

## WILL DIGITAL CURRENCIES REPLACE CASH? – DIGITAL CURRENCY, PRIVACY, AND SURVEILLANCE

Fabian Teichmann & Marie-Christin Falker

### AUTHORS

*Fabian M. Teichmann is an attorney-at-law and public notary in Switzerland. After earning an undergraduate degree in economics and finance (Bocconi University, Italy), he then earned graduate degrees in management (Harvard University, USA), accounting and finance, and law (University of St. Gallen, Switzerland). He also holds a PhD in law (University of Zurich, Switzerland), a doctoral degree in economics and social sciences (Kassel University, Germany), and an LL.M. (King's College, UK). Teichmann teaches courses on compliance, corruption, money laundering, and terrorism financing at various universities. He is the author of several books and over 100 scholarly articles.*

*Marie-Christin Falker is a research associate at Teichmann International (Schweiz) AG. She possesses an undergraduate degree in English and American Culture and Business Studies, focusing particularly on international management and marketing (Kassel University, Germany). She also studied at the University of Maryland, College Park (USA) as an undergraduate.*

### ABSTRACT

*In some nations, including Sweden and South Korea, cash payments are becoming increasingly uncommon. Other nations, such as Germany, continue to predominantly prefer cash. At the same time, digital currency is on the rise, and the announced launch of Facebook's stablecoin Libra, in particular, has caused a debate around digital money. In response, a number of central banks have begun to consider launching their own versions of digital currency. This article analyzes characteristics of both cash and digital currency and illustrates advantages as well as disadvantages of digital money and a cashless society. In particular, privacy concerns regarding digital cash are addressed. In addition, compliance risks are highlighted, and it is deliberated whether the introduction of digital cash could lead to a decrease in crime related to cash and cryptocurrencies.*

## TABLE OF CONTENTS

I.	INTRODUCTION	53
II.	CHARACTERISTICS OF CASH	54
III.	CHARACTERISTICS OF DIGITAL CURRENCY	55
IV.	LEGAL FRAMEWORK	58
	A. Data Protection	58
	1. China	58
	2. United States	58
	3. European Union	59
	4. Venezuela	59
	B. Cryptocurrencies	60
V.	LIBRA	60
VI.	CENTRAL BANK-ISSUED DIGITAL CURRENCY	62
	A. China	62
	B. United States	64
	C. European Union	65
	D. Venezuela	65
VII.	TOWARD A CASHLESS SOCIETY?	66
	A. Benefits of a Cashless Society	68
	B. Risks of a Cashless Society	68
	C. Responses	70
VIII.	DISCUSSION	70
IX.	CONCLUSION	72

## I. INTRODUCTION

The race for a central bank-issued digital currency has begun. Research conducted by cryptocurrency and blockchain research and analysis group The Block analyzed 60+ central banks and found that 18 of these banks publicly acknowledged they were developing a digital currency. These include the central banks of China, Singapore, Iran, UAE, and Europe. Four countries, namely, Tunisia, Senegal, Venezuela, and Uruguay, have already launched their versions, whereas the others have launched pilots or are still in development<sup>1</sup>. In particular, the announced launch of Facebook's Libra cryptocurrency is currently motivating central banks to come up with digital equivalents of their governmental currencies<sup>2</sup>. China seems to be particularly eager to replace cash with a digital currency<sup>3</sup>.

At the same time, the public is becoming increasingly aware of government surveillance techniques and the resulting lack of privacy. Nations such as China are suspected of taking government surveillance to extremes. In China, technologies such as facial recognition are being used to monitor citizens in nearly every aspect of their lives, including crossing the street (which could result in a jaywalking fine) and purchasing a sim-card for a mobile phone (new purchases require users to scan their face). In the context of this extensive governmental surveillance, which is mainly performed using new technology, China's announcement of the intention to introduce a digital currency has caused a debate on whether the Chinese government could attempt to use the currency to monitor its citizens. Because of the possibility of such behavior by governments, many citizens in China and elsewhere are likely to be opposed to the introduction of central bank-issued digital currencies. After all, recent changes brought about by digitalization, which include data brokers' selling of personal data to advertisers and the Cambridge Analytica scandal, where the company used personal data of up to 87 million Facebook users to facilitate Donald Trump's political campaign<sup>4</sup>, are causing privacy to become an increasingly valuable good. Kenneth Rogoff, former International Monetary Fund chief economist, admits in his book *The Curse of Cash*, "We need cash for privacy"<sup>5</sup>.

---

<sup>1</sup> S. Zheng, *At Least 18 Central Banks are Developing Sovereign Digital Currencies*, THE BLOCK (Dec. 26, 2019, 1:45 PM EST), [https://www.theblockcrypto.com/linked/51526/at-least-18-central-banks-are-developing-sovereign-digital-currencies?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=2019-12-26](https://www.theblockcrypto.com/linked/51526/at-least-18-central-banks-are-developing-sovereign-digital-currencies?utm_source=newsletter&utm_medium=email&utm_campaign=2019-12-26).

<sup>2</sup> M. Orcutt, *An Elegy For Cash: The Technology We Might Never Replace*, MIT TECHNOLOGY REVIEW (Jan. 3, 2020), [https://www.technologyreview.com/s/614998/an-elegy-for-cash-the-technology-we-might-never-replace/?utm\\_source=newsletters&utm\\_medium=email&utm\\_campaign=+the\\_download.unpaid.engagement](https://www.technologyreview.com/s/614998/an-elegy-for-cash-the-technology-we-might-never-replace/?utm_source=newsletters&utm_medium=email&utm_campaign=+the_download.unpaid.engagement).

<sup>3</sup> R. Zhong, *China's Cryptocurrency Plan Has a Powerful Partner: Big Brother*, THE NEW YORK TIMES (Oct. 18, 2019), <https://www.nytimes.com/2019/10/18/technology/china-cryptocurrency-facebook-libra.html>.

<sup>4</sup> Tagesanzeiger, *Facebook wegen Cambridge Analytica angeklagt* (Dec. 19, 2018), <https://www.tagesanzeiger.ch/ausland/amerika/facebook-wegen-cambridge-analytica-angeklagt/story/31385518>.

<sup>5</sup> Rogoff quoted in J. Pethokoukis, *The Problem with Cash: A Q&A with Economist Kenneth Rogoff*, AMERICAN ENTERPRISE INSTITUTE (Nov. 10, 2016), <https://www.aei.org/economics/the-problem-with-cash-a-qa-with-economist-kenneth-rogoff/>.

## II. CHARACTERISTICS OF CASH

The term “cash” refers to money in the forms of coins and bills. These are bearer instruments, which means that whoever holds them is assumed to be their owner. Cash transactions are peer-to-peer; there is no third party, such as an intermediary, involved and ownership can be transferred simply by handing over the cash<sup>6</sup>. There is not necessarily even a record of the transaction. Therefore, cash is considered to be highly anonymous. If records are not made, transactions using cash cannot easily be reconstructed. Further, contrary to digital payments, cash provides no data that could be used by companies to build advertising profiles or credit ratings. Similarly, cash does not facilitate governmental tracking of spending and individuals<sup>7</sup>. Moreover, hardly any trust is required in cash transactions: as long as one can verify its legitimacy, there is no danger of losing the money, as would be the case, for instance, if one accepted a check from an insolvent bank<sup>8</sup>.

Further, cash is permissionless, which means it does not require authorization from an institution in order to be used in a transaction. In contrast, people who do not have good credit, a government ID, steady income, or a permanent address will have difficulty opening a bank account. Gender discrimination could also be an issue: some countries do not allow women to open bank accounts<sup>9</sup>. With cash, every person can participate in the system without first being granted permission<sup>10</sup>. The permissionlessness of cash also makes it resistant to censorship, which means it can be used for illegal or culturally taboo activities<sup>11</sup>. As a result, payment by cash is a preferred *modus operandi* for a wide variety of criminals, including drug dealers, arms dealers, and many others.<sup>12</sup>

Because cash is used in the majority of transactions related to organized crime, money laundering (as a necessary consequence of such use) has become a significant threat to national economies and is a global problem<sup>13</sup>. Its effects are felt on a microeconomic scale in the private sector, within which money launderers use front companies to mix legitimate and illegitimate income. In some cases, front companies even sell products at prices below manufacturing cost, which gives them an advantage over legitimate businesses<sup>14</sup>.

---

<sup>6</sup> J. Brito, *The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society*, COIN CENTER (Feb., 2019), <https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf>.

<sup>7</sup> Orcutt, *supra* note 2.

<sup>8</sup> Brito, *supra* note 6.

<sup>9</sup> M. Coker, *How Guardianship Laws Still Control Saudi Women*, THE NEW YORK TIMES (June 22, 2018), <https://www.nytimes.com/2018/06/22/world/middleeast/saudi-women-guardianship.html>.

<sup>10</sup> Brito, *supra* note 6.

<sup>11</sup> Brito, *supra* note 6.

<sup>12</sup> F. TEICHMANN, *UMGEHUNGSMÖGLICHKEITEN DER GELDWÄSCHEREIPRÄVENTIONSMASSNAHMEN* [in German] 3 (Schulthess) (2016).

<sup>13</sup> J. Harvey, *An evaluation of money laundering policies*, 8 J MON L CONT 339 (2005).

<sup>14</sup> This could be the case with real estate, see e.g., F. Teichmann, *supra* note 12 at 155.

This can lead to the crowding out of private sector businesses by criminal organizations. Ultimately, these organizations' management principles do not concur with traditional free market principles, which leads to negative microeconomic and macroeconomic effects<sup>15</sup>. Money laundering laws have been widely established to facilitate the conviction of criminals, particularly those involved in the drug trade. However, for a variety of reasons, money laundering continues to pose a threat to the public<sup>16</sup>.

Money launderers frequently operate within networks of cooperation with other criminals. Therefore, their laundering methods are extremely difficult to substantiate<sup>17</sup>. When working with banks, money launderers utilize front people in order to remain anonymous. These front people pose as the beneficial owners of front companies and bank accounts<sup>18</sup>. Some jurisdictions, such as Dubai, are more cash-intensive than others and so tend to be preferred by money launderers<sup>19</sup>. In addition, the increasing density of compliance and know-your-customer (KYC) regulations in the financial sector has caused many money launderers to relocate their activities to less regulated sectors<sup>20</sup>. These include, among many others, the cryptocurrencies sector<sup>21</sup>. Bitcoin and other cryptocurrencies attempt to mimic the characteristics of cash; however, they are difficult to use and processing a transaction can be a slow process. Additionally, their values often fluctuate<sup>22</sup>. As a result, cash continues to be the most feasible option for individuals who either have no access to a bank account or wish to keep their transactions private.

### III. CHARACTERISTICS OF DIGITAL CURRENCY

“Digital Currency” is a blanket term that includes all forms of electronic money. Thus, virtual currencies and cryptocurrencies are (overlapping) types of digital currency. Digital currencies can be regulated or unregulated but are always intangible. Digital currencies that are spent using electronic wallets or networks are often called digital money. There are no intermediaries involved, which means transactions are fast and transaction fees are

---

<sup>15</sup> J. McDowell, *The Consequences of Money Laundering and Financial Crime*, HOMELAND SECURITY DIGITAL LIBRARY (May, 2001), <https://www.hsdl.org/?view&did=3549>.

<sup>16</sup> F.C. Razzano, *American Money Laundering Statutes: The Case for a Worldwide System of Banking Compliance Programs*, 3 J INT L & PRAC 277, (1994).

<sup>17</sup> F. Teichmann & M.C. Falker, *Money Laundering – Currency Exchange*, J FIN REG COMP (forthcoming).

<sup>18</sup> F. Teichmann & M.C. Falker, *Money Laundering Through Banks in Dubai*, J FIN REGULATION COMP (forthcoming).

<sup>19</sup> F. Teichmann & M.C. Falker, *Money Laundering – The Gold Method*, J MON L CONT (forthcoming).

<sup>20</sup> Teichmann, *supra* note 12 at 27.

<sup>21</sup> F. Teichmann & M.C. Falker, *Money Laundering Through Cryptocurrencies, in: Artificial Intelligence: Anthropogenic Nature vs. Social Origin* (B.S. Sergi & E.G. Popkova eds, Springer, forthcoming).

<sup>22</sup> Orcutt, *supra* note 2.

low<sup>23</sup>. Virtual currencies are a subset of digital currencies that are characterized as usually controlled by their creators and “accepted among the members of a specific virtual community”<sup>24</sup>. Virtual currencies represent a monetary value that is issued, managed, and controlled by private issuers and are used for peer-to-peer transactions. They can be represented by tokens and are not necessarily backed by legal tender. Owing to their lack of regulation, the prices of virtual currencies are rather volatile. Cryptocurrencies such as ethereum or Bitcoin are considered virtual currencies<sup>25</sup>.

Cryptocurrencies are made secure by encryption algorithms and cryptographic techniques. For this reason, they are difficult to counterfeit. They often operate in systems that are blockchain-based and decentralized. These characteristics make the role of a trusted third party such as a central bank redundant. Instead, users transfer funds peer-to-peer with the use of private and public keys<sup>26</sup>. Bitcoin is the most well-known cryptocurrency. Cryptocurrencies share some characteristics with cash; in particular, they are highly anonymous. However, unlike cash, they are not completely anonymous, because details of every transaction (including users’ public keys, the time, and the date) are recorded irrevocably on the blockchain. Like cash, cryptocurrencies have a reputation for being used for criminal activity, primarily owing to the fact that they are not controlled by a central entity and governments have very little jurisdiction over them. According to Jill Carlson, co-founder of Open Money Initiative, cryptocurrencies were not designed to solve mainstream issues such as speed of transactions and stable values; they were created to resist censorship. As a result, cryptocurrencies have been documented as being used to purchase drugs online, buy US dollars in Argentina, pay sex workers, make international monetary transfers, support dissidents in Hong Kong, and move money out of Venezuela<sup>27</sup>. Carlson furthermore argues: “It is time to face this potentially uncomfortable reality: cryptocurrency is most useful when breaking laws and social constructs”<sup>28</sup>. In conclusion, cryptocurrencies facilitate financial activities that would otherwise be prohibited or suppressed.

Like cash, privacy-preserving decentralized technologies have given organizations and people the opportunity to escape censorship. Although the actors in these domains act in accordance with certain regulations, government policies and social norms can hardly be enforced in these contexts. Therefore, stopping censored activities becomes much more

---

<sup>23</sup> Y.B. Perez, *The Differences Between Cryptocurrencies, Virtual, and Digital Currencies*, THE NEXT WEB (Feb. 19, 2019, 9:14 UTC), <https://thenextweb.com/hardfork/2019/02/19/the-differences-between-cryptocurrencies-virtual-and-digital-currencies/>.

<sup>24</sup> Id.

<sup>25</sup> Id.

<sup>26</sup> Id.

<sup>27</sup> J. Carlson, *Cryptocurrency is Most Useful for Breaking Laws and Social Constructs*, COINDESK (Dec. 10, 2019), <https://www.coindesk.com/cryptocurrency-is-most-useful-for-breaking-laws-and-social-constructs>.

<sup>28</sup> Id.

difficult<sup>29</sup>. Data collected by blockchain analytics company Chainalysis supports this claim: in 2019, \$US2.8 billion in Bitcoin were transferred through crypto exchanges by criminals<sup>30</sup>. According to Chainalysis, crypto exchanges have always been “popular off-ramp for illicit cryptocurrencies”<sup>31</sup>. In addition, the share of illicit cryptocurrency has steadily grown since the beginning of 2019. Within the scope of their analysis, especially in relation to crypto exchanges, Binance and Huobi came under scrutiny. Although both exchanges have KYC protocols in place, the requirements are less stringent for over-the-counter (OTC) brokers. As a result, some OTC desks seem to have specialized in providing money-laundering services to criminals<sup>32</sup>.

The small amount of quantitative data available also suggests that the use of cryptocurrency is more predominant in countries with financial restrictions<sup>33</sup>. Data on the cryptocurrency trade in Venezuela has shown that, between the petro (the central bank-issued digital currency) and decentralized cryptocurrency, citizens seem to prefer the latter. Experts also claim that in Palestine, where many financial services such as PayPal are not available, the awareness of Bitcoin and ethereum has increased since 2018. This is not only true for terrorism financiers, but also for irreproachable residents and businesspeople<sup>34</sup>. Thus, it can be assumed that in regions where the public distrusts the government or local currency, where hyperinflation is prevalent, or where there are simply no other alternatives available, residents frequently turn to cryptocurrency. Laws are not always considered acceptable by either citizens of the jurisdiction or by outsiders. Therefore, experts argue that it cannot be concluded that privacy-enhancing technologies are used primarily for illegal or socially unacceptable activities<sup>35</sup>. In particular, in societies and nations where government surveillance seems ubiquitous, citizens use both cash and cryptocurrencies or other privacy-enhancing technologies to protect their privacy.

---

<sup>29</sup> Id.

<sup>30</sup> Chainalysis Team, *Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019*, CHAINALYSIS INC (Jan. 15, 2020), <https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019>.

<sup>31</sup> Id.

<sup>32</sup> Id.

<sup>33</sup> M. Ahlberg, *Nuanced Analysis of Local Bitcoins Data Suggests Bitcoin is Working as Satoshi Intended*, MEDIUM (Feb. 8, 2019), <https://medium.com/@mattahlberg/nuanced-analysis-of-localbitcoins-data-suggests-bitcoin-is-working-as-satoshi-intended-d8bo4d3ac7b2>.

<sup>34</sup> L. Cuen, *In Palestine, Civilians Are Using Bitcoin More Than Hamas*, COINDESK (Aug. 22, 2019), <https://www.coindesk.com/palestinian-civilians-are-using-bitcoin-more-than-terrorists>.

<sup>35</sup> Carlson, *supra* note 27.

## IV. LEGAL FRAMEWORK

### A. Data Protection

Data protection is perhaps the most pressing concern of citizens when it comes to digital currency or cash. In the following sections, we will present the legal framework for various jurisdictions of interest here.

#### 1. China

China has no single comprehensive data protection laws. Instead, there are rules relating to data security and personal data protection that are part of a complex framework. These rules are incorporated across various regulations and laws. The General Principles of Civil Law and the Tort Liability Law have been used to interpret data protection as a right to privacy or right to reputation. These interpretations are, however, not explicit<sup>36</sup>. On June 1, 2017, the PRC Cybersecurity Law, which addresses data privacy protection and cybersecurity, came into effect. Under this law, the data protection obligations include, among others, guidelines on personal information and data security. Current data protection rules are based mainly on the Decision on Strengthening Online Information Protection, effective from December 28, 2012; the National Standard of Information Security Technology, a guideline that came into effect on February 1, 2013; and the National Standard of Information Security Technology, a Personal Information Security Specification that became effective on May 1, 2018<sup>37</sup>. Depending on the industry, provisions contained in other laws and regulations might also apply (e.g., for financial institutions, e-commerce businesses, and certain healthcare providers). Furthermore, provincial-level laws may need to be considered<sup>38</sup>.

#### 2. United States

In the United States, data security laws are largely sector-specific or medium-specific, and include laws and regulations that apply to financial institutions, personal health information, telecommunications firms, credit card information telemarketing, direct marketing, and children's information<sup>39</sup>. Among its 50 states and territories, the United States has an abundance of privacy and data security measures that consist of (but are not limited to) safeguarding data, privacy policies, disposal of data, and data breach notification. Further, the US Federal Trade Commission (FTC) has jurisdiction over many commercial entities under its authority in order to safeguard consumers from unfair trade or deceptive

---

<sup>36</sup> DLA Piper, *Data Protection Laws of the World: China*, DLA PIPER (Last modified Dec. 31, 2019), <https://www.dlapiperdataprotection.com/index.html?c=CN&c2=DE&go-button=GO&t=law>.

<sup>37</sup> Id.

<sup>38</sup> Id.

<sup>39</sup> DLA Piper, *Data Protection Laws of the World: USA*, DLA PIPER (Last modified Jan. 27, 2020), <https://www.dlapiperdataprotection.com/index.html?t=law&c=US>.

practices. The FTC issues regulations that enforce privacy laws and investigate firms for failing to implement reasonable data protection measures, failing to abide by applicable industry self-regulatory principles, and more. In addition, many state attorneys general have similar authority over unfair business practices<sup>40</sup>.

### 3. European Union

In the European Union, the General Data Protection Regulation<sup>41</sup> (GDPR) entered into force in 2016. It became directly applicable in all member states on May 25, 2018 without requiring implementation through national law. An EU directive applies consistently across all member states and is directly applicable. Over 50 areas are covered by the GDPR; however, some are “permitted to legislate differently in their own domestic data protection laws”<sup>42</sup>. Any organization that processes personal data of data subjects in the European Union is obligated to abide by GDPR, even if it is not established within the EU. This concerns the offering of goods and services<sup>43</sup> and the monitoring of the organization’s behavior<sup>44</sup>. In comparison with other regions, the EU regulates data privacy heavily.

### 4. Venezuela

Venezuela does not have general legislation that regulates data protection; instead, there are general principles established in the Constitution and developed by Supreme Court decisions<sup>45</sup>. The framework for personal data protection is based on principles established in the Constitution. The purpose of these principles is to safeguard the intimacy, private life, self-image, honor, confidentiality, and reputation of citizens. In addition, the Constitution establishes the right to access information and data: based on Article 28 of the Constitution, every person has the right to access information and data concerning themselves that is stored in public or private registries. They also have the right to be informed of how this information is used, and the right to rectify, update, and destroy incorrect information that unlawfully affects their rights. Information on individuals and their purchases may be collected, maintained, and arranged into profiles; this also includes their activities. These profiles must be intended for the benefit of the collecting entity or third parties, provided all constitutional rights are respected. Collectors of such information must also guarantee a number of principles, including the principle of free will, principle

---

<sup>40</sup> Id.

<sup>41</sup> General Data Protection Regulation, 2016/679 (EU).

<sup>42</sup> DLA Piper, *Data Protection Laws of the World: Germany*, DLA PIPER (Last modified Jan. 14, 2020), <https://www.dlapiperdataprotection.com/index.html?c=CN&c2=DE&go-button=GO&t=law>.

<sup>43</sup> General Data Protection Regulation, 2016/679, Art. 3 (2) (a) (EU).

<sup>44</sup> General Data Protection Regulation, 2016/679, Art. 3 (2) (b) (EU).

<sup>45</sup> DLA Piper, *Data Protection Laws of the World: Venezuela*, DLA PIPER (Last modified Jan. 28, 2019), <https://www.dlapiperdataprotection.com/index.html?t=law&c=VE>.

of confidentiality, and principle of responsibility. In addition, there is a law against cyber-crime and the Banking Institutions Law, which regulates data protection in the sector<sup>46</sup>.

## B. Cryptocurrencies

Because digital currency raises so many privacy concerns in relation to the wider public, it seems likely that, in the absence of physical cash, citizens will resort to cryptocurrency in order to escape constant surveillance. Cryptocurrencies lack regulation in most jurisdictions. Although Liechtenstein's blockchain act has entered into force on January 1, 2020, and EU countries have been obligated to follow the 5th Anti-Money Laundering Directive (AMLD<sub>5</sub>) since January 10, 2020, regulators of cryptocurrency face a number of obstacles. Apart from the AMLD<sub>5</sub>, there are no common rules for the regulation of virtual currencies. Only "a tiny fraction of Bitcoins or other digital coins"<sup>47</sup> are exchanged for euros. Therefore, most decision makers have not paid cryptocurrencies much attention, thus far. Now that Libra has been announced, the EU in particular seems to be increasingly concerned with cryptocurrencies. However, EU regulators have not agreed on how to treat virtual currencies, yet. In particular, cryptocurrencies could be defined as either payment services, securities, or currencies. However, the option to treat them as currencies is ruled out by most<sup>48</sup>. Furthermore, it has not been agreed upon whether existing rules of governing financial instruments could apply to virtual currencies. Therefore, users of virtual currencies largely operate in a legal gray area in the EU. Other jurisdictions frequently (such as Saudi Arabia, Vietnam, and Bolivia) either ban cryptocurrency entirely, or restrict them (such as China, Morocco, and Ecuador)<sup>49</sup>. However, data collected by the crypto trading platform LocalBitcoins show that in China, India, and Saudi Arabia, cryptocurrencies such as Bitcoin continue to be traded despite bans and restrictions<sup>50</sup>.

## V. LIBRA

As previously mentioned, the introduction of Facebook's stablecoin Libra has motivated multiple governments and central banks to research options for their own digital currency. At the beginning of 2019, experts were still skeptical about state-backed digital currencies. The general manager of the Bank of International Settlements, Augustín Carstens, showed little enthusiasm: "Research and experimentation have so far failed to put

---

<sup>46</sup> Id.

<sup>47</sup> Guarascio, *UPDATE 1-EU Finance Commissioner Pledges to Regulate Digital Currencies* (Oct. 8. 2019), <https://www.cnbc.com/2019/10/08/reuters-america-update-1-eu-finance-commissioner-pledges-to-regulate-digital-currencies.html>.

<sup>48</sup> Id.

<sup>49</sup> Cryptonews, *Countries Where Bitcoin is Banned or Legal in 2020* (n.d.), <https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm>.

<sup>50</sup> Coin.Dance, *LocalBitcoins Volume Charts*, COIN DANCE (Updated Weekly), <https://coin.dance/volume/localbitcoins>.

forward a convincing case [...] Central banks are not seeing today the value of venturing into uncharted territory”<sup>51</sup>. In July, Carstens corrected his March statement and said that central bank digital currencies may be closer to being implemented than initially expected. This change of heart occurred after Facebook revealed its plans for Libra in June<sup>52</sup>.

The Libra association is located in Geneva, Switzerland, and consists of renowned firms such as Spotify, Lyft, Vodafone, and Coinbase. Unlike other cryptocurrencies, Libra is a stablecoin, which means that its value is backed by a reserve of assets. In addition, Libra is centralized, which means that, unlike Bitcoin and other cryptocurrencies, Libra nodes (computers that verify transactions and validate the network) are controlled exclusively by the Libra Association. The fact that Libra is controlled by private companies is being criticized harshly by international experts, especially in Europe, for instance by Yves Mersch, head of the European Central Bank<sup>53</sup>. In line with Germany, France and the United States have also uttered their concerns. Further, Facebook’s multiple data protection breaches and scandals have elicited skepticism regarding Libra, from not only a large proportion of Facebook users but also central bank officials. As a result from the extensive international criticism, some members of the Libra Association, including PayPal, Visa, and Mastercard, have withdrawn their support for the stablecoin.<sup>54</sup>

Apart from data protection concerns, regulators are worried that Libra will interfere with monetary policy, which is a core government function<sup>55</sup>. German Finance Minister Olaf Scholz argued that the issuance of a currency is a core element of state sovereignty that must not fall into the hands of private companies<sup>56</sup>. Facebook is not the only company attempting to venture into finance; corporations such as Google and Apple are also entering the field: Apple has created a credit card, and Google provides an electronic wallet and has announced plans for checking accounts for users of their wallet. The wallet in one’s phone can be used to make, for instance, payments in stores<sup>57</sup>. Thus, tech firms are offering services that have traditionally been associated with banks. However, when

---

<sup>51</sup> A. Carstens, *The Future of Money and Payments*, BANK FOR INTERNATIONAL SETTLEMENTS (MAR. 22, 2019), <https://www.bis.org/speeches/sp190322.pdf>.

<sup>52</sup> M. Orcutt, *Facebook’s Digital Currency May Force Central Banks to Create Their Own*, MIT TECHNOLOGY REVIEW (July 1, 2019), <https://www.technologyreview.com/f/613909/facebooks-digital-currency-may-force-central-banks-to-create-their-own/>.

<sup>53</sup> Y. Mersch, *Money and Private Currencies: Reflections on Libra*, *European Central Bank* (Sept. 2, 2019), <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190902~aedded9219.en.html>.

<sup>54</sup> R. Brandom, *Facebook’s Libra Association crumbling as Visa, Mastercard, Stripe, and others exit*, THE VERGE (Oct. 11, 2019), <https://www.theverge.com/2019/10/11/20910330/mastercard-stripe-ebay-facebook-libra-association-withdrawal-cryptocurrency>.

<sup>55</sup> Colitt & Marsh, *Facebook’s Obstacles in Europe Mount as Germany Opposes Libra* (Sep. 18, 2019), <https://www.bloomberg.com/news/articles/2019-09-18/germany-broadens-european-front-opposing-facebook-s-libra-plan>.

<sup>56</sup> Id.

<sup>57</sup> Wall Street Journal, *Why big tech is getting into finance*, YOUTUBE (Jan. 14, 2020), <https://www.youtube.com/watch?v=oKFpUZT7go4>.

Google or Apple process payments for their clients, they gather vast amounts of data, including the date and time of the payment, the vendor, and the amount transferred. This information is valuable for advertisers. The associated companies all began by offering one service or product, and then gradually widened their range and experienced rapid growth at the same time. In response, several United States' regulatory bodies have initiated antitrust investigations into Google, Facebook, Apple, and other companies. Further, the public seems to be distrustful, especially of Facebook<sup>58</sup>.

The main question regarding Libra is whether private companies should be trusted with one's money. Private stablecoin providers have the potential to unseat banks. Banks, however, are subject to strict compliance requirements and consumer protection rules. Tech giants, on the other hand, could use their networks to monetize information, according to economists Adrian and Mancini-Griffoli of the IMF<sup>59</sup>. They also argue that stablecoin users risk losing their assets, and that stablecoins could undermine financial stability. Central banks, such as the ones in Singapore and China have, in response to Libra, begun to work on their own equivalents, which will be discussed in the following sections.

## VI. CENTRAL BANK-ISSUED DIGITAL CURRENCY

### A. China

The initiative for a Chinese digital currency was commenced in 2014. However, the announcement of the planned launch of Libra seems to have accelerated the process. According to Mu Chanchun, the head of the PBOC digital currency research institute, Libra could be accepted by everyone and therefore widely used as a payment tool. His fear is that it will “develop into a global, super-sovereign currency”<sup>60</sup>. In response, he argued in an online lecture, China would need to protect its monetary sovereignty<sup>61</sup>. According to Chinese officials, their aim is for the Chinese currency, the renminbi, to be used more in international finance and trade. During a speech he gave in July 2019, former central bank governor Zhou claimed that “the dominance of the dollar had eroded the economies of nations with ‘weak’ currencies”, and warned that Libra could lead to similar outcomes<sup>62</sup>.

Under the initiative for a Chinese digital currency, the plan is to distribute the digital money first to commercial banks. Thereafter, users and businesses will be able to register

---

<sup>58</sup> Id.

<sup>59</sup> T. Adrian & T. Mancini-Griffoli, *Digital Currencies: The Rise of Stablecoins*, INTERNATIONAL MONETARY FUND (Sept. 19, 2019), <https://blogs.imf.org/2019/09/19/digital-currencies-the-rise-of-stablecoins/>.

<sup>60</sup> Chanchun quoted in Zhong, *supra* note 3.

<sup>61</sup> Zhong, *supra* note 3.

<sup>62</sup> Zhong, *supra* note 3.

wallets with these commercial banks, according to the PBOC<sup>63</sup>. The pilot digital currency will reportedly be tested in the cities Shenzhen and Suzhou. For this purpose, the PBOC has partnered with several state-owned commercial banks and telecoms<sup>64</sup>. In the Chinese province Anhui, the government has also announced that it will “adopt blockchain technology across governmental service centers”<sup>65</sup>. This includes all levels of government in Anhui, which will be using blockchain, artificial intelligence, and other new technologies to offer governmental services at all times. The stated intention is to “digitize Anhui’s governance infrastructure and streamline the collection and sharing of government data and resources”. In December 2019, the Chinese central government had published a guideline for the Yangtze River Delta Economy Region, which Anhui is part of, to prioritize the development of artificial intelligence, blockchain, cloud computing, and other emerging technologies<sup>66</sup>.

### Concerns

According to economist Gary Liu, the Chinese digital currency will be “highly controlled, manageable, and decided by the central government”<sup>67</sup>, and thus diverge from the original concept of cybersecurity. According to a senior bank official, the Chinese digital currency will not seek to “gain full control of information belonging to the general public”; instead, the PBOC claims the goal is to balance the authorities’ need for information and privacy concerns<sup>68</sup>. China has suggested that it will not provide marketers with spending information; authorities, however, will have access<sup>69</sup>.

Users are already required to authenticate their names and identities with the banks and electronic payment companies that will distribute the digital currency. Further, the central bank will be able to view transaction data<sup>70</sup>. Experts claim that in contrast to Bitcoin

---

<sup>63</sup> C. Wan, Report: China’s Central Bank to Test Digital Currency in Two Cities, Partnering with State-Backed Commercial Banks and Telecom Giants, THE BLOCK (Dec. 9, 2019, 12:35 AM EST), <https://www.theblockcrypto.com/post/49659/report-chinas-central-bank-to-test-digital-currency-in-two-cities-partnering-with-state-backed-commercial-banks-and-telecom-giants>.

<sup>64</sup> Y. Katri, *China’s Digital Currency “Progressing Smoothly,” Says Central Bank*, THE BLOCK (Jan. 6, 2020), [https://www.theblockcrypto.com/linked/52092/chinas-digital-currency-progressing-smoothly-says-central-bank?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=2020-01-12](https://www.theblockcrypto.com/linked/52092/chinas-digital-currency-progressing-smoothly-says-central-bank?utm_source=newsletter&utm_medium=email&utm_campaign=2020-01-12).

<sup>65</sup> Y. Cheng, *Chinese Local Government Eyes Adoption of Blockchain for Service Centers*, THE BLOCK (Jan. 8, 2020), [https://www.theblockcrypto.com/linked/52200/chinese-local-government-eyes-adoption-of-blockchain-for-service-centers?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=2020-01-08](https://www.theblockcrypto.com/linked/52200/chinese-local-government-eyes-adoption-of-blockchain-for-service-centers?utm_source=newsletter&utm_medium=email&utm_campaign=2020-01-08).

<sup>66</sup> Id.

<sup>67</sup> Liu quoted in Zhong, *supra* note 3.

<sup>68</sup> A. John & K. Coghill, *China’s Digital Currency Not Seeking “Full Control” of Individuals’ Details: Central Bank Official*, REUTERS (Nov. 12, 2019), <https://www.reuters.com/article/us-china-markets-digital-currency/chinas-digital-currency-not-seeking-full-control-of-individuals-details-central-bank-official-idUSKBN1XMoH2>.

<sup>69</sup> Zhong, *supra* note 3.

<sup>70</sup> Zhong, *supra* note 3.

and Libra, the currency seems to have been designed to provide Beijing “with unprecedented oversight over money flows, giving Chinese authorities a degree of control over their economy that most central banks do not have”<sup>71</sup>. During a conference in Singapore, Mu Changchun assured the public that users of the digital currency will continue to have privacy in their transactions. At the same time, he claimed that the PBOC will find a balance between “controllable anonymity” and anti-money laundering (AML), counter terrorist financing (CFT), tax issues, online gambling, and any other electronic criminal activities<sup>72</sup>.

Changchun’s statements are questionable: “controlled anonymity” seems a paradox in itself. After all, the government or law enforcement agencies will need to sort through all user information in order to be able to identify AML or CFT breaches. Flex Yang, the founder of a Hong Kong-based financial provider of cryptocurrencies, Babel Finance, argues that “currencies should be neutral”; without anonymity, he argues, the money cannot be considered a currency, “it can only be a payment vehicle”<sup>73</sup>. However, China could agree not to save user data, as long as the person in question has not broken the law. Critics of the new digital currency also argue that China’s persecuted minorities will “face even harsher conditions under a fully integrated financial system controlled by the government”<sup>74</sup>. In an interview with *Coindesk*, an anonymous Chinese bitcoiner stated that a totalitarian state could use blockchain to track every person and their actions, and to enforce strict currency controls. They go on to talk about how their parents (Christian missionaries) have been subject to constant surveillance by the Chinese government. They claim that, once, their WePay and AliPay accounts were frozen. If they had not had cash, they would have been left with no money<sup>75</sup>. These statements raise concerns that the complete digitalization of money would leave political opponents and minorities vulnerable to the repercussions of censorship.

## B. United States

In the United States, lawmakers have asked the Federal Reserve to consider the creation of a digital dollar. On September 30, 2019, Rep. French Hill and Rep. Bill Foster sent a letter to Federal Reserve Chairman Jerome Powell in which they expressed their concerns regarding risks to the US dollar if another nation or private company were to create a widely employed cryptocurrency. In particular, they emphasized their concern that the primacy of the US dollar could be in jeopardy in case of a wide adoption of digital fiat

---

<sup>71</sup> John & Coghill, *supra* note 68.

<sup>72</sup> John & Coghill, *supra* note 68.

<sup>73</sup> Yang quoted in Zhong, *supra* note 3.

<sup>74</sup> L. Cuen, *Bitcoin Dissident Sees Dark Warnings in China’s Blockchain Push*, COINDESK (Oct. 31, 2019, 10:20 AM UTC), <https://www.coindesk.com/bitcoin-dissident-sees-dark-warnings-in-chinas-blockchain-push>.

<sup>75</sup> *Id.*

currencies<sup>76</sup>. Their letter also specifically mentioned Libra. On October 24, 2019, the Federal Reserve stated that it is planning to respond to the letter. Former Federal Deposit Insurance Corporation Chair Sheila Bair also suggested that the Federal Reserve should explore the option of creating a digital currency in order to avoid being disrupted by the private sector or other nations<sup>77</sup>.

### C. European Union

In September 2019, Germany and France responded to the announced launch of Libra by claiming that the stablecoin “posed risks to the financial sector that could block its authorization in Europe”<sup>78</sup>. Both countries support the development of an alternative public cryptocurrency. French finance minister Bruno Le Maire and German finance minister Olaf Scholz released a joint statement at a meeting of euro zone finance ministers in Helsinki, in which they argued that virtual currencies pose risks to financial stability, consumers, and monetary sovereignty<sup>79</sup>. According to European Central Bank (ECB) board member Benoît Cœuré, Libra constituted a “wake-up call”<sup>80</sup>. Accordingly, Libra has motivated new efforts to launch an ECB-backed project, TIPS, in the euro zone. Banks, however, have responded to this project with apprehension. The ECB seems to also be planning a central bank-issued digital currency. According to Cœuré, consumers would be able to use electronic cash, which would be directly deposited at the ECB. Thus, there would be no need for bank accounts, clearing counterparties, or financial intermediaries. As a consequence, transaction costs would decrease. In light of these ambitions, opposition from banks is likely. At the same time, the technical feasibility “remains to be seen”<sup>81</sup>. In November 2019, Cœuré told a conference in Brussels that “a central bank digital currency could ensure that citizens remain able to use central bank money, even if cash is eventually no longer used”<sup>82</sup>.

### D. Venezuela

In 2018, Venezuela, which is plagued by hyperinflation, launched its cryptocurrency called petro. Critics claim that it represents an attempt to collect dollars and open up foreign business channels. The price of petro is based on the oil price; one petro is supposed to

---

<sup>76</sup> F. Hill & B. Foster, *Letter to Jerome H. Powell*, COINDESK (Sept. 30, 2019), <https://www.coindesk.com/wp-content/uploads/2019/10/Foster-Hill-US-Crypto.pdf>.

<sup>77</sup> N. De, *US Lawmakers Ask Fed to Consider Developing a “National Digital Currency”*, COINDESK (Oct. 2, 2019, 23:08 UCT), <https://www.coindesk.com/us-congressmen-ask-fed-to-consider-developing-national-digital-currency>.

<sup>78</sup> Guarascio, *supra* note 47.

<sup>79</sup> Guarascio, *supra* note 47.

<sup>80</sup> Cœuré quoted in Guarascio, *supra* note 47.

<sup>81</sup> Guarascio, *supra* note 47.

<sup>82</sup> B. Cœuré, *Towards the Retail Payments of Tomorrow: A European Strategy*, EUROPEAN CENTRAL BANK (Nov. 26, 2019), <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191126~5230672c11.en.html>.

cost as much as one oil barrel, which is about \$US60<sup>83</sup>. Petro is also backed by Venezuela's oil reserves<sup>84</sup>. Although petro is claimed to be a cryptocurrency, it is supervised and controlled by the federal authority for the supervision and control of cryptocurrencies, which conflicts with the fact that cryptocurrencies are generally decentralized and transparent<sup>85</sup>. It had been expected that Venezuelans would not have much interest in buying petro, because of the high rates of poverty or lack of access to US dollars. Therefore, it has been argued that petro is mainly a vehicle that allows corrupt officials, politicians, and companies to transfer their assets out of the country. It is also argued that there is no real incentive for investors to buy petro, as three dozen regime members have been sanctioned by the US<sup>86</sup>. Other sources state that petro was launched to circumvent these sanctions and overcome liquidity shortages<sup>87</sup>.

Thus far, petro has been unsuccessful in winning over investors: the currency has, in fact, been banned by the United States. Risk-ranking bodies have also labeled it a "scam"<sup>88</sup>. Although petro has failed, other cryptocurrencies such as Bitcoin see an increase in their trade<sup>89</sup> (See e.g., Coin.Dance, 2020). Many Venezuelans keep physical dollar bills to retain their assets, which makes them vulnerable to burglary<sup>90</sup>. Therefore, Venezuelans have resorted to cryptocurrency. There is even a popular local trade, LocalBitcoins, that facilitates exchanges between Bitcoin and bolivars, the national currency<sup>91</sup>. In an effort to revive petro, the Venezuelan president, Nicolas Maduro, has decreed that all airlines flying from Caracas must purchase their fuel using petro and that the currency is to be used to pay for state document services such as passports<sup>92</sup>. When Maduro approved bonuses for public employees and pensioners in December 2019, these were also paid out in petros. However, the petros were quickly exchanged for bolivars, and then for other currencies. At the beginning of 2020, the government blocked the exchange of bolivars for petros<sup>93</sup>.

## VII. TOWARD A CASHLESS SOCIETY?

---

<sup>83</sup> A. Busch, *Venezuelas Kryptowährung Petro ist ein Verzweifelter Versuch an Ausländische Gelder zu Kommen* [in German], NEUE ZÜRCHER ZEITUNG AG (Feb. 21, 2018), <https://www.nzz.ch/wirtschaft/potemkinscher-petro-ld.1359430>.

<sup>84</sup> France24, *Maduro Bids to Revive Venezuela's 'Petro' Cryptocurrency*, FRANCE24 (Jan. 15, 2020), <https://www.france24.com/en/20200114-maduro-bids-to-revive-venezuela-s-petro-cryptocurrency>.

<sup>85</sup> Busch, *supra* note 83.

<sup>86</sup> Busch, *supra* note 83.

<sup>87</sup> France24, *supra* note 84.

<sup>88</sup> France24, *supra* note 84.

<sup>89</sup> For example, see Coin.Dance, *supra* note 50.

<sup>90</sup> Orcutt, *supra* note 2.

<sup>91</sup> Orcutt, *supra* note 2.

<sup>92</sup> France24, *supra* note 84.

<sup>93</sup> France24, *supra* note 84.

According to experts, digital money has the potential to replace cash altogether. Sweden is one example of an almost cashless society. According to the Swedish central bank, the number of payments made using cash is expected to drop to 0.5% by 2020<sup>94</sup>. Further, South Korea intends to phase out cash in 2020<sup>95</sup>. Even in the UK, where cash continues to be rather popular, bus fares can no longer be paid in cash<sup>96</sup>. Many citizens in comparatively cashless societies utilize mobile payment systems provided by banks and fintechs (e.g., Apple Pay or Chinese providers AliPay and WeChat Pay) or credit cards. Naturally, these companies have an interest in promoting a cashless society because they collect transaction fees from their customers<sup>97</sup>. Some financial service providers, including Visa, have launched advertisements and media campaigns to convince customers to give up cash for card payments<sup>98</sup>. Central banks have an interest in a cashless society, as well, as they would be able to “grow the monetary policy tools at their disposal” and “impose negative interest rates across the whole economy”<sup>99</sup>. Further, economist Joseph Stiglitz argued that cash should be abolished in order to hinder financial corruption and tax evasion<sup>100</sup>.

Online, the use of cash has never been possible. Because of the fact that commerce is increasingly relocating to the internet, “the proportion of intermediated payments grows concomitantly”<sup>101</sup>. As online retail is becoming more popular, intermediaries will inevitably have better access to information about buying habits<sup>102</sup>. However, as shown by Bech et al.,<sup>103</sup> on a global scale, the demand for cash has not decreased. A report by the Bank for International Settlements (BIS) found that cash demand, which is measured by proxy through cash in circulation, has increased among the majority of the 46 national economies in its sample. In addition, out of 24 nations investigated, only Sweden and Russia were shown to exhibit signs of substituting cash payments with card payments. The remaining 22 countries showed an increase in both cash demand and online payments with

---

<sup>94</sup> J. Henley, *Sweden Leads the Race to Become Cashless Society*, THE GUARDIAN (June 4, 2016, 16:00 BST), <https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe>.

<sup>95</sup> P. Jenkins, *“We Don’t Take Cash”: Is This the Future of Money?*, FINANCIAL TIMES (May 9, 2018), <https://www.ft.com/content/9fc35dda-5316-11e8-b24e-cad6aa67e23e>.

<sup>96</sup> Transport for London, *Cash Free Buses*, TRANSPORT FOR LONDON (no date), <https://tfl.gov.uk/modes/buses/cash-free-buses>.

<sup>97</sup> B. Scott, *The War on Cash*, NESTA (Aug. 19, 2016), <https://thelongandshort.org/society/war-on-cash>.

<sup>98</sup> P. Jenkins, *supra* note 95.

<sup>99</sup> Brito, *supra* note 6.

<sup>100</sup> R. Chainey, *The US Should Get Rid of Cash and Move to a Digital Currency, Says Nobel Laureate Economist*, WORLD ECONOMIC FORUM (Jan. 17, 2017), <https://www.weforum.org/agenda/2017/01/the-us-should-get-rid-of-cash-and-become-a-digital-economy-says-this-nobel-laureate-economist/>.

<sup>101</sup> Brito, *supra* note 6.

<sup>102</sup> Brito, *supra* note 6.

<sup>103</sup> M.L. Bech et al., *Payments are A-changin’ but Cash Still Rules*, BANK FOR INTERNATIONAL SETTLEMENTS (Mar. 11, 2018), [https://www.bis.org/publ/qtrpdf/r\\_qu1803g.htm](https://www.bis.org/publ/qtrpdf/r_qu1803g.htm).

the use of cards, which suggests that the unique features of cash are valued<sup>104</sup>.

#### A. Benefits of a Cashless Society

In *The Curse of Cash*, economist Kenneth Rogoff argues that cash is “making us poorer and less safe”. In line with Bech et al., Rogoff shows that even though cash is being used less frequently, the amount of cash in circulation is actually growing. According to him, this cash is being used for tax evasion, terrorism, corruption, human trafficking, the drug trade, and a “massive global underground economy”. This could also affect monetary policy, according to Rogoff. After the 2008 global financial crisis, central banks were not able “to stimulate growth and inflation by cutting interest rates significantly below zero for fear that it would drive investors to abandon treasury bills and stockpile cash”<sup>105</sup>.

Compliance officers around the world will likely agree with Rogoff in that cash represents an immense risk factor for all sorts of crime. From a compliance perspective, cash poses tremendous threats to public safety as it is highly anonymous and non-transparent, which makes it well suited to crime and money laundering or terrorism financing. Corruption, particularly bribery, is another concern relating to cash. With money laundering, cash would be generated during a predicate offense. A drug dealer in Zurich, for instance, will accept cash from their clients, with no paper trail or digital record of the transaction. The same is true for bribery and terrorism financing.

Although financial institutions and banks are subject to strict compliance measures, cash-intensive businesses are frequently excluded from these measures. Therefore, money launderers and terrorism financiers are increasingly relocating to less-regulated sectors. Our 2016 quantitative study showed that, out of the 153 responding compliance experts, 74.5% agreed that money launderers are relocating to less-regulated sectors<sup>106</sup>. Therefore, it can be assumed that, in a cashless society, it would be much more difficult for criminals to continue their illicit activities without being detected. After all, every digital transaction would be traceable, which in itself could serve as a deterrent for criminals. In addition, they would need to find new methods to be able to conduct untraceable transactions.

#### B. Risks of a Cashless Society

According to Scott A. Shay<sup>107</sup>, chairman of Signature Bank, the US government frequently seizes money from its citizens before conducting an investigation, even if government staff members have no proof of wrongdoing. When a person’s or company’s assets are seized, the defendant frequently has no other option than to settle. In one instance,

---

<sup>104</sup> Id.

<sup>105</sup> K. ROGOFF, *THE CURSE OF CASH 1* (Princeton University Press) (2016).

<sup>106</sup> Teichmann, *supra* note 12, at 85.

<sup>107</sup> S.A. Shay, *Cashless Society: A Huge Threat To Our Freedom*, CNBC LLC (Dec. 12, 2013), <https://www.cnbc.com/2013/12/12/cashless-society-a-huge-threat-to-our-freedomcommentary.html>.

which was argued before the Supreme Court, the government had seized all the money of a small family-owned grocery store because its cash deposits were below the \$US10,000 threshold, which triggered a report to the government. As a result, the defendants were deprived of money they needed to defend themselves. In such cases, defendants often are under pressure to settle or plead guilty<sup>108</sup> owing to the fact that they have no access to their financial assets. However, they can use cash to finance their daily life, so that they do not go hungry. In a cashless society, the freezing of a family's financial assets could accordingly have fatal consequences.

Algorithms that instantaneously review and evaluate financial transactions are available, and in use by credit and debit card firms. The technology is typically used to issue fraud alerts following unusual consumer purchases. In 2010, Mastercard and Visa banned online-betting payments in response to pressure from the US government. Thus, gambling sites struggled to continue operating, regardless of their location or legality. At present, these restrictive mechanisms can be circumvented through the use of cash. In a cashless society, however, the government would have “unprecedented access to information and power over citizens”, according to Shay<sup>109</sup>.

In addition, it has become easier for governments to gather information. JP Morgan is one of the largest US banks; its size is that of 3,000 smaller banks combined, and the top four US banks have control over circa 60% of US banking deposits. Thus, there are fewer access points for the government. There are compliance hurdles in place for banks that wish to deal with certain customers, which make business relations with them expensive. In response, some banks, including JP Morgan, refrain from dealing with these clients altogether. In this manner, the government can prevent certain individuals or companies from accessing the financial system<sup>110</sup>. Therefore, it could be argued that a cashless society could lead to extensive governmental control over human behavior.

Shay calls this phenomenon, which he describes as economic singularity, “econgularity”. He defines econgularity as the moment in time when technological surveillance, big data manipulation, and a cashless economy converge<sup>111</sup>. In light of the data presented in section 4.0, this scenario could potentially be approaching faster than expected. With econgularity, Shay argues that it would be possible for government staff members to order the freezing of funds or decline withdrawals or payments for individuals who are suspected of misconduct or those are political opposers. Before the person is able to access their funds again, their case might need to be reviewed, which would take time. In the meantime, the individual “might starve to death”. In addition, anyone suspected of helping the person could be cut off from accessing their assets, as well<sup>112</sup>. Naturally, a cashless society will not

---

<sup>108</sup> Id.

<sup>109</sup> Id.

<sup>110</sup> Id.

<sup>111</sup> Id.

<sup>112</sup> Id.

take this form in all jurisdictions; however, some governments could take the opportunity to exert greater control over their citizens. According to crypto expert Jerry Brito, the death of cash will inevitably cause “the birth of perfect financial control”<sup>113</sup>.

### C. Responses

In the United States, citizens have begun to argue that cashless businesses violate their civil rights. Cities such as San Francisco, Washington D.C., and Philadelphia have therefore ruled these businesses out. In New York City, legislation that prevents retail establishments from refusing to accept cash payments was introduced in February 2019<sup>114</sup>. In August, the law was rescinded, but reintroduced in December 2019 (The New York City Council, n.d.). As of January 2020, the New York Council has voted to ban cashless stores and restaurants<sup>115</sup>, which means cashless businesses could face fines of up to \$US500 per violation. In addition to the fear of governmental surveillance and censoring of payments, some opponents have also argued that cashless businesses discriminate against low-income people, who are often undocumented immigrants or people of color<sup>116</sup>. In New York City, 25% of underbanked citizens and 12% of unbanked citizens are people of color, whereas only 3% of white New Yorkers are unbanked<sup>117</sup>. This raised the question of whether cashless businesses are a manifestation of racial discrimination. This could also be problematic for every other demographic that does not have access to a bank account (e.g., homeless or unemployed persons). Businesses that operate cash-free argue that a ban of cash payments increases efficiency, saves money and time by cutting out the need for armored vehicles for transportation, and protects their employees against robbery<sup>118</sup>.

## VIII. DISCUSSION

Ultimately, an abandonment of cash could facilitate more effective crime prevention and prosecution. However, we suggest that replacing cash with a digital form is rather unnecessary: the development of digital cash requires an abundance of resources, including time, money, human resources, and materials. In addition, once established, the technology will need to be maintained, which will require further resources. If the intention is to create digital currency with the same characteristics and anonymity as physical cash, there

---

<sup>113</sup> Brito, *supra* note 5.

<sup>114</sup> R. Bellan, *As More Cities Ban Cashless Businesses, New York Wants to Follow* (Mar 6, 2019), <https://www.citylab.com/equity/2019/03/cashless-cash-free-ban-bill-new-york-retail-discrimination/584203/>.

<sup>115</sup> C. Jones, *New York Says Don't Ditch Your Cash: City is Latest to Ban Cashless Restaurants, Stores* (Jan. 24, 2020), <https://eu.usatoday.com/story/money/2020/01/23/new-york-city-bans-cashless-businesses/4551974002/>.

<sup>116</sup> Bellan, *supra* note 114.

<sup>117</sup> Federal Deposit Insurance Corporation, *FIC National Survey of Unbanked and Underbanked Households – Executive Summary*, FEDERAL DEPOSIT INSURANCE CORPORATION (Oct., 2018), <https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf>.

<sup>118</sup> Bellan, *supra* note 114.

is no use in replacing physical cash in the first place. Cryptocurrencies, on the other hand, are useful primarily for criminals, as they do not require the transacting parties to meet at one location. Thus, they facilitate discreet payments without personal contact. When it comes to blockchain, the technology shows great potential in the area of smart contracts. These could enable legal transactions; in particular, trading with rights and securities could be simplified.

Although at present a cashless society is not yet in sight, an increasing number of payments are conducted via credit or debit card. Statistics relating to credit card and cash spending are indicators of consumer spending habits, which could also be used to analyze the broader economy as a whole<sup>119</sup>. A 2017 study conducted by global payments company TSYS, which investigated consumer payment, has shown that, currently, debit cards are the most popular payment method. In particular, out of 1,222 consumers, 54% chose debit cards as their preferred form of payment, while 26% selected credit cards, and 14% stated that they preferred cash. It was also shown that consumers are becoming increasingly interested in mobile wallets<sup>120</sup>. In 2016, global analytics and advice firm Gallup found that Americans are using increasingly less cash – in 2011, 36% of analyzed Americans reported that they made almost all purchases using cash; in comparison, this number had shrunk to 24% in 2016<sup>121</sup>. These findings are consistent with a multitude of other surveys. There are, however, nations that diverge from this trend: Germany is the most prominent example of a country where residents continue to prefer cash over credit or debit card payments, mainly for privacy reasons<sup>122</sup>.

In light of these findings, financial service providers will see themselves presented with increasingly high compliance requirements. With regard to data protection compliance, it is of immense importance that customer data is handled responsibly. This includes accurate encryption and theft-prevention measures. At the same time, customers must be made aware of how their data is used and who has access to it. Herein, it should be ensured that customers have the option to opt out of providing their data for certain purposes such as advertisement. A study by researchers from MIT, UCL, and Aarhus University has recently shown that out of 10,000 websites, only 11.8% meet minimal requirements of the GDPR. In particular, many websites make it difficult for users to opt out of tracking. Pop-up windows for cookie consent are often designed so that rejecting tracking is much more difficult than consenting to it – in most cases, there is an option to “accept all” but none to “reject all”. In addition, 32.5% of the surveyed websites bypass EU law via implicit consent, which assumes that failure to respond to a pop-up window or the visiting of the

---

<sup>119</sup> M. Shepherd, *19 Cash vs Credit Card Spending Statistics*, FUNDERA INC (Dec. 31, 2019), <https://www.fundera.com/resources/cash-vs-credit-card-spending-statistics>.

<sup>120</sup> TSYS, *Consumer Payment Study*, 7, 38, TOTAL SYSTEM SERVICES INC (Mar., 2018), [https://www.tsys.com/Assets/TSYS/downloads/rs\\_2017-us-consumer-payment-study.pdf](https://www.tsys.com/Assets/TSYS/downloads/rs_2017-us-consumer-payment-study.pdf).

<sup>121</sup> A. Swift & S. Ander, *Americans Using Cash Less Compared With Five Years Ago*, GALLUP (July 12, 2016), <https://news.gallup.com/poll/193649/americans-using-cash-less-compared-five-years-ago.aspx>.

<sup>122</sup> M. Campbell, *Germany is Still Obsessed with Cash*, BLOOMBERG (Feb. 6, 2018), <https://www.bloomberg.com/news/features/2018-02-06/germany-is-still-obsessed-with-cash>.

site alone implies consent<sup>123</sup>. When handling sensitive customer data, practices such as the assumption of implicit consent or potential data breaches could lead to significant reputational damages for the institution if thematized by the media.

In the absence of predefined standards, however, financial institutions will also face a number of unresolved questions. In order to ensure legal security and prevent compliance scandals, these questions must be addressed urgently, so that institutions do not operate in dangerous legal gray areas. On January 1, 2020, Liechtenstein's new blockchain act (German: Token- und VT-Dienstleister Gesetz, TVTG) entered into force. Liechtenstein is one of the first jurisdictions to regulate blockchain and its potential uses, which includes financial services. With the introduction of the TVTG, the Due Diligence Act (German: Sorgfaltspflichtgesetz, SPG) has been amended so that due diligence requirements include service providers for virtual currencies<sup>124</sup>. Due diligence measures aim to prevent money laundering, terrorism financing, and organized crime.

## IX. CONCLUSION

Although cryptocurrencies, led by Bitcoin, have been around for over ten years now, up until recently most central banks and governments seemed to perceive no significant threat to traditional money from digital currency. This sentiment has changed drastically since the planned launch of Libra was announced by Facebook. Overall, reactions to Libra have been overwhelmingly negative: multiple central bank officials and politicians have expressed concerns regarding implications for privacy and monetary policy. In particular, the experts have argued that money should not be issued by a private company, but by a sovereign entity, i.e., a central bank. Central banks are also concerned that Libra could become a widely used payment method that is preferred over governmental currency. In response, multiple central banks have announced that they will begin developing their own digital currency, or have accelerated their already existing research efforts. China will likely be the first nation to issue a digital currency. However, China's ambitions are viewed critically by the public: the country is known to use new technologies for the surveillance of its citizens; as a result, opponents fear that the digital currency will be used to surveil and control citizens.

In particular, the PBOC seems to intend to replace physical cash with digital cash. Digital cash, however, can never be as private as physical cash; accordingly, the public does not seem convinced that their data will not be used for purposes other than processing payments. In addition, digital cash is not censorship-resistant, which means that certain groups of people (e.g., minorities or homeless persons) could be prevented from accessing the monetary system. These concerns apply to cashless societies in general. However, a

---

<sup>123</sup> M. Nouwens et al., *Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence*, CORNELL UNIVERSITY (Jan. 8, 2020), <https://arxiv.org/abs/2001.02479>.

<sup>124</sup> Sorgfaltspflichtgesetz (Dec. 11, 2008)[in German], Art. 3 Sec. 1 (f).

cashless society would come with the advantage that organized crime would be significantly hindered. As a consequence, money laundering would also become a less pressing issue. However, in this scenario, it must be ensured that there is an appropriate legal framework for financial service providers to operate within, so that data protection and compliance breaches can be prevented. Ultimately, only time will tell whether cash will, at some point, be replaced by digital currency. Totalitarian governments could use digital currency to surveil the public, marginalize political opponents, or even prevent citizens from accessing the financial system altogether. Therefore, the creation of an ethical, internationally valid framework is crucial. The establishment of such a framework would naturally be highly challenging. Therefore, the international community should ensure that countries that seek to violate human rights through their use of digital currency are penalized with hard sanctions, and that their citizens are protected from governmental control.