remains strong.

The mechanism of an ICO is like an enormous game of Old Maid. While both the issuer and the primary market issuers make a killing, investors who buy these tokens at high prices in the secondary market are ultimately left holding worthless tokens. Even in a scenario where the issuer's business project succeeds, the fruits of that success are not shared with the token owner, so it is almost certain that the tokens will be worthless once the overheated market cools down. In this sense, the whole thing is an extremely unethical setup.

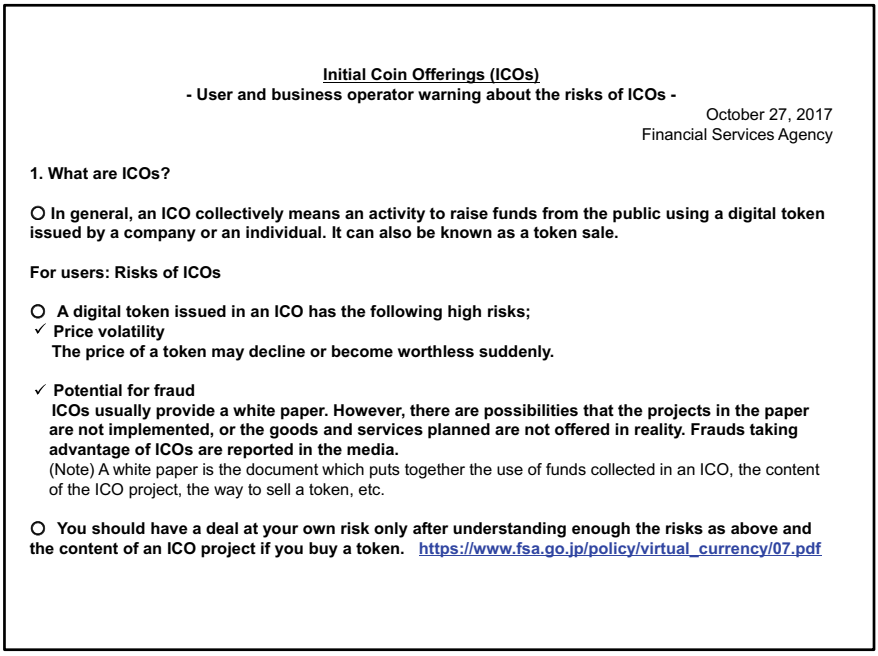
Regulatory authorities around the world have begun to attempt regulating this problem-ridden practice of ICOs.

The U.S. Securities and Exchange Commission (SEC) has expressed the view that some ICOs are equivalent to the sale of marketable securities in the open secondary market as defined by the Securities Act. It is also pushing for the prosecution of

those who conduct ICOs that are patently fraudulent. There also exist ICOs that are deemed similar to private placements under the Securities Act and regulated to offer only to accredited investors. However, there is information to show that such ICO tokens are then being resold to the general public, something that is not technically allowed under the law, and it remains to be seen whether the regulations can function as intended. In this way, the general trend in the U.S. is in the direction of regulating ICOs as a whole under the Securities Act.

Meanwhile, China banned ICOs in September 2017. A joint statement issued by various Chinese financial regulatory authorities sternly pointed out that ICOs had destroyed economic and financial order. It is said that there were as many as 65 ICO platforms in China at that time, and that an average of 10 ICOs were being held each week. According to local reports, the authorities had to step into regulate the market after it overheated to the extent that elderly people began to invest their retirement funds in bitcoins without even understanding what they were. Under the new regulations, issuers were forced to return the funds raised to the investors even in cases where the ICO had been conducted before the regulations had been promulgated.

In Japan, too, the FSA issued a warning about the risks of ICOs in October 2017 (see Fig. 6). Unusually for a document published by an administrative authority, the warning utilizes strong language, such as "become worthless suddenly" and "potential for fraud." Japan launched a system for the registration of crypto asset



**Initial Coin Offerings (ICOs)**
**- User and business operator warning about the risks of ICOs -**

October 27, 2017
Financial Services Agency

**1. What are ICOs?**

○ **In general, an ICO collectively means an activity to raise funds from the public using a digital token issued by a company or an individual. It can also be known as a token sale.**

**For users: Risks of ICOs**

○ **A digital token issued in an ICO has the following high risks;**
✓ **Price volatility**
**The price of a token may decline or become worthless suddenly.**

✓ **Potential for fraud**
**ICOs usually provide a white paper. However, there are possibilities that the projects in the paper are not implemented, or the goods and services planned are not offered in reality. Frauds taking advantage of ICOs are reported in the media.**
(Note) A white paper is the document which puts together the use of funds collected in an ICO, the content of the ICO project, the way to sell a token, etc.

○ **You should have a deal at your own risk only after understanding enough the risks as above and the content of an ICO project if you buy a token.** https://www.fsa.go.jp/policy/virtual_currency/07.pdf

**Fig. 6** Japan's FSA also issued a warning about the risks of ICOs

exchange businesses in 2017, with "crypto asset exchange business" being defined broadly to include the act of issuing ICO tokens. As a result, there have been no ICOs in Japan apart from the ones held by the single ICO exchange company in the country. Companies that had been planning an ICO and became unable to hold one are expressing their resentment, but ultimately this de facto regulation of ICOs at a time when the market was roaring and investors were expecting enormous appreciation in the value of their digital assets has been for the greater social good in the sense that it prevented investors from suffering huge losses.

BTC remained strong as a result of the expectation that bitcoins would be the "money of the future" and could be used to make payments at some point (although this is unlikely even in the future). The price of Ethereum rose dramatically as a platform for ICOs. With this strong rise in the price of two types of crypto assets, people began to expect that other cryptocurrencies would also strengthen as the second or third Bitcoin or Ethereum.

As a result, a large number of mostly worthless crypto assets began to see a dramatic surge in their prices starting May 2017. As relatively well-known cryptocurrencies were bought up by investors and appreciated, the associated sentiment was transmitted also to crypto assets that were relatively unknown and were of little worth. This can be thought of as a phenomenon similar to "sector rotation to low-level stocks" when the stock market is on the rise.

And then, the icing on the cake of the 2017 crypto asset market boom was the listing of bitcoin futures on the Chicago Mercantile Exchange (CME) and the Chicago Board Options Exchange (CBOE). With the launch of bitcoin futures, investors began to expect that crypto assets would be officially recognized as financial products and that enormous investment funds would start pouring into them from financial institutions and institutional investors. This expectation was what rocket-launched the price of BTC from USD 10,000 to USD 20,000 within the space of three weeks.

## 6 Cyber Attacks on Bitcoin Exchanges

From the start of 2018, the crypto asset market entered a correction phase. One reason for the fall in prices was an incident in which NEM tokens with a market value of JPY 58 billion[9] were stolen from Coincheck, a fledgling bitcoin exchange that had not yet completed its registration under the Crypto Assets Act. An unauthorized entry was made into Coincheck's system using the private key of a digital signature managed by the company, and all the NEM tokens in possession of the company were transferred to a different account. All the customer assets in Coincheck's custody were stolen.

How could such a thing happen? For a company to which customers had entrusted their precious crypto assets, Coincheck did not have sufficient safeguards in place. It had put the NEMs deposited by all 260,000 of its customers into a single large wallet. The wallet was connected to the Internet at all times, enabling assets to be

[9] A digital currency, the abbreviation standing for "New Economy Movement."

| | Amount (XEM) | Remitting address | Receiving address |
|---|---|---|---|
| 2018/1/26 8:26 | 800,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 4:33 | 1,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 3:35 | 1,500,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 3:29 | 92,250,000 | NC4C6PSUW5 | NA6JSWNF247 |
| 2018/1/26 3:28 | 100,000,000 | NC4C6PSUW5 | NDDZVF32WB |
| 2018/1/26 3:18 | 100,000,000 | NC4C6PSUW5 | NB4OJJCLTZW |
| 2018/1/26 3:14 | 100,000,000 | NC4C6PSUW5 | NDZZJBH6IZP |
| 2018/1/26 3:02 | 750,000 | NC4C6PSUW5 | NBKLOYXFIVF |
| 2018/1/26 3:00 | 50,000,000 | NC4C6PSUW5 | NDODXOWFIZ |
| 2018/1/26 2:58 | 50,000,000 | NC4C6PSUW5 | NA7SZ75KF6Z |
| 2018/1/26 2:57 | 30,000,000 | NC4C6PSUW5 | NCTWFIOOVIT |
| 2018/1/26 0:21 | 3,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:10 | 20,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:09 | 100,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:08 | 100,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:07 | 100,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:06 | 100,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:04 | 100,000,000 | NC3BI3DNMR2 | NC4C6PSUW5 |
| 2018/1/26 0:02 | 10 | NC3BI3DNMR2 | NC4C6PSUW5 |

**Chart 2** Movement of NEM tokens during the Coincheck incident. *Source* Created by author using NEM blockchain information

deposited or withdrawn at will. The procedure for transferring crypto assets from the wallet was protected by no more than a single cryptographic key, and the safety management of this key appears to have been sloppy, as someone managed to make unauthorized use of it to transfer all the NEM tokens (see Chart 2).

In Chart 2, the "NC3…" address highlighted in gray belonged to Coincheck. NEM tokens worth JPY 58 billion deposited by Coincheck's customers were all stored in this address. Meanwhile, the "NC4…" address highlighted in black was the address the thief had prepared. On January 26, the thief made the first transfer of XEM[10] 10 at 0:02 h. Within 20 min of this, additional transfers worth XEM 5.23 billion had been made. The thief then re-transferred the stolen NEM tokens from the NC4 address to multiple other addresses. There were more illegal transfers from NC3 to NC4 that same day, sometime during the hours of 03:00, 04:00, and 08:00.

Of course, the greatest share of the blame goes to the thief who made these illegal transfers. This person, who then became the sole manager of JPY 58 billion worth of NEM tokens, gradually exchanged them for other currencies over the Internet and, having laundered all the funds, vanished into thin air.

This is not an isolated incident, and the problem is not just Coincheck's. There have been numerous incidents of the hacking of crypto asset exchange companies and the theft of their crypto assets. Exchanges currently operating could also be vulnerable—they may unwittingly be putting the assets their customers have deposited with them at risk. At the current time, there are neither any uniform security standards

[10]ISO code for NEM.

across the crypto asset industry, nor is there any disclosure requirement regarding the management structures, governance, or status of security measures in these companies.

Japan was one of the first countries to enact laws to regulate crypto asset exchange companies, and it has a registration system for such companies. However, the main objectives of existing laws and systems are to prevent money laundering and terrorism financing. Current laws related to crypto assets are not based on an awareness that the exchanges are holding customer assets worth large sums of money and they, therefore, have not created strong user protection mechanisms. Given that the current situation is very different from what had been assumed at the time of these laws' formulation, the laws need to be revised. The crypto asset industry should also utilize systems used by trust banks and insurance companies to autonomously promote initiatives that help limit damage. Further, the authorities must work to dispel user concerns by establishing standards for security measures and enforcing compulsory disclosure. To prevent the recurrence of incidents such as the one discussed above, efforts must also be made to constantly keep relevant systems and regulations up to date.

For most people, one of the strange things about the abovementioned incident is that the NEM funds cannot be restored to the original address even though their transfer to the thief's address can be confirmed. If such a thing had happened with a bank deposit, as soon as it became clear that the stolen funds were in a specific deposit account, that account could be frozen by the authorities, and it could be expected that the stolen funds would eventually be returned to the account they were stolen from.

Right from the time people first began to talk about the Bitcoin, the special concept behind this cryptocurrency has drawn attention. This involves a policy of not being governed by a trusted central bank, which is why the Bitcoin is called "trustless." It is thought that this special characteristic of the Bitcoin is the reason it was able to break through national barriers resulting from differences in governing laws and political systems and become truly international in its usage.

By contrast, the conventional system, which is governed by a trusted central bank, exists in a "trust-based" environment. Because we live in a world that assumes the presence of trusted central authorities such as the government, the central bank, the court system and so on, a trustless world seems extremely special and risky to us. Nevertheless, the existence of the Bitcoin has been acknowledged, and the trust-based and trustless worlds have been coexisting.

For instance, geeks who are directly connected to the Bitcoin network through what are called "nodes," live in a trustless world. On the other hand, amateur users cannot directly connect to a node. They simply have bitcoin deposits with bitcoin exchanges and depend on these exchanges to trade their bitcoins for them. In the case of these amateur users, the bitcoin exchange becomes the "trusted third party," so a trust mechanism exists within this relationship (see Fig. 7).

In the aforementioned incident, the NEM tokens were stolen and laundered in a trustless world. There being no trusted central authority in that world, no entity, including the national government, could arbitrarily rewrite the information to restore

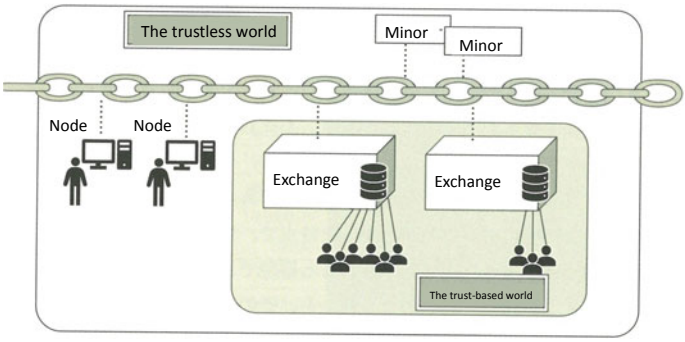



**Fig. 7** Challenge of a trust-based world existing within a trustless world

the stolen funds. In light of the NEM theft incident, therefore, trustlessness is a double-edged sword.

Can the government appropriately control this alien concept of cryptocurrencies? In other words, can it make good use of its positive aspects while compensating for/rectifying its negative ones? In order to deal with this novel challenge, those concerned will need to put their heads together and find solutions, including those in the form of international regulation systems.

## 7 Cashless Society and Central Bank Digital Currencies

(1) Heating Up of the Central Bank Digital Currency Argument—Shock to the System from the Emergence of the Bitcoin

Until around 2012, there were no serious discussions among central bank officials and related persons about the digitization of banknotes (paper money) through the issuance of a central bank digital currency (CBDC). This is probably because of the strong level of confidence in existing settlement systems such as bank note systems, systems provided by the central bank or private banks, and the international settlement system SWIFT (Society for Worldwide Interbank Financial Telecommunication). In a sense, the topic itself was considered taboo. To some extent, people realized that e-money would eventually be used and that the world would become increasingly cashless, but it was thought that this was in the distant future. However, starting around 2013, an increasing number of central-bank officials and others began to bring up the idea of central banks issuing digital currencies. This development was related to the Bitcoin beginning to draw attention on a global scale.

To be sure, the Bitcoin was drawing attention in countries around the world, and its price was soaring, but in the view of financial experts, the currency's utility as a payment method was low, and it was clearly still in its experimental stages. So,

imagine the shock waves sent through the financial industry, and especially in the central banks, when the Bitcoin began to be used worldwide via the Internet.

Until then, financial transactions in capital or securities were regulated by each country's financial authorities. Regulatory authorities in each country issued licenses based on domestic laws to businesses facilitating such transactions, permitting them access to the domestic market. With the internationalization of finance, the international exchange of capital and securities expanded among the developed countries, but despite the fact that the majority of financial transactions simply involve an electronic exchange of information, national boundaries have continued to represent major barriers to financial transactions.

However, as mentioned earlier, during the Cyprus financial crisis of March 2013, bitcoins managed to break through this barrier very easily. In principle, anyone can buy and sell bitcoins so long as they are connected to the Internet. In fact, it was widely touted that international transfers could be made very inexpensively using bitcoins compared with regular money transfers, for which hefty transfer charges apply.

The rise in Bitcoin's popularity set many imaginations on fire regarding the future of finance. If existing banknotes and inter-bank networks were difficult to use due to the associated high costs, perhaps they would be replaced by crypto assets, which can be exchanged over the Internet. Perhaps the first central bank to conduct experiments and gain experience in the area would become the de facto standard-bearer of the future. Anticipating such a future, central banks, which have traditionally not competed with their international counterparts, began to compete. As a result, discussing the idea of central banks issuing digital currencies stopped being taboo.

(2) A Diversity of Ideas Related to CBDCs—Three Main Types

Different people and organizations seem to have different ideas about what a CBDC is. Even when it comes to the appellations, apart from the relatively common CBDC, there are terms such as Central Bank Cryptocurrency (CBCC), as often used by the Bank for International Settlements (BIS); Digital Base Money (DBM), as used by the European Central Bank (ECB); and Digital Fiat Currency (DFC), as seen in central-bank discussions in emerging market economies (EMEs).

The technologies used and implementation formats are also diverse. First, there is the concept of central banks issuing e-money similar to Suica. It would not be impossible for an e-currency like Suica to replace banknotes in terms of functionality, but it is predicted that it would be technologically challenging to keep a centrally-managed system like Suica up and running at all times and to maintain its nationwide settlement functions.

Another idea is for central banks to issue digital currencies using blockchain technology similar to that of the Bitcoin. While such a currency would be based on a private blockchain platform like the MUJF coin or SMBC coin and have restricted access, the central bank would fix the value of one unit of the coin at one yen and guarantee this value.

A third and very bold idea is to introduce a currency based on a public blockchain platform, which can be competitively mined by private mining farms and used widely by the public. Those who advocate for this idea are of the view that mining for currencies is an efficient and stable means of operating a digital currency. In addition to the above, there are also a number of proposals for digital currencies based on an amalgamation of one or more of the above formats.

Not all of those proposals can be discussed here, but CBDCs can be divided into the following three types in an effort to understand the direction of the debates.

The first type is inspired by the Bitcoin, and is a form of digital currency currently being researched by central banks in developed countries. Discussions about this type of digital currency, called CBDC or CBCC, are led by the BIS's Committee on Payments and Market Infrastructures (CPMI). There are no examples of actual implementation so far.

The second type of digital currency, called DFC, is being promoted mainly by African nations and EMEs. It is based on the idea of the central bank becoming involved in private-sector platforms (such as M-PESA), the use of which have been promoted toward achieving greater financial inclusion in developing countries in Africa and elsewhere. The discussions have mainly been led by the countries of Africa at the International Telegraph Union Telecommunication Standardization Sector (ITU-T), but other countries—including China, Russia, and India—have also joined.

The third type is a digital currency is being considered by South American central banks, which have been promoting dollarization as a way to combat inflation. One of the characteristics of this type of digital currency, exemplified by such currencies as the Uruguayan e-Peso and the Venezuelan petro, is that it is often extemporaneously launched.

(3) CBDCs in Developed Countries—Research that is Still Far from Implementation

The BOJ's survey titled "Central Bank Digital Currencies—Discussions and Experiments by Overseas Central Banks" (BOJ Review 2016-J-19) summarizes the current status of the study of digital currencies by the central banks of the major advanced nations.

Chart 3 below summarizes the status of the study of digital currencies in key countries as presented by the survey. However, none of these countries has actually issued a CBDC as of the present time. Some of the reasons for this may be that advanced nations have well-developed fund settlement services, the financial system of each country centered around its central bank is a key part of the nation's economic infrastructure, and there is a desire not to impart a needless shock to this system. Therefore, discussions of digital currencies in developed nations are still in the stage of theoretical study.

(4) CBDCs and Financial Inclusion in EMEs and Developing Countries

(i) The Netherlands (De Nederlandsche Bank)

In March 2016, De Nederlandsche Bank (DNB) announced in its annual report that it would develop a prototype of the DNBcoin based on blockchains/distributed ledger technology (DLT). A senior bank official said in a speech later that year in June, that the central bank would conduct its own verification tests on bitcoin software in an effort to more deeply understand the functioning of blockchains. It was also revealed that the DNBcoin had been developed primarily for the purpose of tests to be conducted within the DNB, and that it would not be in wide circulation for public use.

(ii) Canada (The Bank of Canada)

Through a speech delivered by Deputy Governor Carolyn Wilkins on June 17, 2016, the Bank of Canada (BOC) revealed that it would conduct experiments on DLT in partnership with commercial banks and private-sector corporations. BOC staff have explained the overall details of the experiment at various venues, including forums of various kinds. For instance, at the October 2016 Chicago Payments Symposium, the BOC announced its plan to use a pseudo environment replicating interbank transactions to enable private-sector financial institutions participating in the experiment to deposit funds into a BOC special account as security, in return for which the BOC would issue DLT-based central bank debt certificates (deposit securities). The BOC has stated that the objective of this experiment is to comprehend the mechanisms, limits, and possibilities of DLT technology by testing it in an experimental large-scale settlement system environment.

(iii) The United Kingdom (The Bank of England)

In the UK, in February 2016, following discussions with the staff of the Bank of England (BOE), University of London research scholars published a paper proposing a system for the RSCoin, a digital currency to be issued by the central bank. Under this scheme, intermediary entities called "mintettes," which link the central bank and users, would play a specific role in issuing and managing RSCoins. While the central bank would be the issuing entity for RSCoins, multiple mintettes would be commissioned with processing tasks, such as checking and approving the details of transactions and sending the relevant information to the central bank. Further, in order to ensure the appropriate functioning of mintettes, the central bank would regularly check to confirm the consistency of the generated "blocks" (in the blockchain), and if any inappropriate processing were to be detected, the mintette responsible for that process would be excluded.
In a speech given in June 2016, Governor Mark Carney revealed that the BOE was thinking of incorporating the use of DLT in its core operations and studying and analyzing ideas related to the issuance of a CBDC. Further in a public letter of intent to design a new Real-Time Gross Settlement (RTGS) system released in September 2016, the BOE announced that DLT, while not yet mature enough as a technology to guarantee the extremely high standards of stability required in an RTGS system, held the potential to change the way settlements were made, and that the BOE would continue to research this technology in collaboration with academics, fintech companies, and central banks in other countries.

(iv) Russia (The Bank of Russia)

The Bank of Russia announced in October 2016 that it had developed a prototype of a DLT-based financial information communication tool called Masterchain in collaboration with market participants. Deputy Governor Olga Skorobogatova said that the prototype would continue to be studied by the FinTech consortium, including the possibility of its future incorporation within the country's next-generation financial infrastructure.

(v) China (The People's Bank of China)

As of date, the People's Bank of China (PBOC) has not officially announced having conducted experiments related to blockchains or DLT. On the other hand, it has revealed to external sources that it already has the systems in place to start issuing its own digital currency in the medium term. Specifically, the PBOC held an investigative committee meeting on January 20, 2016, at which views on digital currencies were exchanged with experts. Additionally, the investigative committee has asked the PBOC's study group to not just incorporate the results of digital currency-related research from both within and outside China, but also to further clarify the Bank's strategic goals with regard to digital currencies and work toward enabling the Bank to announce the issue of a digital currency as early as possible.
In a Bloomberg article dated September 16, 2016, Deputy Governor Fan Yifei wrote about the format of digital currency being considered by the PBOC. He said that the Bank was leaning toward an indirect approach, where a digital currency would first be issued by the central bank to private banks, and the latter would then offer deposit and withdrawal services related to the currency to the general public. As for the reasons why such an approach was preferred, Mr. Fan noted that utilizing the existing banknote circulation framework would make it easy to gradually replace banknotes with the digital currency, and that the participation of private banks in managing the digital currency issued by the central bank would disperse the risks as well as promote innovation, thereby contributing to the real economy and helping respond to the needs of the people.

**Chart 3** Digital currency consideration status in major countries. *Source* BOJ Review 2016-J-19

As recently as 2010, about half the world's population did not have a bank account. However, that number has declined dramatically in recent years, owing to rapid progress in IT-based financial inclusion initiatives in EMEs and developing nations. The M-PESA initiative that was begun in Kenya is a representative example (details in the next section). China's progress toward realizing a cashless society has also been remarkable.

Taking such changes into account, EMEs and other developing economies have begun contemplating the idea of positioning such new means of settlement as "digital fiat currency." I will dedicate a separate section to discussing the actual status of developments toward realizing cashless societies.

What is important to note here is the move to call these new payment methods "digital fiat currency." ITU-T is one of the sectors of the International Telecommunication Union and is in charge of formulating international standards in the field of telecommunications. In 2017, the Focus Group on Digital Currency including Digital Fiat Currency (FG DFC) was set up as a subsidiary body of the ITU-T. The focus group is chaired by representatives from African nations as well as China, Russia and India. Their first meeting was held in October 2017 in Beijing. At the workshop that

was also held as part of this meeting, the head of the PBOC's Digital Currency Organization attracted widespread attention by announcing that the PBOC had already completed technological experiments necessary for issuing digital currency.

(5) Central Bank Digital Currency Implementation in South America

Unlike the developed nations, which are still pondering the issue, many central banks in South America have already issued digital currencies. In countries like Ecuador, Uruguay, and Venezuela, a national digital currency is the reality, not a research topic. This has to do with the fact that such countries have long struggled with inflation. Given that their domestic currency systems have never been sufficiently functional, and going by their previous experiences with dollarization policies, they were able to go ahead and issue experimental digital currencies without worrying much about its impact on their existing currency systems.

Of the three countries mentioned above, Venezuela is the one that has drawn the most attention. In January 2018, Venezuelan President Nicolás Maduro ordered the issuance of the first 100 million petros, the CBDC of Venezuela backed by its petroleum reserves. According to Maduro, the price of one petro is equivalent to the price of one barrel of Venezuelan oil. He further explained that shares in oil reserves and in diamond and gold mines would be sold to prop up the currency.

The petro was issued and circulated using blockchain technology, similar to the Bitcoin. It takes the form of an ERC-20 token. In other words, it was issued by an ICO implemented by a country. It is said that Venezuela managed to raise USD 5 billion through the issue of this currency.

Maduro took over as president of Venezuela after the death of former president Hugo Chávez, long known as a high-profile foe of the United States. As is widely known, Maduro's government was subjected to U.S. sanctions that have undermined the nation's economy and resulted in astronomical inflation rates. Maduro was able to implement an executive order creating the petro despite opposition from the country's National Assembly (in which the opposition party is in the majority), which characterized the presidential order as unconstitutional. Under normal circumstances, a country like Venezuela would be unlikely to raise even a single dollar attempting to procure funds in the normal way in the international financial market. Many media reports have expressed serious misgivings about the fact that Venezuela was able to issue a CBDC that was effectively like a magic wand that could make many of its problems go away.

## 8 Cashlessness and the Future of Currencies

(1) Trends Toward Cashlessness Around the World

When considering the various possible forms of cash settlement systems, one is likely to begin by looking back at the historical stages of the evolution of cash

settlement systems. For instance, many human societies progressed from gold coins to paper money, and from paper money to banking system-based electronic payments. One might further consider how the banking system has progressed to allow us to make payments 24/7. One can also think of the progress from bank tellers to ATMs to mobile payment systems. These are the various stages of progress in financial settlements seen in the developed parts of the world.

However, not all the world's countries have gone through the same payment system evolution stages. In the case of telephones, for instance, the developed world had landline phones before the advent of mobile phones. Mobile phones then became increasingly small, and at some point, began to include Internet functions, eventually evolving into today's smartphones. However, in EMEs and developing countries, the smartphone is the first type of phone used by a growing number of people who never had the chance to see or use a landline phone.

The functioning of a bank branch requires electricity, water, phones, and other infrastructure. However, there are many places in the world that do not have such infrastructure. It is in these kinds of places that the digitization of settlements is now spreading rapidly.

For instance, one of the payment methods used widely in Africa is M-PESA. Based on software developed by a Kenyan student in April 2007, M-PESA began as a new settlement/money-transfer service offered by mobile network operator Safaricom using the SMS feature of smartphones. This money transfer service is cheaper than other similar services, and the fee structure is designed to facilitate frequent transfers of small sums.

Of course there are banks, bank branches, as well as banknotes in Kenya, where this new system of payment emerged, but it is only in the capital Nairobi and its suburbs that banknotes can be used for all the usual purposes. Because of the lack of bank branches in the Savanna regions, people living there have no choice but to keep wads of banknotes with them. This, however, puts them at risk of being robbed. When they want to save money, people put it into bottles and bury the bottles in the ground, but this puts the money at the risk of being swept away by floodwaters. Money transfers are entrusted to long-distance bus drivers, but there is no guarantee that such bus drivers will be conscientiously honest. This was the situation in rural Kenya through 2006 (see Chart 4).

It was into this world that M-PESA arrived in around 2007. M-PESA agencies spread rapidly throughout Kenya, enabling people to make money transfers simply by entering the number advertised by the agency into their mobile phones. M-PESA soon became the most widely used method of money transfer (over 90% of those who responded to the survey said that they used it). The legal currency of Kenya is the Kenyan shilling, and M-PESA payments are essentially made in the legal currency.

It appears that the Central Bank of Kenya (CBK) has also become involved in the M-PESA initiative, which is now being promoted as a national project. The initiative, in the same format, is also spreading to other countries, including Tanzania, South Africa, and India.

Meanwhile, Alipay, WeChat Pay, and other QR code payments have become quite common in China. For instance, there are no longer any booths selling entry tickets

(%)

| Year | 2006 | 2009 | 2013 |
|---|---|---|---|
| Family/Friends | 57.2 | 35.7 | 32.7 |
| Buses/matatus (minibuses used as public transport) | 26.7 | 4.0 | 5.4 |
| Money transfer services | 5.3 | 0.4 | 1.9 |
| Checks | 3.8 | 1.2 | 1.3 |
| Direct bank transfers | 9.6 | 3.2 | 4.3 |
| Post offices | 24.2 | 3.4 | 1.3 |
| Mobile money | 0.0 | 60.0 | 91.5 |

**Chart 4** Usage rates of various domestic money transfer channels in Kenya (comparing figures for 2006, 2009, and 2013). *Source* FinAccess National Survey 2013 (since two or more options can be chosen, the total does not add up to a 100)

to the Palace Museum, a world heritage site in Beijing. Instead, there is a large board bearing a magnified QR code that those wishing to gain admission can scan using their smartphones to make an electronic payment. This has eliminated long lines at the entrance and greatly reduced waiting times. It has also eliminated the problem of ticket snatchers, and is likely to have significantly reduced operational expenses related to manning ticket booths and cash management.

It is the inconvenience endured by those without access to the banking system that is propelling the trend toward cashlessness in China and the African countries. As of 2010, half the global population had no access to banks and could not use banks for savings or money transfers (see Fig. 8).

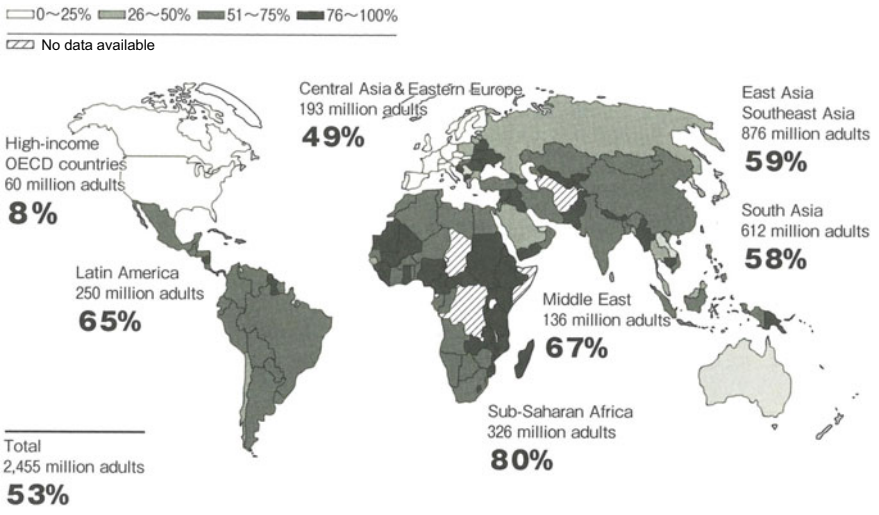



**Fig. 8** Ratio of the population without access to banks as of 2010. *Source* World Bank

Of these people, those who were able to obtain smartphones were quite eager to use systems like M-PESA, Alipay, and WeChat Pay, resulting in the rapid spread of such systems. Once something like this happens, business establishments have to hop on board by offering QR-code-based payment methods or risk being left behind. Once most businesses are on board, people stop carrying wallets and small change. Unmanned convenience stores crop up, and society becomes increasingly cashless. It is said that, in China, people seeking donations or begging for money are now forced to print QR codes on their donation boxes or begging baskets.

There are also increasingly cashless societies among the developed nations—Sweden and other Scandinavian countries are some examples. The Scandinavian countries were keen to promote electronic settlements as national projects beginning from the 1990s. Given their small populations, it was important for them as nations to make efficient use of their human resources, and promoting electronic payments was a strategically important means of doing so.

It is a fact that most stores in Sweden either do not or cannot accept cash. It is only tourists who bring in krona notes without realizing this, putting store clerks on the spot, as they are unable to give the customer any change.

Cashlessness directly promotes a more efficient society. Once cash is no longer used, there is no need to spend resources managing, transporting, or guarding it. Once payments are made electronic, theft by store clerks is no longer an issue, and training employees to manage the cash register—which traditionally involves handling cash, coupons, and a variety of cards—becomes a much simpler process.

(2) Trend Toward Cashlessness in Japan

In Japan, however, there is an extremely large amount of cash in circulation, equivalent to 20% of the country's GDP (see Fig. 9). Japan is a relatively safe country and has a large network of ATMs, making it easy for anyone to make large payments with cash. Reflecting this, many people choose to use cash.

For instance, the Kyoto branch of the BOJ sees strong demand for unwrinkled banknotes that is rare even for Japan. Unwrinkled banknotes have traditionally been used in various kinds of celebrations as well as to pay for singing or dancing lessons, and this tradition remains alive even today in the city of Kyoto. It will probably be difficult to relinquish old systems and traditions with a long history.

A country like Japan does not have a blank slate from which to take on the challenge of cashlessness. It has a history of gradually evolving settlement methods. Because of this, Japanese people have a great deal of trust in banks and banknotes. This trust, developed during a long history of experience, is in some ways an obstacle to the spread of cashlessness and, thereby, to society's overall rationalization.

The Growth Strategy Council—Investing for the Future (Headquarters for Japan's Economic Revitalization) decided upon an extremely half-baked target for cashlessness by raising the target rate of cashless payments from 20% at present to 40% in 10 years. If the idea is to increase society's efficiency, the target should be to realize a fully cashless society.

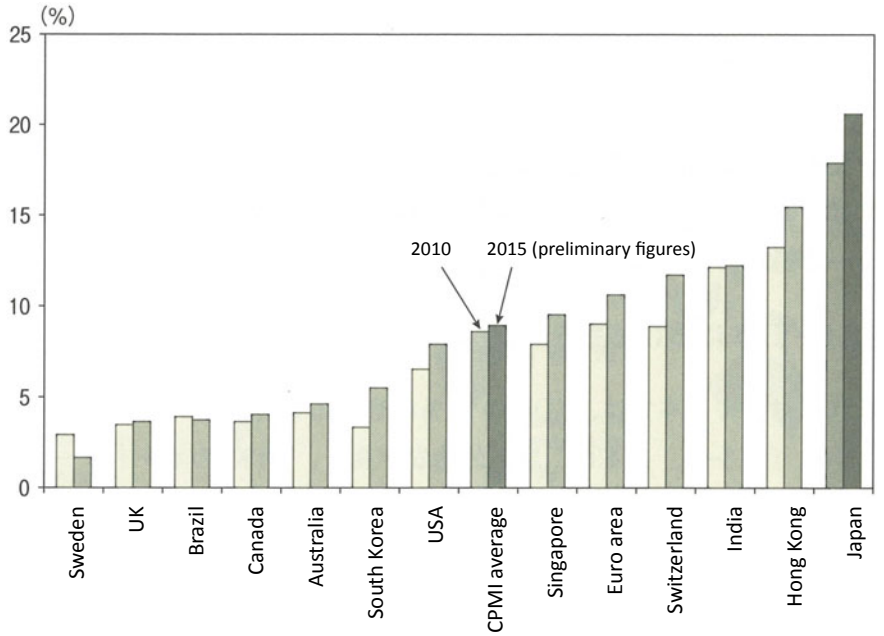



**Fig. 9** Outstanding cash in circulation as a percentage of GDP among the world's major economies (2010 → 2015). *Source* BIS Committee on Payments and Market Infrastructures

If such a goal were to be realized, the improvement in efficiency achieved for Japanese society as a whole would be immeasurable. This is particularly true in light of Japan's prospective population decline, which will make it increasingly difficult to find the necessary supermarket or convenience store staff to account for and manage cash, to guard it, transport it, and so on.

Japan can implement cashlessness at a moment's notice if it wants to, because the necessary systems already exist, having been established through the evolutionary stages of its payment methods. Credit cards, prepaid transportation cards, as well as debit cards for instant settlement are all issued and used in Japan today.

However, there are people who do not want to use credit cards because debt is incurred or because of the dangers of overspending. Different generations of Japanese users are most comfortable with different modes of payment, and many in Japan are of the view that accommodating all these different preferences is an important element of customer service.

For instance, bank cards and credit cards with magnetic strips are still used in Japan. Such magnetic-strip-based cards represent a major risk for society, as they have enabled major fake credit card scams. However, a large number of banks are of the view that allowing customers to continue using the cards they have been issued is an essential element of good service that responds to customer needs and increases customer trust.

The credit card business operates based on commissions amounting to more than 3–4% of sales. A great deal of work is involved in processing acquirer-side (member-store) and issuer-side (user) information related to international credit card networks such as Visa and Mastercard, timing the activation of such information accurately, and performing customer management. Many business establishments are unable to afford the fees involved.

By contrast, the cost burden on those making or receiving payments is close to zero in the case of services such as Alipay and WeChat Pay, because the processing is done over the Internet. Of course, Internet-based payment services such as LINE-pay and Mercari also exist in Japan, but they are not widely used.

As society becomes increasingly digitized, cash payments will eventually be replaced by payments using cards and smartphones. Rather than reflecting meticulous and far-sighted planning by the government or the central bank, this transition should be seen as a natural evolution of an economic mechanism playing a key role in the functioning of Japanese society as a whole.

## References

Back A (2002) Hashcash-a denial of service counter-measure. http://www.hashcash.org/papers/hashcash.pdf

Bayer D, Haber S, Stornetta WS (1993) Improving the efficiency and reliability of digital time-stamping

Benedetti H, Kostovetsky L (2018) Digital Tulips? returns to investors in initial coin offerings

Chaum D (1982) Blind signatures for untraceable payments. Advances in Cryptology Proceedings of Crypto. 82

Haber S, Stornetta WS (1991) How to time-stamp a digital document. J Cryptol 3(2):99–111

Haber S, Stornetta WS (1997) Secure names for bit-strings. In: Proceedings of the 4th ACM conference

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Okamoto T, Ohta K (1989) Divertible zero-knowledge interactive proofs and commutative random self-reducibility. Advances in Cryptology—EUROCRYPT'89, LNCS 434, pp 134–149. Springer-Verlag