UCL

## UCL Centre for Blockchain Technologies

# Discussion Paper Series

Q2 2021

CBT

# Foreword

With this issue, we encourage the debate on Central Bank Digital Currency (CBDC).

CBDC will arrive soon. This is simply an unavoidable consequence of technology and will either follow innovation needs from central bankers or citizen demand for easier payments tools.

The introduction of CBDC has huge implications that go well beyond a change of support in circulating cash from paper/metal to crypto codes. Indeed, it opens a vast domain of possibilities that central banks and governments are both keen to explore and scared by the consequences.

In the present environment, central banks are struggling to find a hedge on which to operate. Remarkably, the cornerstones of the central banking mantra, namely the relation between interest rates and inflation, and the effects of quantitative easing on the currency value, have been proved unsubstantiated by facts. There is therefore a strong need to rethink the means of central bank interventions. CBDC provides a possibility for a direct link between central bank emission and citizen spending ability. This is a new monetary policy instrument that could be a game-changer. Furthermore, to some governments, the perspective of having an ultimate means of state control on citizen's behavior is too appealing to be ignored. For the same reason, for many citizens, the perspective of being obliged to use government-traceable means of payments is unacceptable. Tolls to make digital currencies untraceable are readily available; however, the fear that this will be a huge gift to criminals is well-founded. Technology is neutral, it both creates the problem and offers the solution. Conversely, the application of technology is not neutral and the way we design CBDC now will impact our future for many years to come.

Enjoy your reading

**Tomaso Aste**
UCL CBT Scientific Director & Chairman of the Editorial Board

August 2021

*Acknowledgement*

*The editorial board wishes to thank Juan Ignacio Ibañez for his high-quality work and strong perseverance, without which this discussion paper series would have never been possible.*

# Discussion Paper Series Contents

*The following are published in this edition:*

#1

**Central Bank Digital Currencies and the GDPR: Reconciling blockchains with the right to be forgotten**

*Pierre Ostercamp*

#2

**Will Central Bank Digital Currencies (CBDC's) Eliminate the Need for Cryptocurrencies?**

*Kelly Ann Coulter*

#3

**Regulating Financial Innovation: DLT Potential and Promise for Financial Market Infrastructures (FMIs)**

*Pavel Kulikov*

# Editorial Board

# Discussion Paper #1

## Central Bank Digital Currencies and the GDPR: Reconciling blockchains with the right to be forgotten

*Pierre Ostercamp*

Postgraduate student on the MSc Regulation Programme

London School of Economics

**Abstract**

Using a blockchain to issue a central bank digital currency (CBDC) may yield benefits such as immutability (tamper resistance), enhanced security of data storage, and efficiency gains. However, the immutability of blockchains conflicts with the principles and rights of the EU's General Data Protection Regulation (GDPR); in particular, the right to erasure ('right to be forgotten'). For a blockchain-based CBDC not to breach the right to be forgotten, one of two conditions must be fulfilled: all personal data recorded on the blockchain must either be a) stored or manipulated in a way that brings it outside of the GDPR's scope; or b) erased or sufficiently obfuscated when a data subject exercises their right to be forgotten.

# Central Bank Digital Currencies and the GDPR:

# Reconciling blockchains with the right to be forgotten

*Pierre Ostercamp*[*]

**Abstract**

*Using a blockchain to issue a central bank digital currency (CBDC) may yield benefits such as immutability (tamper resistance), enhanced security of data storage, and efficiency gains. However, the immutability of blockchains conflicts with the principles and rights of the EU's General Data Protection Regulation (GDPR); in particular, the right to erasure ('right to be forgotten'). For a blockchain-based CBDC not to breach the right to be forgotten, one of two conditions must be fulfilled: all personal data recorded on the blockchain must either be a) stored or manipulated in a way that brings it outside of the GDPR's scope; or b) erased or sufficiently obfuscated when a data subject exercises their right to be forgotten.*

**Contents**

**I. Introduction** ..... **2**

**II. CBDCs and the GDPR** ..... **3**

**III. Pseudonymisation and Anonymisation** ..... **6**

1. Anonymisation Threshold ..... 6

2. Encryption ..... 8

3. Hashing ..... 10

**IV. Erasing Personal Data** ..... **11**

1. Defining Erasure ..... 11

2. Encryption ..... 12

3. Off-Chain Personal Data ..... 13

4. Chameleon Hashes ..... 13

[*] Pierre Ostercamp, postgraduate student on the MSc Regulation programme at the London School of Economics, and policy analyst at XReg Consulting, a regulatory consultancy specialising in cryptoassets.

## I. Introduction

Following over a decade of technological innovation in payment systems, one of the latest research areas is the development of a central bank digital currency ('CBDC'). In contrast to traditional electronic fiat currency constituting a liability of an intermediary, a CBDC is 'monetary value stored electronically that represents a liability of the central bank and can be used to make payments'.[1] There are numerous purported benefits of a CBDC, including increased efficiency of payments, financial inclusion, and the removal of trust in intermediaries to honour the value of deposits.

However, the legal and economic risks are daunting. Transitioning from traditional to digital fiat currency could result in disintermediation of retail banks, bank runs during losses of confidence, financial instability, and increased money laundering. Nonetheless, central bank interest in CBDCs is evident: the Bank for International Settlements found that, of the central banks that they surveyed in 2019, 80% were working on CBDCs.[2]

As CBDC interest and literature has expanded since 2019, research has centred around their design, benefits, risks, and monetary impact, leaving scope for further research into the legal implications of CBDCs.[3] One of the most significant legal challenges in designing a CBDC is ensuring adequate protection of personal data, especially in the EU under the comprehensive General Data Protection Regulation ('GDPR').

While distributed ledger technology ('DLT') is a popular design choice for CBDC projects, it renders GDPR compliance even more difficult since DLT essentially comprises a digital database shared between multiple entities.[4] The most prevalent form of DLT is a blockchain, which is a chain of blocks of data linked to each other using cryptography, the practice of secure communication.[5] These links are typically made using a cryptographic hash function, which is a mathematical algorithm that transforms any given input into a fixed-length output (the 'hash').[6]

---

[1] Walter Engert and Ben S. C. Fung, 'Central Bank Digital Currency: Motivations and Implications' (2017) 1-2 <https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf> accessed 20 June 2021.
[2] BIS, 'Impending arrival – a sequel to the survey on central bank digital currency' (2020) 3 <https://www.bis.org/publ/bppdf/bispap107.pdf> accessed 20 June 2021.
[3] Frederic Tronnier et al, 'Towards Central Bank Digital Currency – A Systematic Literature Review' (Pacis 2020) 12 <https://aisel.aisnet.org/pacis2020/131> accessed 20 June 2021.
[4] Koshik Raj, *Foundations of Blockchain* (Packt Publishing 2019) 15.
[5] ibid 23.
[6] Douglas Stinson, *Cryptography: Theory and Practice* (CRC Press 2018) 9.

New blocks added to the chain are linked to the hash value of the previous block, so any amendment or erasure of a block resulting in a change in its hash value will break the chain.[7] This fundamental characteristic means the blockchain is virtually immutable, ie tamper-resistant.[8] However, the immutable and append-only design of blockchains conflicts with several of the GDPR's principles[9] and rights[10]; in particular, the right to erasure ('right to be forgotten') and the right to rectification, as well as the principles of data minimisation and storage limitation.

This paper focuses on compliance with the right to be forgotten (the 'Right') in the context of a retail CBDC using a permissioned blockchain in which a centralised authority controls access to the network.[11] It will be shown that for a blockchain-based CBDC not to breach the Right, one of two conditions must be fulfilled: all personal data must either be a) stored or manipulated in a way that brings it outside of the GDPR's scope; or b) erased or sufficiently obfuscated when a data subject exercises their right to be forgotten.

First, Section II will outline the GDPR and the Right, as well as CBDCs and their design. Section III will then proceed to discuss the scope of the GDPR and methods of bringing personal data outside of its scope. Next, Section IV will examine the notion of erasure under the GDPR and methods of achieving erasure on a blockchain. Finally, in Section V, a conclusion will be drawn on the solutions to designing a CBDC blockchain that enables compliance with the Right, and the action needed to support such innovation.

## II. CBDCs and the GDPR

The GDPR was introduced to strengthen and harmonise the data protection framework across the EU, superseding the 1995 Data Protection Directive[12] ('DPD'). While the GDPR simply 'applies to the processing of personal data'[13], broadly construed notions of personal data and data processing in both the GDPR and EU case law have established a broad scope of application. Personal data is defined in the GDPR as 'any information relating to an identified

[7] cf Raj (n 4) 19-20.
[8] ibid 13.
[9] GDPR art 5(1)(a)-(f).
[10] GDPR arts 15-22.
[11] cf Raj (n 4) 16.
[12] Directive 95/46/EC.
[13] GDPR art 2(1). Exceptions to the GDPR's application are listed under art 2(2).

or identifiable natural person ('data subject')'[14], where identifiability should be assessed with regard to 'all the means reasonably likely to be used' to identify the data subject.[15]

As such, users' public keys (used for encrypting or verifying transactions) and transaction data typically recorded on blockchains could be considered personal data.[16] Since any operation performed on personal data constitutes processing under the GDPR[17], blockchain operations involving public keys or transaction data may fall within the scope of the GDPR. Where personal data processing is within the scope of the GDPR, parties that determine the processing ('data controllers'[18]) must comply with the Right when it is exercised.

The right to be forgotten is the right that a data subject has to 'obtain from the controller the erasure of personal data concerning [them] without undue delay'.[19] The Right arises in six situations listed under GDPR Article 17(1)(a)-17(1)(f), though not all of these would necessarily apply to data processing for a blockchain-based CBDC. For example, personal data processing which is necessary to maintain the CBDC blockchain could be deemed outside of the scope of Articles 17(1)(a) or 17(1)(c) respectively, on the basis of either a necessary purpose or overriding legitimate grounds for the processing. Even where consent is withdrawn, Article 17(1)(b) provides that processing can continue on the basis of other legal grounds.[20]

Additionally, Article 17(3)(b) may apply and deny the Right where processing is in line with a legal obligation, the public interest, or the 'exercise of official authority vested in the controller'. Therefore, processing to maintain the CBDC blockchain could be deemed necessary and thus permissible insofar as it serves the public interest. Equally, it is conceivable that a data controller in this context, such as the European Central Bank (ECB), would have the official authority to conduct such processing.

Regarding sensitive personal data as defined by Article 9(1), the Right may be refused if any of the exceptions under Article 9(2) apply and the processing is otherwise lawful, though erasure could still be required based on an objection to the processing under Article 17(1)(c).[21] In any case, erasure of sensitive data may be refused under Article 9(2)(g) if continued

---

[14] GDPR art 4(1).
[15] GDPR recital 26.
[16] Michèle Finck, *Blockchain Regulation And Governance In Europe* (Cambridge University Press 2019) 93.
[17] GDPR art 4(2).
[18] GDPR art 4(7).
[19] GDPR art 17(1).
[20] Legal grounds for personal data processing are listed under GDPR art 6(1).
[21] Jure Globocnik, 'The Right to Be Forgotten is Taking Shape' (2020) 69(4) GRUR International 380, 384.

processing is 'necessary for reasons of substantial public interest'.[22] Conversely, legal requirements may oblige erasure under Articles 17(1)(d) or 17(1)(e), which implies that future legislative amendments could, in turn, require amendments to the methods of personal data processing and the CBDC blockchain itself. Whether amendments could be implemented, and compliance with the Right achieved when it is exercised, depends on the design of the CBDC.

The primary choices in designing a CBDC relate to a) technology (DLT or conventional technology); and b) availability (retail or wholesale).[23] This paper will focus on the context of a retail CBDC as this is the current focus of most central banks, including the ECB.[24] To inform their decision, the ECB has conducted detailed analyses into the prospect of issuing a CBDC[25], and engaged in public consultation on its possible design features as well as associated benefits and challenges.[26]

Proponents of a blockchain-based digital euro allude to various potential advantages of DLT, such as immutability, enhanced security of data storage, and efficiency gains.[27] Others, however, argue that DLT offers no significant advantages over conventional centralised systems and lacks in both performance and scalability.[28] Although project Stella (a CBDC research project conducted by the ECB and the Bank of Japan) found that a DLT-based CBDC offered sufficient performance to cater to the European and Japanese financial markets, legal issues remain, including the various tensions between DLT and the GDPR.[29]

---

[22] ibid.
[23] BIS, 'Quarterly Review' (2020) 87 <https://www.bis.org/publ/qtrpdf/r_qt2003.pdf> accessed 20 June 2021.
[24] cf BIS (n 2) 3; Yves Mersch, 'An ECB digital currency – a flight of fancy?' (2020) <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html> accessed 20 June 2021.
[25] ECB, 'Report on a digital euro' (2020) <https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf> accessed 20 June 2021.
[26] ECB, 'Questionnaire on a digital euro' (2020) <https://www.ecb.europa.eu/euro/shared/files/Questionnaire_on_a_digital_euro.pdf> accessed 20 June 2021.
[27] Jonas Gross et al, 'The Digital Euro and the Role of DLT for Central Bank Digital Currencies' (2020) 6-7 <https://www.researchgate.net/publication/341354711_The_Digital_Euro_and_the_Role_of_DLT_for_Central_Bank_Digital_Currencies> accessed 20 June 2021.
[28] cf BIS (n 23) 97.
[29] OMFIF and IBM, 'Central bank digital currencies' (2018) 26 <https://www.omfif.org/ibm/> accessed 20 June 2021.

## III. Pseudonymisation and Anonymisation

### 1. Anonymisation Threshold

The GDPR applies to the processing of personal data but not anonymous data, so it is essential to draw a clear line between the two. Approaches to this distinction can broadly be placed in two opposing categories: the risk-based approach, and the strict, virtually zero-risk approach. The risk-based approach to distinguishing between personal and anonymous data under the GDPR uses a subjective criterion to assess the identifiability of a data subject in light of the means 'reasonably likely to be used' as specified under Recital 26.

On the other hand, the strict approach uses an objective criterion and deems data to be personal data based on almost any risk of identification. However, the scope of the GDPR would be overly inclusive under this strict approach. In taking account of almost all risks, the strict approach runs in opposition to Recital 26, to the detriment of both legal certainty and potentially valuable data processing and innovation.

A similarly strict approach is seen in the definition of anonymisation proposed by the Article 29 Working Party (the 'Working Party'): 'processing personal data in order to irreversibly prevent identification'.[30] Since modern technology and availability of data make irreversible anonymisation exceedingly challenging[31], or even impossible according to some commentators[32], this definition of anonymisation is at best strict, and at worst fundamentally flawed.

Conversely, a flexible definition of personal data could allow pseudonymisation to be qualified as anonymisation insofar as it brings the difficulty of identification beyond the range of the means 'reasonably likely to be used', thus bringing the data outside of the scope of the GDPR. Although pseudonymisation cannot achieve anonymisation in the strict sense[33], there is legal precedent within EU case law supporting the use of a subjective criterion in assessing identifiability. Most notably, in *Breyer,* the CJEU's judgment that dynamic IP addresses

---

[30] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 3 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 20 June 2021; EPRS, 'Blockchain and the General Data Protection Regulation' (2019) 20 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 20 June 2021.

[31] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation' (2013) 31 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 20 June 2021.

[32] Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal From Non-Personal Data Under The GDPR' (2020) 10(1) International Data Privacy Law 11, 35.

[33] cf Article 29 Working Party (n 30).

constitute personal data hinged upon consideration of the 'means reasonably likely to be used'.[34]

Since the GDPR's Recital 26 is analogous to that of the DPD, the judgment in *Breyer* should remain authoritative under the GDPR despite having been made under the DPD.[35] Following the legal precedent of the *Breyer* judgment, pseudonymised personal data could be considered anonymous data under the GDPR and thus outside of the GDPR's scope.[36] Even if pseudonymisation is not qualified as anonymisation, GDPR Article 11(1) implies that pseudonymisation can result in the data controller escaping the obligation to comply with the Right unless the data subject provides supplementary information to enable their identification.[37]

If one does use the subjective criterion to assess identifiability, the essential considerations to determine whether data is within the scope of the GDPR are a) the interpretation of 'means reasonably likely to be used'; and b) the perspective from which identifiability should be assessed.[38] In *Breyer*, the CJEU made the significant judgment that means which are not 'reasonably likely to be used' include those 'prohibited by law' or 'practically impossible' in light of the disproportionate time, cost and effort required for identification.[39]

While it is self-evident that 'practically impossible' means are not 'reasonably likely to be used', the exclusion of any illegal means from consideration seems irrational: wherever there is significant value to be gained from identifying an individual, illegal means such as computer hacking could plausibly be used in pursuit of financial gain. Moreover, although there may not be sufficient incentives to identify the average person, frequent data breaches affecting large groups of people indicate that the collective value of these individuals' data may suffice to incentivise hackers to (illegally) identify individuals.

Regarding the perspective of assessment, the same data may constitute personal data from the perspective of one party but not another. The *Breyer* judgment supports a test of identifiability from the perspectives of both the data controller, predictably, and that of some

---

[34] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779 para 48.
[35] Miranda Mourby et al, 'Are 'Pseudonymised' Data Always Personal Data? Implications Of The GDPR For Administrative Data Research In The UK' (2018) 34(2) Computer Law & Security Review 222, 227.
[36] ibid.
[37] GDPR art 11(1).
[38] ICO, 'Overview of the General Data Protection Regulation (GDPR)' (2017) 4 <https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf> accessed 20 June 2021.
[39] *Breyer* para 46.

third parties, potentially, depending on whether it is reasonably likely that these parties would be involved with the data subject's identification.[40] In the context of a CBDC, whereas an issuer or intermediary may hold the information necessary to identify a data subject from their personal data, the same data could be considered anonymous in the hands of third parties without access to such information.[41]

### 2. Encryption

Encryption is a process through which information is transformed into an unintelligible format, where reversal of this process ('decryption') requires the use of a decryption key.[42] Without knowledge of the decryption key, one can only decrypt the data by testing every possible key (a 'brute-force attack') until the original, intelligible message is found.[43] Since encrypted personal data still preserves a link to the data subject, it could be treated as personal data under the GDPR.[44] In theory, however, strong encryption of personal data could meet the threshold for anonymity by ensuring that identification cannot be achieved through the means 'reasonably likely' to be used.

Recital 26 of the GDPR specifically includes consideration of the time and cost of identification, which could be made prohibitively high with state-of-the-art encryption. Where the number of potential decryption keys is sufficiently large, 'the adversary will not be able to test them all in any reasonable amount of time'.[45] Indeed, the Working Party asserts that where state-of-the-art encryption is used, identification of the original data subjects through decryption is impossible except for those with the decryption key.[46] This assertion implies that pseudonymisation through sufficiently strong encryption can render personal data anonymous from the perspective of anyone without access to the decryption key.

However, whether encryption can achieve anonymity under the GDPR is unconfirmed by courts and regulatory authorities. With a view to enhancing legal certainty, guidance should be issued by data protection authorities on the minimum standards for encryption to be

---

[40] *Breyer* para 49; Thomas Buocz et al, 'Bitcoin And The GDPR: Allocating Responsibility In Distributed Networks' (2019) 35 Computer Law & Security Review 182, 190.
[41] cf Mourby et al (n 35).
[42] cf Stinson (n 6) 1-2.
[43] ibid.
[44] Dean Armstrong et al, *Blockchain And Cryptocurrency: International Legal and Regulatory Challenges* (Bloomsbury Professional 2019) 123. Indeed, this is the stance of the Working Party.
[45] cf Stinson (n 6) 1-2. The current state-of-the-art standard for data encryption is the Data Encryption Standard.
[46] cf Article 29 Working Party (n 30) 20.

considered to achieve anonymity.[47] Further, data protection certifications could be issued under GDPR Article 42 to prove compliance with the GDPR.

Pervasive minimum standards, however, are unlikely to emerge since most data would require a unique contextual assessment of identifiability, including an evaluation of the differing motives for identifying data subjects.[48] For example, there may be stronger motives for identifying data subjects that are known to be high net-worth individuals in order to target them in a hack or robbery for financial gain.

Another impediment to broad minimum standards is that current standards of encryption may be superseded by technological innovation resulting in data being deemed as personal data once again. The relevant data would then have to be erased when a data subject exercises their Right, or better encrypted to meet the threshold for anonymity. While Recital 26 accounts for this by requiring consideration of technological developments, the scope of these considerations is unclear, notably whether new areas of research such as quantum computing should be considered.[49]

Research suggests that cryptographic algorithms such as AES, SHA-2, and SHA-3 could remain secure after the introduction of quantum computing.[50] However, most public-key cryptographic algorithms frequently used in blockchain-based payment systems would be rendered insecure by the advent of quantum computing.[51] In this situation, the brute-force attack necessary to identify an individual may return within the scope of the 'means reasonably likely to be used'. These data would then be deemed personal data under the GDPR, even if they had previously fallen outside the GDPR's scope.

In response to the threat of the quantum era, the National Institute of Standards and Technology ('NIST') is selecting for standardisation public-key cryptographic algorithms that would be resistant to quantum computing.[52] Equally, firms and governments should consider the extent to which this threat applies to their current operations, especially with regard to the protection of data.

---

[47] Jelena Madir, *FinTech: Law and Regulation* (Edward Elgar Publishing 2019) 247.
[48] cf Article 29 Working Party (n 33) 23.
[49] cf EPRS (n 30) 23.
[50] National Institute of Standards and Technology, 'Report on Post-Quantum Cryptography' (2016) 2-3 <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf> accessed 20 June 2021.
[51] ibid.
[52] National Institute of Standards and Technology, 'Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process' (2020) <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf> accessed 20 June 2021.

The Working Party made the significant recommendation that systems processing personal data should have the capacity to adapt to technological developments in order to remain compliant with data protection requirements.[53] In the context of permanent blockchains, any future technological developments could be possible, which arguably results in the conclusion that any pseudonymised data recorded on a permanent blockchain should be considered personal data.[54] A more pragmatic conclusion, however, is that ongoing compliance with the GDPR in line with advances in cryptography would require an adjustable blockchain design.

While many blockchains are not adjustable, such an architecture is feasible and indeed more straightforward in the case of a permissioned blockchain network, as the centralised authority has direct control over its design. Even in the absence of clear minimum standards for encryption, collaboration between the ECB and the Working Party's successor, the European Data Protection Board ('EDPB'), in the designing and updating of the CBDC blockchain could help to achieve continued GDPR compliance in line with both technological and legal developments.

### 3. Hashing

As secure hash functions are generally irreversible, the hash could be considered as anonymous data even if it was derived from an input of personal data, with pseudo-anonymous hashes recorded on distributed ledgers therefore being outside of the scope of the GDPR. One example of this is the DLT used by Quorum, which only appends hashes of personal data to the public ledger, with the original data kept on private ledgers.[55]

Despite the irreversibility of hash functions, the Working Party does not consider them to achieve anonymisation as the function's inputs could still be deduced, enabling identification of the data subject.[56] The primary security threat in this context is a brute-force attack in which all potential inputs are tested until the one corresponding to the relevant hash is found.[57] These attacks are more difficult the broader the range of potential inputs, though if some components

[53] cf EPRS (n 30) 24.
[54] ibid.
[55] ECB and BoJ, 'Balancing confidentiality and auditability in a distributed ledger environment' (2020) 9 <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf> accessed 20 June 2021.
[56] cf Article 29 Working Party (n 30) 20.
[57] cf Stinson (n 6) 144-5.

of the inputs such as individuals' names and addresses are known, or the range of inputs is otherwise predictable, brute-force attacks can be easier to perform.[58]

One way of impeding brute-force attacks is to add unique, random data (a 'salt') to the input before it is hashed, as this increases the range and decreases the predictability of potential inputs. Depending on the salt, the input, and the hashing algorithm, however, identification of the input and the related individual could still be achieved through means reasonably likely to be used.[59] By instead using a 'pepper', which is similar to a salt but is kept secret, identifiability of the data subject can be further reduced. Additionally, if the pepper is deleted from storage after hashing, the risk of identification is significantly decreased.

Where a secure hashing algorithm such as SHA-256 (used on the Bitcoin network) is used, the brute-force attack necessary to identify a data subject would be computationally difficult to complete; though not impossible.[60] These hashes could, therefore, be deemed outside of the GDPR's scope by virtue of such attacks being beyond the 'means reasonably likely to be used', though there is not yet adequate guidance on the threshold to be met for this to be the case.[61]

## IV. Erasing Personal Data

### 1. Defining Erasure

The notion of erasure for compliance with the Right is not defined in the GDPR and remains unclear. In the *Google Spain*[62] case that established the Right, the judgment (under the DPD) only required Google to remove links between the relevant data and the individual. As such, it could be argued that removing such links on blockchains would achieve compliance with the Right, though this is a questionable stance.[63]

In stark contrast to this argument, there is support for a strict interpretation of erasure: GDPR Article 17(2) mentions the erasure of 'any links to, or copy or replication of, those personal data', indicating that the removal of links to personal data does not constitute erasure

[58] cf Article 29 Working Party (n 30) 20-21: 'if the range of input values the hash function are known they can be replayed through the hash function in order to derive the correct value for a particular record'.
[59] ibid.
[60] ibid.
[61] cf Finck (n 16) 94.
[62] Case C-131/12 *Google Spain SL and Google Inc.* EU:C:2014:317.
[63] cf Armstrong et al (n 47) 122.

if there remain copies or replications of the data. Further, the court's judgment in *Nowak* explicitly defines erasure of personal data as its destruction.[64]

However, the *Nowak* judgment was made under the DPD, and DPD Article 28 references the 'blocking, erasure or destruction of data'[65], implying a difference between erasure and destruction of data. Additionally, this implies a difference between erasure and blocking of data, the latter of which is now referred to as restriction of processing under Article 18 of the GDPR. The corollary is that erasure of data might not require its destruction, but neither can it necessarily be achieved through the restriction of processing.

Since the GDPR is a technology-neutral and principles-based regulation, it is nonetheless conceivable that alternative technological methods of achieving the same objective, ie rendering personal data inaccessible, would be permissible for compliance with the Right. Indeed, the notion that erasure may be declared under the GDPR without strict erasure taking place is proposed by commentators such as Michèle Finck[66], and supported by several judgments including *Google v CNIL*[67] and *GC and Others*[68] in which the removal of links to the data was deemed sufficient.

However, these decisions related to publicly available search engine results, whereas the application of this pseudo-erasure argument to personal data recorded on blockchains currently lacks legal certainty.[69] If a loose interpretation of erasure under the GDPR is adopted, the restriction of access to these data could be deemed to secure compliance with the Right. In any case, measures that ensure that identification of the data subject cannot be achieved through the means reasonably likely to be used may, pursuant to Recital 26, suffice by bringing the data outside of the GDPR's scope.

### 2. Encryption

One potential solution for erasure on blockchains is to encrypt personal data before storing it on-chain, and then delete the decryption key when the data subject exercises their Right.[70] If

[64] Case C-434/16 *Peter Nowak* EU:C:2017:994, para 55: 'erased, that is to say, destroyed'.
[65] DPD art 28.
[66] cf Finck (n 16) 107.
[67] Case C-507/17 *Google v CNIL* EU:C:2019:772.
[68] Case C-136/17 *GC and Others* EU:C:2019:773.
[69] cf Finck (n 16) 107.
[70] Luis-Daniel Ibáñez et al, 'On Blockchains and the General Data Protection Regulation' (2018) 8 EU Blockchain Forum and Observatory <https://eprints.soton.ac.uk/422879/> accessed 20 June 2021.

state-of-the-art encryption is used, it would be virtually impossible to access the personal data without the decryption key, and so deleting the key could constitute erasure under the GDPR.[71] However, this would not achieve compliance with the Right under a strict interpretation of erasure, since the personal data could still be accessed through a brute-force attack.[72]

As emphasised by the Working Party, 'as long as the key or the original data are available … the possibility to identify a data subject is not eliminated'.[73] Despite this, if the attack would be computationally difficult enough, it may be beyond the 'means reasonably likely to be used' and thus outside of the GDPR's scope.[74] However, technological innovation could outdate current standards. The data may then be deemed personal and accessible once again, with stronger encryption necessary to meet the new threshold for anonymity or erasure.

### 3. Off-Chain Personal Data

Another possible solution is to store personal data off-chain in an encrypted database, and store the hash values of the data on-chain with references to the database.[75] Erasure of the off-chain personal data could then constitute erasure under the GDPR, leaving only hashed personal data on-chain. However, unless the hashed data are deemed anonymous under the GDPR, they would still be subject to the Right. In theory, the data subject could still be judged as identifiable from their hashed personal data as it could be used in a brute-force attack to find the corresponding input of the hash function (the original personal data). While identification could be rendered extremely difficult, it would not be impossible, and so compliance with the Right in this case would only be possible on the basis of a flexible notion of erasure.

### 4. Chameleon Hashes

Despite the immutability of blockchains, strict erasure under the GDPR can be achieved through certain innovative blockchain designs such as chameleon hash functions which allow blocks to be amended or removed without invalidating the rest of the blockchain. Ateniese et

---

[71] John Timmons and Tim Hickman, 'Blockchain and the GDPR: Co-existing in contradiction?' in Josias Dewey (ed.), *Blockchain & Cryptocurrency Regulation* (Global Legal Group 2020) 202.
[72] cf Armstrong et al (n 47) 124.
[73] cf Article 29 Working Party (n 33) 29; cf Ibáñez et al (n 70) 9.
[74] cf Ibáñez et al (n 70) 9.
[75] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 4(1) European Data Protection Law Review 17, 23.

al propose an innovative exploitation of chameleon hash functions that can 'allow designated authorities to edit, rewrite or remove previous blocks of information without breaking the chain'.[76]

This functionality is achieved by using a secure 'trap door' key to find collisions for the hashes of the relevant blocks, ie different inputs that yield the same hash value as the original inputs.[77] As such, the entire blockchain can remain linked through the hash values of blocks despite a block being amended or even removed.[78] Accenture filed a patent with Dr Ateniese for this redactable blockchain and is working with countries such as France, Sweden, and the USA on CBDC projects, though whether this erasure functionality will be adopted remains to be seen.[79]

Removal of blocks containing personal data would constitute erasure in the strict sense, though some criticise this solution as the blockchain would lose its fundamental trait of absolute immutability. Nevertheless, some degree of immutability is conserved in the solution proposed by Ateniese et al, as 'the blockchain remains immutable to users, and bad actors won't be able to make changes'.[80] Perhaps of more significant concern is that if the trap door key is lost or deleted, then the possibility of amendment or erasure of blocks is lost.[81]

Also, data controllers and processors cannot be forced to delete archived copies of the blockchain or to accept the changes and process the new chain.[82] Nonetheless, according to GDPR Article 17(2), a controller will have complied with the Right as long as they erase the relevant personal data and take 'reasonable steps' to inform other relevant controllers of the erasure request.[83]

## V. Concluding Remarks

This paper has found that the design of a blockchain-based CBDC that enables compliance with the right to be forgotten depends on the definitions of personal data and erasure under the

---

[76] Giuseppe Ateniese et al, 'Redactable Blockchain – or – Rewriting History in Bitcoin and Friends' (2017) *2017 IEEE European Symposium on Security and Privacy* 111.
[77] ibid 117.
[78] ibid.
[79] Accenture, 'Editing The Uneditable Blockchain' (2016) 7 <https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf> accessed 20 June 2021.
[80] cf Ateniese et al (n 76) 114.
[81] cf Finck (n 16) 108.
[82] ibid; cf Accenture (n 79).
[83] GDPR art 17(2).

GDPR, both of which lack legal certainty and guidance, and can be construed in either a strict or flexible manner. Firstly, if a flexible definition of personal data is adopted using a subjective criterion in assessing a data subject's identifiability, pseudonymisation methods such as encryption and hashing of personal data could suffice to bring the data outside of the GDPR's scope.

Conversely, a strict definition of personal data using an objective criterion for identifiability would qualify these pseudonymised data as personal data within the scope of the GDPR and subject to erasure requests. According to a flexible interpretation, erasure could be achieved through the encryption or hashing of personal data and subsequent deletion of the decryption key or off-chain personal data. However, under strict definitions of both anonymisation and erasure, blockchains would need to enable the amendment or removal of blocks containing personal data to facilitate compliance with the right to be forgotten. One such blockchain design is enabled by the use of chameleon hashes, which could allow personal data to be fully erased.

Since the appropriate solutions ultimately depend on the definitions of personal data and erasure under the GDPR, data protection authorities such as the EDPB should issue guidance on these concepts to enhance legal certainty and thus stimulate technological innovation. Although each dataset would require an independent assessment of identifiability due to their unique characteristics, this guidance could at least either reassure data controllers that flexible notions of personal data or erasure are compatible with the GDPR, or emphasise that strict definitions must be followed.

Equally, the GDPR could be amended to clarify the notions of personal data and erasure, yet this is not recommended as a solution. The GDPR is a technology-neutral statute, and so should not require updates in line with technological developments such as blockchains. Further, regulatory upheaval would be a costly and arduous process for the public and private sectors alike, both of which are still working on compliance with the GDPR as it stands. Amendment to the GDPR would therefore be undesirable and premature, whereas the provision of guidance would constitute a straightforward and effective solution to the underlying issue of legal uncertainty.

# Discussion Paper #2

## Will Central Bank Digital Currencies (CBDC's) Eliminate the Need for Cryptocurrencies?

*Kelly Ann Coulter*

Researcher

University of Essex

**Abstract**

As of February 2021 there were 4,501 crypto coins on the market (Best 2021). In response to the explosion of blockchain development, The Bank of England are considering the introduction of a Central Bank Digital Currency (CBDC) (Bank of England 2021a). This would give the central bank the ability to build on their traditional centralised role in the economy, ensuring stability by providing certainty and liquidity in the financial system, as the UK's monetary and fiscal policy manager. This paper is sectioned into three parts addressing the question: Will a CBDC eliminate the need for cryptocurrency? The historical and contemporary role of the Bank of England is considered, crypto coins and CBDC are assessed against their competencies, and finally a comparison between the capability of crypto coins and a CBDC, comprises of an evaluation to whether either can meet the Bank of England's policy objectives. This paper finds that, if crypto assets become progressively governed by regulation through incorporation into existing and developing legal frameworks (Ferreira 2021; Agnikhotram and Kouroutakis 2018; Bank of England 2021a; Department of Treasury 2021), far from being exclusive assets, both a CBDC and crypto-assets present a range of potential opportunities to contribute to a host of financial instruments, that can operate in an interoperable, inclusive FinTech sector. This will result in supporting an open, competitive, and free market, ultimately benefitting end users in an increasingly globalised financial system.

**Keywords**: Central Bank Digital Currency (CBDC), Cryptocurrencies, Stablecoins, Bank of England, Crypto Assets, Bitcoin, FinTech, Financial Stability, Regulation, Financial Inclusion.

# "Will Central Bank Digital Currencies (CBDC's) Eliminate the Need for Cryptocurrencies?"


## Abstract

As of February 2021 there were 4,501 crypto coins on the market (Best 2021). In response to the explosion of blockchain development, The Bank of England are considering the introduction of a Central Bank Digital Currency (CBDC) (Bank of England 2021a). This would give the central bank the ability to build on their traditional centralised role in the economy, ensuring stability by providing certainty and liquidity in the financial system, as the UK's monetary and fiscal policy manager. This paper is sectioned into three parts addressing the question: Will a CBDC eliminate the need for cryptocurrency? The historical and contemporary role of the Bank of England is considered, crypto coins and CBDC are assessed against their competencies, and finally a comparison between the capability of crypto coins and a CBDC, comprises of an evaluation to whether either can meet the Bank of England's policy objectives. This paper finds that, if crypto assets become progressively governed by regulation through incorporation into existing and developing legal frameworks (Ferreira 2021; Agnikhotram and Kouroutakis 2018; Bank of England 2021a; Department of Treasury 2021), far from being exclusive assets, both a CBDC and crypto-assets present a range of potential opportunities to contribute to a host of financial instruments, that can operate in an interoperable, inclusive FinTech sector. This will result in supporting an open, competitive, and free market, ultimately benefitting end users in an increasingly globalised financial system.


**Keywords:** Central Bank Digital Currency (CBDC), Cryptocurrencies, Stablecoins, Bank of England, Crypto Assets, Bitcoin, FinTech, Financial Stability, Regulation, Financial Inclusion

## Introduction

The invention of cryptocurrency has developed the opportunities for investing and transacting in online markets, where Bitcoin and other altcoins have offered a novel non-sovereign alternative to fiat money. Cryptocurrency is created and controlled by online communities who are non-state entities, unbound by geo-political borders. As such, they usually consist of a community of network of users who employ user agreement through consensus mechanisms and utilise cryptographic protocols to achieve secure transactions with validated transfers of value stored on a public blockchain (Nakamoto 2008; Hileman and Rauchs 2017). Cryptocurrency is not governed by a traditional central authority, subsequently not legally enforced by the UK government as a currency, or legal tender (Treasury Committee 2018; Department of Treasury 2021). Similarly, the Euro-system central banks also do not recognise virtual currency as money or currency from a legal perspective (European Central Bank 2015).

As of February 2021 there were 4,501 crypto coins (Best 2021). Cryptocurrencies as they are colloquially known, or 'crypto-assets' as they are considered by the UK government (Treasury Committee 2018; Department of Treasury 2021), are along with Bitcoin, part of a wider crypto market (Martin, Cunliffe, and Munksgaard 2019). It is a market that is growing in capacity of coins and in trading volume (Best 2021) and is an economy with a growing market capital (Kharif 2021). In response to this pluralisation of money markets and competition of digital technology, the Bank of England has proposed their own development upon fiat currency, with the introduction of a sovereign backed Central Bank Digital Currencies (CBDC) (Bank of England 2021c) setting up a task force to coordinate efforts (Bank of England 2021a).

The European Central Bank (ECB) have described how a CBDC could be considered as; "a third form of base money, next to (i) overnight deposits with the central bank, currently available only to banks, specific non-bank financial firms, and some official sector depositors; (ii) banknotes, being universally accessible but arguably of limited efficiency and relying on old technology. Some publications distinguish the case of "wholesale" and "general purpose" CBDC, the former being only accessible to certain firms, while the latter universally accessible to all households" (Bindseil 2020, 2).

For the purposes of this paper, the discussion takes a similar stance and is centred around a general purpose CBDC offered in the form of deposit accounts, with the central bank to all households and corporations[1]. However, the evaluation takes a more of a user centred perspective, in focusing on a Bank of England retail CBDC, and its potential impact on the financial system. It considers the central banks contemporary role as operators and supervisors, and their ability with a CBDC to achieve their aim to pursue key public interest objectives in the payments sphere: safety, integrity, efficiency and access (Bank of England n.d.).

This paper will therefore consider the extent that a central bank digital currency will eliminate the need for cryptocurrencies in three separate but related sections. First, the historical role that the Bank of England has taken as the state authorised central bank will be discussed, analysing the former and contemporary rights and privileges which have dictated their historical operational monetary and fiscal policy activities. The second section of the paper will then move on to assess the competencies (including the potential benefits and challenges) of crypto coins including stable coins, and a CBDC. Finally in the third part, it will conclude evaluating the necessity for decentralised cryptocurrencies as non-state conferred currency, compared to the proposed centralised sovereign backed CBDC, controlled by the Bank of England.

## A Brief History of Central Banking: What is the Bank of England's Role?

### The Bank of England Charter

Since the Bank of England's charter by Parliament in 1694, monetary policy in the United Kingdom has typified the way in which the political and economic activity of fiat currency creation has been undertaken and legally enforced. Key decisions on how much currency and what types of currency are in circulation, are predominate examples of the ways in which powers are exerted through monetary policy by this central authority (The Bank of England 1969; Bank of England n.d.). Currency creation can then be considered a highly political and economic activity, with the Bank of England having the ability explicitly set monetary policy

[1] For a full technical review of two prominent arguments against CBDC, namely (i) risk of structural disintermediation of banks and centralization of the credit allocation process within the central bank and (ii) risk of facilitation systemic runs on banks in crisis situations and a tiered proposal solution, see (Bindseil 2020).

around this activity. They do so, in their own words to "promote the good of the people by maintaining monetary and financial stability" (The Bank of England n.d., 1).

Whilst it is not entirely clear how the bank should achieve such an ambiguous aim, Morgan (1965, 1) provided further guidance on the broad category of 'maintaining monetary and financial stability' suggesting that the functions of a modern central bank are "four- fold: to act as a manager of National Debt and banker to the government; to regulate the currency; to be a bankers bank, and to act as lender of last resort". However, in terms of currency formation, the specific function of determining the quantity of money in circulation seemed not be part of the Banks initial role, when in 1832, John Palmer the Governor of Bank of England made no mention of controlling money supply. Instead, he stated that the chief functions of the Bank were to:

"Furnish the paper money with which the public act around them, and to be a safe place deposit for the public money, and for the money of individuals who prefer a public body like the Bank to private bankers" (Abel Monitor 1841, 57).

## The Parliamentary Act and Legal Tender

The Parliamentary Act as the legal mechanism utilised to set up the Bank of England, was however vague in its wording, and did not explicitly specify a power for the Bank of England to issue notes per se (The Bank of England 1969). Enacting upon the 'bills or notes' section[2] within the Act, the bank interpreted the guidance and was consequently able to issue notes in the form of a sealed bill; an interest-bearing promissory note to cash (gold and silver) depositors or borrowers. Promissory notes were just one of three forms of paper money the Bank of England were issuing upon their formation, with the other two forms of paper money comprising of the running cash note payable to the bearer, and the accomptable note. The former note surviving the test of time being "in fact, the true forerunner of the modern Bank note"[3] (The Bank of England 1969, 211), thus eventually becoming the fiat currency that is the hallmark of the traditional British national legal tender.

[2] Section 28 provided that "…all and every bill or Bills obligatory and of Credit under the Seal of the said Corporation…" shall be assignable by endorsement. (see The Bank of England, 1969).
[3] The earliest running cash notes were completely hand written and it was probably not until sometime between 1696 and 1699 that partly printed notes came into regular use. (see The Bank of England, 1969).

In May 1696, the government allowed the Bank of England to suspend specie payment so that it was released from its contractual duty to redeem notes for gold (Duryea 2010). However, the government gave the Bank freedom to continue business as usual, in its activity of issuing bank notes and enforcing payment upon its own debtors. Additionally, imposing an heir of authority to the currency as nationally legitimised, any person who was found to have counterfeited Bank of England notes could be sentenced to death (HMSO 1830).

## Currency Issuance

Sir Theodore Janssen, one of the first Directors of the Bank of England, acknowledged the distinct nature that public banking was taking, particularly the historical unconventional business practice of regularly issuing notes as currency. He noted that "the giving out Notes payable to Bearer" …, a practice that he thought "...liable to many Dangers and inconveniences…" was a peculiarity – among public banks – of the new Bank of England. A year later in 1697 Janssen recognised the banks increasing dependence on note issuing, admitting that "…the custom of giving Notes hath so much prevailed amongst us that the Bank could hardly carry on Business without it" (The Bank of England 1969, 211).

Sir Janssen's warning does not appear to have altered the banks practices as centralisation of the money supply was further consolidated in 1708, when parliament conferred another privilege to the Bank of England by making it unlawful for any corporate body, other than the Bank, to issue demand notes. This also added a similar prohibition of any partnership of a bank of no more than six persons (The Bank of England 1969). Competition for the Bank of England was restricted as competitors were constrained by the new rules by being proscribed from issuing bank notes redeemable on demand, and not being able to make short term loans under a six-month period. Thus, the competitors were small banks with less than seven partners who were severely limited in their operations. This imposed a great advantage on the Bank of England as a corporation with the opportunity to capitalise on their legalised privileges on issuing interest bearing currency.

## The South Sea Company and Country Banks

The South Sea Company newly created in 1711, led by Prime minister Robert Harley, was however one such example as a significant competitor for the Bank of England. Yet, this corporate competition was short lived, and after nine years collapsed under the weight

inflationary monetary expansion and stock speculation. Due to the 'South Sea Bubble crisis', the Bank of England was allowed by the British government to suspend specie payments on an indefinite basis. The Bank of England's bank notes therefore successfully railed against economic pressures of the Jacobite rebellions of 1715 and 1745, and the South Sea crisis in 1720. With around £3 million notes in circulation during 1720 (The Bank of England 1969), the bank held its rank as the leading corporation in the English banking system.

During the late eighteenth century, a few small, private partnerships formed to issue notes in response to the Bank of England's policy of monetary expansion. 'Country banks' as they were known, would use Bank of England notes as reserves and pyramided their own notes on top of them, and by 1793 there were nearly 400 fractional reserve banks of issue in England (Rothbard 2012). By 1833, the Bank of England Act was established. This Act granted the Bank of England's notes as legal tender status in England and Wales for the amount stated on the note with the provision that "the Bank continued to pay on demand notes in legal coin (an obligation from which they were released by the Gold standard of 1925)" (The Bank of England 1969). Country banks could now redeem their notes into Bank of England notes as opposed to in specie. This furthered and consolidated the Bank of England's power to functioning as the central bank of England. The centralisation of monetary supply and the responsibility for the management of monetary policy therefore has remained stable key features of the Bank of England's history.

## Central Bank Digital Currencies (CBDC's): What is the Future of State Money?

### Centralisation of Digital Currency for Financial Certainty and Stability

The four UK financial authorities – the Bank of England, HM Treasury, the Financial Conduct Authority and the Prudential Regulatory Authority – work together to make sure the UK financial sector runs smoothly, efficiently and effectively (Bank of England n.d.). In addition to cash and reserves, financial instruments, the policy that accompanies them and the banks role, have inevitably developed over the period since the Bank of England's charter; particularly so in the 21st century with digitalisation and transformation of financial services (Dow 2017).

The Bank of England supply the ultimate means of payment for banks (bank reserves), and a highly convenient and visible one for the public (cash). Cash however is currently the only means by which the public can hold central bank money (Borio et al. 2017), however, use of cash for has significantly decreased over time (BBC 2019). With the potential introduction of national central bank digital currencies in the 21st century (Bank of England 2021c), the Bank of England have the ability to build on their traditional centralised role in the payment system, ensuring stability by providing certainty and liquidity in the financial system as the UK's manager of monetary policy.

## Fostering Innovation in the Payments Infrastructure

A CBDC could present a number of opportunities for the way that the Bank achieves its objectives of maintaining an open and innovative but safe competitive monetary system, whilst upholding vital financial stability in serving the public interest (Bank for International Settlements 2021a). Technology has changed the future of money tremendously (Maurer 2015). Innovative digital products and services such as cryptocurrency, smart contracts and blockchain are everchanging the economic landscape (Deloitte 2019; Vadgama and Tasca 2020), where the number of blockchain and smart contract projects hosted on GitHub from January 2013 to April 2018 rapidly increased (Cong and He 2018). Smart contracts are being deployed across a range of sectors both in the financial sector, public sector, supply chain management, and the automobile, real estate, insurance, and health care industries (Alliance 2016; Cong and He 2018; Hu et al. 2018).

With the rise in blockchain services, advanced features such as smart contracts will ultimately be the basis of the future of financial services (V. Chang et al. 2020). This demand to adapt to the market and modernise financial services, will drive the Bank of England to foster innovation in their supervisory role of Financial Market Infrastructures (FMI's) (Bank of England n.d.). As the organisation faces a change in external environment, fostering innovation should encourage greater competition by the Bank of England.

Sweden and how the Riksbank have encouraged innovation in the retail payments market is a prime example of how a bank has responded to a changing fintech economy. Sweden is already a low cash society and with the Riksbank innovation, this has resulted in over half of the Swedish population having downloaded the fast payments app (Swish) on their smart

phone, leading it to become a prominent feature in the retail payment landscape, providing a substitute for cash in person to person (P2P) payments (Skingsley 2017). In the modern economic landscape where banks face competition from global economy and a plurality of private technology companies offering monetary services, it is necessary for the Bank of England to adapt itself to the changes in the digital economy.

A particular benefit of the implementing a CBDC by the central bank is that it could enhance existing payments infrastructure for both wholesale and retail (Bank of England 2021a). This could increase the speed and efficiency of payments, while reducing costs and generally support a resilient payments landscape (Bank of England 2020). This is ever important as meeting future payment needs in the digital economy becomes increasingly vital in light of usability, stability and security challenges that are associated with global ecommerce activity (Manyika 2016; Singh et al. 2020; Karpunina et al. 2020; Gilderdale 2017).

## Encouraging Interoperability and Financial Inclusion

The ultimate benefits of adopting a new payment technology will depend on the competitive structure of the underlying payment system and data governance arrangements (Bank for International Settlements 2021a). Encouraging greater competition can reduce barriers to entry and boost access to global markets through increased interoperability. Co-ordinating interoperability is particularly essential in the payments sector (Lammer, Garcia, and Polverini 2016). The growth of cross-border payments has been influenced by factors including; manufacturers expanding their supply chains across borders; cross-border asset management and global investment flows; international trade and e-commerce; and migrants sending money via international remittances (Committee on Payments and Market Infrastructures 2020). However cross border payments can be complex. They can provide more challenges than domestic ones involving various intermediaries, time zones and jurisdictions limiting operating hours, capital control regulations, resulting in long transaction times associated with high fees (Bank of England n.d.; Cojocaru and Cojocaru 2015; Pablo, Pacheco, and Lozano 2021). CBDCs built on digital identification present the opportunity to improve cross-border payments, and limit the risks of currency substitution (Bank for International Settlements 2021a).

A CBDC can assist in the efforts to coordinate interoperability among cross border payment structures, which also promotes financial inclusion by increasing access to financial services for unbanked and under banked populations and enhance peer to peer international payments (Bank of England 2021a). Mobile banking has commonly been viewed as a tool for an alternative to traditional forms of banking for the unbanked and under banked economically disadvantaged citizens, with initiatives (for example M-Pesa (Jack and Suri 2011)) most prevalent in Africa and the developing world (Asongu and Odhiambo 2019; Maurer 2008; Asongu 2015; Donner and Tellez 2008; Batista and Vicente 2020). Mobile financial services tend to offer a level of convenience and affordability that low-income earners require, whereas the basic bank accounts offered to the unbanked poor are expensive to maintain (Makore, n.d.).

If for example a retail CBDC is aiming to increase access to financial services for the unbanked and under banked populations, a requisite should be for the central bank to address the needs of those at the bottom of the pyramid in financial inclusion strategies. Financial intervention for these populations who use alternative financial services therefore needs to address the needs of the excluded populace, found by the FDIC unbanked and under banked survey to differ widely, but common among lower-income households, less-educated households, younger households, black and Hispanic households, and working-age disabled households (Burhouse et al. 2016). The elements of socio-economic status as well as education, are key to promoting financial inclusion and challenges that CBDC intervention will have to address, if they are to act as an intervention tool for the poorest in society. It must therefore offer interoperability with open payment platforms, and have the opportunity to provide financial inclusion measures for the public good (Bank for International Settlements 2021a).

## Maintaining Sovereignty and Financial Stability

Design and implementation of a CBDC by the Bank of England will not only stand as an intervention tool but also secure the central banks sovereignty over monetary policy. This market power could work to legitimise attempts at financial reform. In the bank's main role as monetary policy maker, who are a publicly accountable institution, this puts them in the ideal position to maintain financial stability and confidence in the UK banking system, a pivotal responsibility of the Bank of England. The stability of the financial system is

dependent upon the operational resilience of the system's ability to absorb and adapt to economic shocks and disruptions (Bank for International Settlements 2021b; Bank of England n.d.; Financial Stability Board 2020). The extent to which a CBDC can fulfil financial and economic stability will therefore rest on the success of it as an intervention policy tool for reform providing conditions such as settlement finality, liquidity and integrity (Bank for International Settlements 2021a).

## Cryptocurrencies: Cyberspace Money Without Flags?

### Bitcoin as the Leading Cryptocurrency

Bitcoin was the original blockchain which stands as the virtual currency with the most popularity and highest market capital to date (Coinmarketcap n.d.); representing a benchmark for the crypto markets. Bitcoin was the first of a peer to peer digital currency that eliminated the need for a third party, such as a central bank to validate transactions, by utilising a distributed ledger system where the decentralised consensus mechanism - Proof of Work - ensured validity and trust within the network (Nakamoto 2008; Hileman and Rauchs 2017).

Due to the distributed, global nature of cryptocurrency that is not bound by geo-political borders, bitcoins can be described as cyberspace money without flags, requiring no issuance from any state government or central authority. Regardless of lacking legal tender status, cryptocurrency can function like any other currency - to buy and sell goods or services or be traded as an asset or currency in global markets. Trading as an asset or currency can be conducted on crypto platforms, for example in a similar way to a foreign exchange currency. Coinbase (2021), Binance (2021), and Huobi (2021) are examples of centralised crypto exchanges and decentralised peer to peer exchanges such as Uniswap (2021) or Tokenlon (2021) offer similar services.

Bitcoin as a digital currency has faced a problem of currency definition, which in part serves to undermine public reassurance with debates over its role as a currency, or asset in the financial markets (Yermack 2015; HMRC 2014). Proponents have argued that Bitcoin currently does not fulfil the criteria of being a currency, because it does not function as a medium of exchange, a unit of account, or a store of value (Cermak 2017). Bornholdt and Sneppen (2014) have analysed the market forces driving Bitcoin, specifically the perception of the value of Bitcoin. They concluded that 'perception of value in a social system is

generated by a voter-like dynamic, where fashions form' (ibid. p1). These 'fashions' are based on perceptions, such as attitudes and values toward Bitcoin which in a social system, can then influence positively or negatively on the crypto market. Dependent upon the societal consensus of Bitcoin's definition, whether Bitcoin can substitute as a real economic alternative to fiat currency, has therefore been debated (Dodd 2018).

The academic literature is rich in discussion on economic debates over Bitcoin's value (Bornholdt and Sneppen 2014; Hayes 2015; Ciaian, Rajcaniova, and Kancs 2016). Economists have predominately reported on the value of bitcoin, with research focusing on the rising price of Bitcoin and its volatility (Ciaian, Rajcaniova, and Kancs 2016; Hileman and Rauchs 2017). Excess volatility is an impediment for digital currency, leading Baur and Dimpfl (2018) to conclude that Bitcoin cannot function as a currency. However, Cermak (2017) claimed that the volatility of Bitcoin has been steadily decreasing throughout its lifetime.

Bitcoin's potential technological vulnerabilities are well documented (Barber et al. 2012; Eyal and Sirer 2018; Courtois, Song, and Castellucci 2016), with many scholars in the information technology sector also probing the notion to whether Bitcoin will ever be an option for a stable, and sustainable main currency (Courtois, Song, and Castellucci 2016; Eyal and Sirer 2018; Barber et al. 2012). The security of Bitcoin has attracted much attention in this area, as it is essential for market stability that any sustainable currency remains stable, safe and secure for users[4]. The usefulness and security reassurance is an issue for non-crypto end users, who found these reasons a barrier to Bitcoin adoption, as they questioned the value and security issues (Presthus and O'Malley 2017).

Operational challenges for end users such as technological barriers, structural vulnerabilities and access issues, are compounded with Bitcoin's ubiquitous legal character and regulatory challenges (Perkins and Enwezor 2016; Kakavand, Kost De Sevres, and Chilton 2017; Ioannou 2020). Its reputation has been tarnished by its close association with illicit ecommerce activities on dark markets, such as Silk Road (Greenberg 2020), as well as illegal activities such as money laundering (van Wegberg, Oerlemans, and van Deventer 2018) and

[4] For an insightful and developed technical analysis of Bitcoin's properties and stability, see (Bonneau et al. 2015).

terrorism financing (Greenberg 2020; Teichmann 2018; Amiram, Jorgensen, and Rabetti 2020; Chainalysis 2020).

It is important to consider that cryptocurrency privacy features can be appealing to criminals (Kottasova 2018; Chainalysis 2021). On the other hand cryptocurrencies can provide a complementary currency, offering a host of economic benefits (Nica, Piotrowska, and Schenk-Hoppp 2017). Low transaction costs, a low level of entry, worldwide speed, and pseudo-anonymity of the transactions, are often posited as the main advantages of cryptocurrency use, making it an attractive transaction media particularly for example in African countries (Nseke 2018). Further, Bitcoin has been reportedly used as an alternative currency option, particularly in South American countries to avoid rising hyperinflation (Di Salvo 2019). Venezuela's success in driving crypto adoption as number 3 in the global crypto adoption index (Chainalysis 2020) for example, illustrates a logical response to how citizens use cryptocurrency to mitigate economic instability and government mistrust. Sayfang (2010) concluded that complementary currencies;

"are a creative, innovative and increasingly mainstream policy tool with an important role to play in the development of localities, alongside national and international currencies. Whether one adopts an orthodox or an alternative perspective on money, economic activity and society, there are strong justifications for their use" (Seyfang 2010).

Despite the Bitcoin hype and a decade of growth as the leading cryptocurrency, this has not yet led Bitcoin to become a stable global cryptocurrency for the purchasing and exchanging goods and services online, or to conduct business swiftly, without access related issues and the financial burden of high transactional costs (Taskinsoy 2019). The inefficiency of Bitcoin as a medium of exchange, has resulted in Bitcoin becoming predominately used as a speculative asset (A. D. Lee, Li, and Zheng 2020). More generally it is used for investment purposes, as opposed to a medium of exchange, for day-to-day transactions to buy and sell lower priced goods and services as an alternative currency, (D. G. Baur, Hong, and Lee 2018; Ghysels and Nguyen 2019).

## Cryptocurrency Stability and Stable coins

In an attempt to tackle some of the technical barriers (such as high transaction fees and volatility), some private non sovereign backed altcoins have addressed these issues by being

developed with technical stability features to solve these barriers. Once for example the high transaction fees issue is resolved, altcoins can position themselves as an alternative currency. There are a number of cryptocurrencies which have lower transaction fees than Bitcoin (Nasdaq 2018), including Dash (Marley 2018), Ethereum (Buterin 2013), Litecoin (Lee 2011), Bitcoin Cash (Bitcoin Cash n.d.) and Ripple (Ripple n.d.); whilst some such as Nano (Nano n.d.) claim to offer fee-less transactions (Lemahieu, n.d.). Open competition from a plethora of cryptocurrencies gives options for an alternative currency, with user friendly payment systems and the stability this provides, as an applied medium of exchange for consumption in the real economy.

The stability of a cryptocurrency can be driven by its volatility and is often a key feature. The volatility dynamics in the crypto market are clearly acknowledged (Katsiampa 2019; Catania, Grassi, and Ravazzolo 2018; Yi, Xu, and Wang 2018; Abakah et al. 2020). Examining the relationship between volatility and returns of leading cryptocurrencies, to investigate spill overs within the cryptocurrency market, (Liu and Serletis 2019) found statistically significant transmission of shocks and volatilities among the leading cryptocurrencies. Conversely, seeking properties of crypto stability, Elbahrawy et al. (2017) considered the history of the entire crypto market by analysing the behaviour of 1469 cryptocurrencies introduced between April 2013 and May 2017, revealing that several statistical properties of the market have in fact been stable for years. These included for example the number of active cryptocurrencies, market share distribution, and the turnover of cryptocurrencies (Elbahrawy et al. 2017).

Volatility in the crypto market leads to price fluctuations (Sovbetov and Sovbetov 2018; Katsiampa 2019; Yi, Xu, and Wang 2018), putting it at odds with the requirement for currency to remain a stable unit of account and good store of value (from an orthodox economic perspective). Whilst there are tools using trading volume for instance, to predict volatility in the crypto markets (Bouri et al. 2019), stable coins offer a reliable source of stability. Price volatility around Bitcoin and other top market capital cryptocurrencies therefore illustrates the necessity for stable coins. Bolstered by the Decentralised Finance (DeFi) markets, stable coins can provide lower volatility crypto-assets which can be pegged to fiat currency. Tether is an example of this, which serves as an option to use cryptocurrency as a legitimate fiat alternative, where it aims to offer consumer confidence that the value of the instrument will be consistent from one day to the next (Tether n.d.).

The adoption of stable coins as stable crypto assets is particularly useful for emerging blockchain applications, such as DeFi. These can act to welcome retail and institutional investors into the market who are seeking cash flow and income generation through crypto yields. Particularly in the DeFi space, staking and yield farming using decentralised platforms such as Compound (2021), BlockFi (2021), or alternative platforms (SourceForge 2021), or taking advantage of decentralised lending and borrowing of crypto collateralised stable coins, can provide potential passive income (Rapoza 2021), and help to stabilise volatility in the crypto markets (Kahya, Krishnamachari, and Yun, n.d.).

## CBDC's vs Cryptocurrency: Will Central Bank Digital Currencies Eliminate the Need for Cryptocurrencies?

### Consumer Protection

Consumers are protected in the free market from anti-competitive behaviours from traditional companies (McMahon 2020), however crypto projects are often organisations which are communally decentralised in their structure, with no central organisation or authority to regulate (Lianos et al. 2019; Herian 2018; Walch 2019). This raises legal challenges for regulators to address, in light of dispute resolution and enforceability issues (Kaal and Calcaterra 2018). Further, as (Dupont and Maurer 2015, 1) point out "blockchain systems occasion a reconsideration of two of the central legal devices of modernity: the ledger and the contract". An independent set of rules, a subset of law known as 'Lex Cryptographia' (Wright and De Filippi 2015), could displace court enforcement by code enforcement, however, in practice it is likely that this would involve incorporating cryptocurrency into existing frameworks (Ferreira 2021), or implicate an extension to existing legal doctrines (Agnikhotram and Kouroutakis 2018).

Cryptocurrencies including Bitcoin, with their absence of legal standing as UK legal tender (HMRC 2014; Department of Treasury 2021), could be considered a case against supporting the use of it as a medium of exchange within the UK's free market. Bitcoin is not circulated for public use by the UK's central bank – the Bank of England. Bitcoin is only able to be issued once mined on the network and acts as a decentralised and distributed cryptocurrency (Nakamoto 2008). This is in stark contrast to fiat currency, which is controlled and regulated by the Bank of England as a central authority in the UK (Bank of England 2021b).

Operationally, the centralisation and decentralisation feature are an important distinction to make between fiat currencies and cryptocurrencies, the latter which can evoke different levels of decentralised permissioned and permissionless blockchain features (Hileman and Rauchs 2017). The very nature in the way they are designed and operate, is therefore politically and socially influenced in varying degrees, and this has its own governance consequences for users (Golumbia 2016; Dodd 2018; Filippi and Loveluck 2016; Nabilou 2020).

## Financial Governance

The concern of financial governance within society raises questions of who should create and control monetary policy, and to what extent? Fiat money in society has had a long history of political support by governments with its bestowed legal tender status, economic regulatory frameworks protections, and legal mechanisms in place for arbitration and dispute resolution. As a result of cryptocurrencies falling outside the remit of the state's governance including the Bank of England's monetary policy (including its regulatory safeguards), has led some critics to argue that crypto poses a threat to the stability of the financial system by destabilising the economy (Jopson 2016; Inman 2014).

Concern about cryptocurrencies are echoed by those who highlight the link of cryptocurrency to criminal funding and illicit activities (Teichmann 2018; Amiram, Jorgensen, and Rabetti 2020; Kottasova 2018). However, whilst digital currency is a recent monetary development in the last decade, it is clear that illegal drug markets existed before Silk Road and did not emerge in a vacuum inventing an online drug trade where none had existed before, and nor did it invent the technologies upon which it is dependent (Martin, Cunliffe, and Munksgaard 2019). Illicit cryptocurrency transactions have risen, both in total value and as a share of all cryptocurrency activity, however, illicit transactions still constitute a small share of all cryptocurrency activity at just 1.1% (Chainalysis 2021).

The Chainalysis report accounts a low prevalence rate of 1.1%, which could be considered a relatively low risk to financial stability. Further, as crypto assets increasingly become regulated (Department of Treasury 2021) both in the crypto currency exchange and DeFi markets (Wintermeyer 2021; Dale 2021), concerns about illicit activity may be allayed with the inception of a regulatory framework applied to digital currencies (Perlman 2019; Treasury 2020).

Structural issues of cryptocurrencies such as security and the risk of technical vulnerabilities, may be addressed by development of smart contracts. Smart contracts have seen significant efforts to improve security by introducing new programming languages and advance verification methods, with new verification tools and methods available for smart contract and distributed ledgers (Harz and Knottenbelt 2018). Functional problems such as crypto volatility and its associated risk of price fluctuations, is circumvented via stable coin volatility harvesting. Adoption of a weighted risk contribution index can serve volatility harvesting, where an index which combines a basket of five crypto assets with an investment in gold, aims to improve the risk profile of the resulting portfolio (Koutsouri et al. 2020). Cryptocurrency market returns can accordingly have hedging and safe-haven properties, but the responses of cryptocurrency markets depend on the type of uncertainty (Colon et al. 2021).

## Implications for Monetary Policy

Considering the governance issues of cryptocurrency and given their structural and functional properties, a CBDC could share some characteristics that can positively influence monetary policy. Innovation is one of the most influential factors which have emanated from cryptocurrencies, forcing the central bank to face an adaptive, fast paced financial market with blockchain adoption. As cash declines and digital payments rise in society, it is inevitable that payment infrastructures need to accommodate global commerce transactions, at a low cost and fast speed, therefore requiring interoperability (Lammer, Garcia, and Polverini 2016).

With the explosion of smart contracts and other blockchain projects, this has proven that consumers want to contract in a fast and efficient way, obviating third party intermediaries, who slow the process and cause more cost to the end user. This is most observed from a financial inclusion perspective, where a retail CBDC interoperability mechanism can work to increase access to financial services for unbanked and under banked populations, by enhancing peer to peer cross border payments (Bank of England 2021a). Cryptocurrencies can already offer this advantage of precluding third party intermediaries from their transactions, through their decentralised properties. However, this benefit comes at a cost for non-custodial accounts, which is that the users must take responsibility in acting as their own bank (Dingle 2018).

## Trust in the System

One specific benefit of a CBDC over cryptocurrencies, is the reputation of their creator. The Bank of England as the UK's central bank historically, has taken the role in directing monetary policy and maintaining financial stability, for the public good. This implicit trust by the public is grounded in knowing that the Bank of England as an accountable public institution will not suddenly fail, liquidate or disappear with their money, as was the case for example with the cryptocurrency 'Onecoin' (Cellan-Jones 2019).

Notably, Bitcoin as the original blockchain was borne incidentally of the back of the 2008 financial crisis, at a time when public faith was low among public institutions allowing it to gain legitimacy (Weber 2015). Due to the perceived failings of the financial system, this helped drive Bitcoin adoption (Saiedi, Broström, and Ruiz 2021). Consumers, particularly those that have lost trust in their financial institutions, may wish for a safe place deposit for their money. They may prefer a public body like the central bank, compared to a private commercial bank. This was in fact, a chief function of the central bank according to John Palmer, Governor of the Bank of England during 1832 (Abel Monitor 1841), much before the financial crisis of 2008 occurred.

The cryptocurrency markets could be considered a strong hedge against geopolitical risks in most cases, but it could be considered a weak hedge and safe haven against economic policy uncertainty during a bull market (Colon et al. 2021). Cryptocurrencies including stable coins could pose as competition for the central bank, and under certain geo-political conditions drive adoption. Competition is not a new phenomenon and the Bank of England have faced a history of competitors, including the South Sea Company and country banks (The Bank of England 1969). In spite of this, they have used their legal privilege to their advantage which has reduced competition for currency issuance; this is likely to continue to be the case. Most money in the modern economy is in the form of bank deposits, which are created by commercial banks (McLeay, Radia, and Thomas 2014) and therefore competitive currency issue becomes less of an issue. In any case, as cryptocurrency continues to be regulated as a crypto asset class, currency issuance becomes less of a threat to the bank as more people use it as an investment vehicle, rather than a medium of exchange (D. G. Baur, Hong, and Lee 2018).

For consumers who are concerned with privacy of transactions, privacy focused cryptocurrencies can play a role (Li et al. 2019). Similarly, those who wish to speculate on crypto assets, can do so on volatile coins (McCoy and Rahimi 2020). Consumers who have a need for income generation assets can consider private stable coins and their volatility harvesting options (Koutsouri et al. 2020). The most economically challenged in society could also contemplate stable coins for their the value stability benefits (Calabia 2020). Alternatively, those who are unbanked or under banked may consider a retail CBDC for the accessibility it could offer over crypto coins and consequential responsibility, commitment and challenges that are associated with being their own decentralised bank, in terms of usability and security (Dingle 2018).

## Conclusion

The centralisation of monetary supply, and the responsibility for the management of monetary policy, have remained stable key features of the Bank of England's history. In its role as the central bank since receiving its charter from Parliament in 1694, the Bank of England can make use of its historical reputation, and sovereignty of currency policy, to engender trust in the UK financial system. Facing competition from external environmental factors, has diminished in the past, by levying their currency issuing privileges (Kynaston 1995). However, with the invention of the internet and subsequent technological developments in payments systems and digital tokenisation, decentralised smart contracts and blockchain use cases, the central bank is now confronted with the tackling issue of sustaining financial certainty, stability, and growth in a revolutionised financial system. This presents a contemporary challenge in the digital currency economy, that currently operates as a largely under-regulated market, and one that is out of the banks centralised control, even in light of their respective operational monetary and fiscal policy management of the economy.

By fostering innovation and learning from other countries successes', the bank can adapt to the challenges in the everchanging digital infrastructure. Innovative products such as a CBDC, can assist the bank to meet its objective - which have remained throughout its history to 'promote the good of the people by maintaining monetary and financial stability'. Introduction of a CBDC has the potential to promote financial inclusion (Bank of England 2020), for those who are currently unbanked or underbanked. In this regard, a retail CBDC would work well for end users who require low cost, fast transactions, and easy accessibility (Calabia 2020). Interoperability with current payment infrastructure will be a necessary

requisite for a retail, or wholesale CBDC, as an intervention tool for financial inclusion (Committee on Payments and Market Infrastructures 2020) .

As smart technology develops in the economy (Y. Chang, Iakovou, and Shi 2020; Vadgama and Tasca 2020) and the debate persists on governance of blockchain (Nabilou 2020; Poncibò 2021; Kakavand, Kost De Sevres, and Chilton 2017), regulation will inevitably follow as regulators, policy makers and law professionals apply digital currency to existing and developing legal frameworks (Ferreira 2021; Agnikhotram and Kouroutakis 2018). This will work to legitimise cryptocurrency as crypto assets positioned in their own asset class (Perlman 2019). The extent to which they will be an appropriate option of alternative finance, may depend on the level of appropriate consumer protection available. Stable coins may be part of this class, which provides the consumer with more choice, specifically related to instruments with low volatility (Kahya, Krishnamachari, and Yun, n.d.).

Both a potential CBDC and crypto-assets, therefore present a range of opportunities and challenges to contribute to an inclusive, globalised financial system. Singularly, neither can exclusively bring the entirety of benefits to users, or individually overcome the obstacles required for guaranteed future stability in their totality. But both CBDC's and crypto assets are capable of satisfying different properties and the utility of money – a unit of account, store of value and medium of exchange, to various extents for the public good; a key objective for the Bank of England. Ultimately, the plethora of public and private currencies on the market, once reached legal maturity in terms of governance, can provide the element of choice to consumers in an open, innovative, and competitive free market. Future research would benefit from exploring the specific design details and development of the proposed Bank of England's CBDC, and the public demand for it against cryptocurrency.

## References

Abakah, Emmanuel Joel Aikins, Luis Alberiko Gil-Alana, Godfrey Madigu, and Fatima Romero-Rojo. 2020. "Volatility Persistence in Cryptocurrency Markets under Structural Breaks." *International Review of Economics and Finance* 69 (September): 680–91. https://doi.org/10.1016/j.iref.2020.06.035.

Abel Monitor, Esq. 1841. "FACTS AND FALLACIES." https://play.google.com/books/reader?id=lT0KAQAAMAAJ&hl=en_GB&pg=GBS.PA1.

Agnikhotram, Sai, and Antonios Kouroutakis. 2018. "Doctrinal Challenges for the Legality of Smart Contracts: Lex Cryptographia or a New, Smart Way to Contract." *Journal of High Technology Law* 19. https://heinonline.org/HOL/Page?handle=hein.journals/jhtl19&id=300&div=13&collection=journals.

Alliance, Smart Contracts. 2016. "Smart Contracts: 12 Use Cases for Business & Beyond." *Chamber of Digital Commerce* 56: 1–53.

Amiram, Dan, Bjorn N Jorgensen, and Daniel Rabetti. 2020. "Coins for Bombs - Does Bitcoin Finance Terrorist Attacks?" *SSRN Electronic Journal*, November. https://doi.org/10.2139/ssrn.3616207.

Asongu, Simplice A. 2015. "The Impact of Mobile Phone Penetration on African Inequality." *International Journal of Social Economics* 42 (8): 706–16. https://doi.org/10.1108/IJSE-11-2012-0228.

Asongu, Simplice A., and Nicholas M. Odhiambo. 2019. "Mobile Banking Usage, Quality of Growth, Inequality and Poverty in Developing Countries." *Information Development* 35 (2): 303–18. https://doi.org/10.1177/0266666917744006.

Bank for International Settlements. 2021a. "III. CBDCs: An Opportunity for the Monetary System."

———. 2021b. "Basel Committee on Banking Supervision Principles for Operational Resilience Principles for Operational Resilience Iii." www.bis.org.

Bank of England. n.d. "Cross-Border Payments | Bank of England." Accessed June 27, 2021a. https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments.

———. n.d. "Financial Market Infrastructure Supervision | Bank of England." Accessed June 27, 2021b. https://www.bankofengland.co.uk/financial-stability/financial-market-infrastructure-supervision.

———. n.d. “Financial Sector Continuity | Bank of England.” Accessed June 27, 2021c. https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity.

———. n.d. “Monetary Policy .” Accessed June 27, 2021d. https://www.bankofengland.co.uk/monetary-policy.

———. 2020. “Central Bank Digital Currency: Opportunities, Challenges and Design | Bank of England.” https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper.

———. 2021a. “Central Bank Digital Currencies.” 2021. https://www.bankofengland.co.uk/research/digital-currencies.

———. 2021b. “How Is Money Created? .” Bank of England. 2021. https://www.bankofengland.co.uk/knowledgebank/how-is-money-created.

———. 2021c. “Bank of England Statement on Central Bank Digital Currency.” https://www.bankofengland.co.uk/news/2021/april/bank-of-england-statement-on-central-bank-digital-currency.

Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. 2012. “Bitter to Better—How to Make Bitcoin a Better Currency.” In *International Conference on Financial Cryptography and Data Security*, 399–414. Springer.

Batista, Catia, and Pedro C. Vicente. 2020. “Adopting Mobile Money: Evidence from an Experiment in Rural Africa.” *AEA Papers and Proceedings* 110 (May): 594–98. https://doi.org/10.1257/pandp.20201086.

Baur, Dirk, and Thomas Dimpfl. 2018. “Excess Volatility as an Impediment for a Digital Currency.” *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2949754.

Baur, Dirk G., Ki Hoon Hong, and Adrian D. Lee. 2018. “Bitcoin: Medium of Exchange or Speculative Assets?” *Journal of International Financial Markets, Institutions and Money* 54 (May): 177–89. https://doi.org/10.1016/j.intfin.2017.12.004.

BBC. 2019. “The Decline of Cash in the UK - in Charts - BBC News.” *BBC*, June 7, 2019. https://www.bbc.co.uk/news/business-48544695.

Best, Raynor. 2021. “Number of Crypto Coins 2013-2021.” *Statista*. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.

Binance. 2021. “Binance.” 2021. https://www.binance.com/en.

Bindseil, Ulrich. 2020. “Tiered CBDC and the Financial System.”

Bitcoin Cash. n.d. “Bitcoin Cash - Peer-to-Peer Electronic Cash.” Accessed May 13, 2021. https://bitcoincash.org/.

BlockFi. 2021. “The Future of Finance.” 2021. https://blockfi.com/.

Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. 2015. “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.” In *Proceedings - IEEE Symposium on Security and Privacy*, 2015-July:104–21. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SP.2015.14.

Borio, Claudio, Stijn Claessens, Benjamin Cohen, Dietrich Domanski, Hana Halaburda, Krista Hughes, Jochen Schanz, Hyun Song, Morten Bech, and Rodney Garratt. 2017. “Central Bank Cryptocurrencies 1.” *BIS Quarterly Review*. www.blockchain.info;

Bornholdt, Stefan, and Kim Sneppen. 2014. “Do Bitcoins Make the World Go Round? On the Dynamics of Competing Crypto-Currencies.” *ArXiv Preprint ArXiv:1403.6378*.

Bouri, Elie, Chi Keung Marco Lau, Brian Lucey, and David Roubaud. 2019. “Trading Volume and the Predictability of Return and Volatility in the Cryptocurrency Market.” *Finance Research Letters* 29 (June): 340–46. https://doi.org/10.1016/j.frl.2018.08.015.

Burhouse, Susan, Karyen Chu, Ernst. Keith, Ryan Goodstein, Alicia Lloro, Gregory Lyons, Joyce Northwood, et al. 2016. “FDIC National Survey of Unbanked and Underbanked Households.”

Buterin, Vitalik. 2013. “Ethereum Whitepaper .” *Ethereum*. https://ethereum.org/en/whitepaper/.

Calabia, Christopher. 2020. “Could the Poor Bank on Stablecoins? Discussion Prompts for Innovators, Regulators, and Consumers by F. Christopher Calabia :: SSRN.” *FinDev*, July. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3671661.

Catania, Leopoldo, Stefano Grassi, and Francesco Ravazzolo. 2018. “Predicting the Volatility of Cryptocurrency Time-Series.” In *Mathematical and Statistical Methods for Actuarial Sciences and Finance, MAF 2018*, 203–7. Springer International Publishing AG. https://doi.org/10.1007/978-3-319-89824-7_37.

Cellan-Jones. 2019. “Mystery of the Disappearing ‘Cryptoqueen’ Ruja Ignatova - BBC News.” *BBC*, September 26, 2019. https://www.bbc.co.uk/news/technology-49826161.

Cermak, Vavrinec. 2017. “Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoin’s Volatility Based on a GARCH Model.” *SSRN Electronic Journal*, May.

https://doi.org/10.2139/ssrn.2961405.

Chainalysis. 2020. “The 2020 Geography of Cryptocurrency Report Analysis of Geographic Trends in Cryptocurrency Adoption, Usage, and Regulation.” https://go.chainalysis.com/2021-Crypto-Crime-Report.html.

———. 2021. “The Chainalysis 2021 Crypto Crime Report.” https://go.chainalysis.com/2021-Crypto-Crime-Report.html.

Chang, Victor, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, and Mitra Arami. 2020. “How Blockchain Can Impact Financial Services – The Overview, Challenges and Recommendations from Expert Interviewees.” *Technological Forecasting and Social Change* 158 (September): 120166. https://doi.org/10.1016/j.techfore.2020.120166.

Chang, Yanling, Eleftherios Iakovou, and Weidong Shi. 2020. “Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities.” *International Journal of Production Research* 58 (7): 2082–99.

Ciaian, Pavel, Miroslava Rajcaniova, and d’Artis Kancs. 2016. “The Economics of BitCoin Price Formation.” *Applied Economics*. https://doi.org/10.1080/00036846.2015.1109038.

Coinbase. 2021. “Home .” 2021. https://www.coinbase.com/dashboard.

Coinmarketcap. n.d. “Bitcoin Market Capital.” Accessed November 13, 2018. https://coinmarketcap.com/.

Cojocaru, Camelia, and Silviu Cojocaru. 2015. “SEPA and Payments Industry - Challenges Concerning Standards and Operations.” *Manager Journal* 22 (1): 309–21. https://ideas.repec.org/a/but/manage/v22y2015i1p309-321.html.

Colon, Francisco, Chaehyun Kim, Hana Kim, and Wonjoon Kim. 2021. “The Effect of Political and Economic Uncertainty on the Cryptocurrency Market.” *Finance Research Letters* 39 (March): 101621. https://doi.org/10.1016/j.frl.2020.101621.

Committee on Payments and Market Infrastructures. 2020. “Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap - Technical Background Note.” www.bis.org.

Compound. 2021. “Compound.” 2021. https://compound.finance/.

Cong, Lin William, and Zhiguo He. 2018. “Blockchain Disruption and Smart Contracts.”

Courtois, Nicolas, Guangyan Song, and Ryan Castellucci. 2016. “Speed Optimizations in Bitcoin Key

Recovery Attacks." *Tatra Mountains Mathematical Publications* 67 (1): 55–68.

Dale, Brady. 2021. "DeFi Is Now a $100B Sector -." *Coindesk*, April 29, 2021. https://www.coindesk.com/defi-100-billion-dolla.

Deloitte. 2019. "Global Blockchain Survey." https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf.

Department of Treasury. 2021. "UK Regulatory Approach to Cryptoassets and Stablecoins: Consultation and Call for Evidence." London. www.gov.uk/official-documents.

Dingle, Simon. 2018. *In Math We Trust: Bitcoin, Cryptocurrency and the Journey To Being Your Own Bank*. Jonathon Ball Publishers. https://www.google.co.uk/books/edition/In_Math_We_Trust/ysXnDwAAQBAJ?hl=en&gbpv=0.

Dodd, Nigel. 2018. "The Social Life of Bitcoin." *Theory, Culture & Society* 35 (3): 35–56. https://doi.org/10.1177/0263276417746464.

Donner, Jonathan, and Camilo Andres Tellez. 2008. "Mobile Banking and Economic Development: Linking Adoption, Impact, and Use." *Asian Journal of Communication* 18 (4): 318–32. https://doi.org/10.1080/01292980802344190.

Dow, Sheila. 2017. "Central Banking in the Twenty-First Century." *Cambridge Journal of Economics* 41: 1539–57. https://doi.org/10.1093/cje/bex051.

Dupont, Quinn, and Bill Maurer. 2015. "Ledgers and Law in the Blockchain." Kings Review. June 23, 2015. https://www.kingsreview.co.uk/essays/ledgers-and-law-in-the-blockchain.

Duryea, Scott N. 2010. "WILLIAM PITT, THE BANK OF ENGLAND, AND THE 1797 SUSPENSION OF SPECIE PAYMENTS: CENTRAL BANK WAR FINANCE DURING THE NAPOLEONIC WARS." *Libertarian Papers* 2 (15): 1.

Elbahrawy, Abeer, Laura Alessandretti, Anne Kandler, Romualdo Pastor-Satorras, and Andrea Baronchelli. 2017. "Evolutionary Dynamics of the Cryptocurrency Market." *Royal Society Open Science* 4 (11). https://doi.org/10.1098/rsos.170623.

European Central Bank. 2015. "Virtual Currency Schemes-a Further Analysis," February. https://doi.org/10.2866/662172.

Eyal, Ittay, and Emin Gün Sirer. 2018. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." *Communications of the ACM* 61 (7): 95–102.

Ferreira, Agata. 2021. “Regulating Smart Contracts: Legal Revolution or Simply Evolution?” *Telecommunications Policy* 45 (2): 102081. https://doi.org/10.1016/j.telpol.2020.102081.

Filippi, Primavera, and Benjamin Loveluck. 2016. “The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure by Primavera De Filippi, Benjamin Loveluck :: SSRN.” *Internet Policy Review* 5 (4). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691.

Financial Stability Board. 2020. “COVID-19 Pandemic: Financial Stability Implications and Policy Measures Taken.” www.fsb.org/emailalert.

Ghysels, Eric, and Giang Nguyen. 2019. “Price Discovery of a Speculative Asset: Evidence from a Bitcoin Exchange.” *Journal of Risk and Financial Management* 12 (4): 164. https://doi.org/10.3390/jrfm12040164.

Gilderdale, Stephen. 2017. “SWIFT’s Customer Security Programme: Preventing, Detecting ...: Ingenta Connect.” *Journal of Security Operations & Custody* 9 (3). https://www.ingentaconnect.com/content/hsp/jsoc/2017/00000009/00000003/art00002?utm_source=TrendMD&utm_medium=cpc&utm_campaign=Journal_of_Securities_Operations_%2526_Custody_TrendMD_0.

Golumbia, David. 2016. *The Politics of Bitcoin: Software as Right-Wing Extremism*. U of Minnesota Press.

Greenberg, Andy. 2020. “Feds Seize $1 Billion in Stolen Silk Road Bitcoins .” *Wired*, May 11, 2020. https://www.wired.com/story/feds-seize-billion-stolen-silk-road-bitcoin/.

Harz, Dominik, and William Knottenbelt. 2018. “Towards Safer Smart Contracts: A Survey of Languages and Verification Methods.” *Cryptography and Security*, September. http://arxiv.org/abs/1809.09805.

Hayes, Adam. 2015. “What Factors Give Cryptocurrencies Their Value: An Empirical Analysis.”

Herian, Robert. 2018. *Regulating Blockchain: Critical Perspectives in Law and Technology*. Routledge.

Hileman, Garrick, and Michel Rauchs. 2017. “Global Cryptocurrency Benchmarking Study.” *Cambridge Centre for Alternative Finance*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224.

HMRC. 2014. “Revenue and Customs Brief 9 Bitcoin and Other Cryptocurrencies. Policy.” London. https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies.

HMSO. 1830. “Statutes at Large ...: (29 v. in 32) Statutes or the United Kingdom, 1801-1... - Google Books.” 1830. https://www.google.co.uk/books/edition/Statutes_at_Large_29_v_in_32_Statutes_or/eK5qQAEWLiYC?hl=en&gbpv=1&pg=PA403&printsec=frontcover#v=onepage&q&f=false.

Hu, Yining, Madhusanka Liyanage, Ahsan Mansoor, Kanchana Thilakarathna, Guillaume Jourjon, and Aruna Seneviratne. 2018. “Blockchain-Based Smart Contracts-Applications and Challenges.” *ArXiv Preprint ArXiv:1810.04699*.

Huobi. 2021. “Huobi.Com - Bitcoin Exchange.” 2021. https://www.huobi.com/en-us/.

Inman, Philip. 2014. “Bitcoin Could Pose Threat to Financial Stability of UK.” The Guardian. 2014. https://www.theguardian.com/technology/2014/sep/11/bitcoin-threat-financial-stability-uk-bank-of-england.

Ioannou, Llias. 2020. “Legal Regulation of Virtual Currencies: Illicit Activities and Current Developments in the Realm of Payment Systems.” *UCL Centre for Blockchain Technology* 3.

Jack, William, and Tavneet Suri. 2011. “Mobile Money: The Economics of M-PESA.” National Bureau of Economic Research.

Jopson, Barney. 2016. “Regulators Say Bitcoin Poses a Threat to Financial Stability.” *Financial Times*, 2016. https://www.ft.com/content/e0880cf6-3800-11e6-9a05-82a9b15a8ee7.

Kaal, Wulf, and C Calcaterra. 2018. “Crypto Transaction Dispute Resolution on JSTOR.” *American Bar Association* 73 (1). https://www.jstor.org/stable/26419193.

Kahya, Ayten, Bhaskar Krishnamachari, and Seokgu O Yun. n.d. “Reducing the Volatility of Cryptocurrencies-A Survey of Stablecoins.”

Kakavand, Hossein, Nicolette Kost De Sevres, and Bart Chilton. 2017. “The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.” *SSRN Electronic Journal*, June. https://doi.org/10.2139/ssrn.2849251.

Karpunina, Evgeniya K., Sergey N. Yashin, Alexey S. Molchan, Ekaterina V. Lisova, and Elena A. Derkacheva. 2020. “The Price of Pleasure: The Challenges and Threats of the Digital Economy.” In *Lecture Notes in Networks and Systems*, 111:363–73. Springer. https://doi.org/10.1007/978-3-030-39797-5_37.

Katsiampa, Paraskevi. 2019. “An Empirical Investigation of Volatility Dynamics in the Cryptocurrency Market.” *Research in International Business and Finance* 50 (December): 322–35.

https://doi.org/10.1016/j.ribaf.2019.06.004.

Kharif, Olga. 2021. “Bitcoin (BTC USD) Cryptocurrency Price Rise Leads $2 Trillion Crypto Market Cap.” *Bloomberg*, April 2021. https://www.bloomberg.com/news/articles/2021-04-05/crypto-market-cap-doubles-past-2-trillion-after-two-month-surge.

Kottasova, Ivanna. 2018. “Bitcoin Is Too Hot for Criminals. They’re Using Monero Instead.” CNN. January 3, 2018. https://money.cnn.com/2018/01/03/technology/bitcoin-popularity-criminals-monero/index.html.

Koutsouri, Aikaterini, Francesco Poli, Elise Alfieri, Michael Petch, Walter Distaso, and William J. Knottenbelt. 2020. “Balancing Cryptoassets and Gold: A Weighted-Risk-Contribution Index for the Alternative Asset Space.” In *Mathematical Research for Blockchain Economy*, 217–32. Springer. https://doi.org/10.1007/978-3-030-37110-4_15.

Kynaston, David. 1995. *The Bank of England : Money, Power and Influence 1694-1994*. Edited by David. Roberts, Richard and Kynaston. 2nd ed. New York: Oxford University Press.

Lammer, T, J Garcia, and S Polverini. 2016. “Establishing Payments Interoperability: Coordination Is Key.” World Bank. September 26, 2016. https://blogs.worldbank.org/psd/establishing-payments-interoperability-coordination-key.

Lee, Adrian D., Mengling Li, and Huanhuan Zheng. 2020. “Bitcoin: Speculative Asset or Innovative Technology?” *Journal of International Financial Markets, Institutions and Money* 67 (July): 101209. https://doi.org/10.1016/j.intfin.2020.101209.

Lee, Charlie. 2011. “Litecoin Whitepaper .” https://whitepaper.io/document/683/litecoin-whitepaper.

Lemahieu, Colin. n.d. “Nano: A Feeless Distributed Cryptocurrency Network.”

Li, Yannan, Willy Susilo, Guomin Yang, Yong Yu, Xiaojiang Du, Dongxi Liu, and Nadra Guizani. 2019. “Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies.” *IEEE Network* 33 (5): 111–17. https://doi.org/10.1109/MNET.2019.1800271.

Lianos, Ioannis, Philipp Hacker, Stefan Eich, and Georgios Dimitropoulos. 2019. *Regulating Blockchain: Techno-Social and Legal Challenges*. Oxford University Press.

Liu, Jinan, and Apostolos Serletis. 2019. “Volatility in the Cryptocurrency Market.” *Open Economies Review* 30 (4): 779–811. https://doi.org/10.1007/s11079-019-09547-5.

Makore, Mildred P. n.d. “Exploring Use of Mobile Banking Services by the Poor: Case of Wizzit Bank,

South Africa."

Manyika, James. 2016. "Digital Economy:Trends, Opportunities and Challenges."

Marley, Nathan. 2018. "Whitepaper · Dashpay/Dash Wiki ." Github. August 23, 2018. https://github.com/dashpay/dash/wiki/Whitepaper.

Martin, James, Jack Cunliffe, and Rasmus Munksgaard. 2019. *Cryptomarkets: A Research Companion*. Emerald Group Publishing. http://sdc-evs.ebscohost.com/EbscoViewerService/print?an=2255567&db=nlebk&format=EB&lang=eng&ppIds=[%22pp_22%22,%22pp_23%22,%22pp_24%22,%22pp_25%22,%22pp_26%22,%22pp_27%22,%22pp_28%22,%22pp_29%22,%22pp_30%22,%22pp_31%22,%22pp_32%22,%22pp_33%22,%22pp_34%22.

Maurer, Bill. 2008. "Retail Electronic Payments Systems for Value Transfers in the Developing World." *Department of Anthropology, University of California*.

———. 2015. *How Would You like to Pay?: How Technology Is Changing the Future of Money*. Duke University Press.

McCoy, Mason, and Shahram Rahimi. 2020. "Prediction of Highly Volatile Cryptocurrency Prices Using Social Media." *International Journal of Computational Intelligence and Applications* 19 (04): 2050025.

McLeay, Michael, Amar Radia, and Ryland Thomas. 2014. "Money in the Modern Economy: An Introduction." *Bank of England Quarterly* 1 (March). https://papers.ssrn.com/abstract=2416229.

McMahon, Kathryn. 2020. "Competition Law of the EU and UK." HeinOnline.

Morgan, E Victor. 1965. *The Theory and Practice of Central Banking, 1797-1913*. Psychology Press.

Nabilou, Hossein. 2020. "Bitcoin Governance as a Decentralized Financial Market Infrastructure." *UCL Centre for Blockchain Technology* 3.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

Nano. n.d. "Nano | Digital Money for the Modern World." Accessed June 26, 2021. https://nano.org/.

Nasdaq. 2018. "Which Cryptocurrencies Have the Lowest Transaction Fees? | Nasdaq." *Nasdaq*, March 30, 2018. https://www.nasdaq.com/articles/which-cryptocurrencies-have-lowest-

transaction-fees-2018-03-30.

Nica, Octavian, Karolina Piotrowska, and Klaus Reiner Schenk-Hoppp. 2017. “Cryptocurrencies: Economic Benefits and Risks.” *SSRN Electronic Journal*, November. https://doi.org/10.2139/ssrn.3059856.

Nseke, Pisso. 2018. “How Crypto-Currency Can Decrypt the Global Digital Divide: Bitcoins a Means for African Emergence.” *INTERNATIONAL JOURNAL OF INNOVATION AND ECONOMIC DEVELOPMENT* 3 (6): 61–70. https://doi.org/10.18775/ijied.1849-7551-7020.2015.36.2005.

Pablo, Urbiola, Lucia Pacheco, and Jesus Lozano. 2021. “Innovation and Competition in Payments: Evolving Policy Challenge...: Ingenta Connect.” *Journal of Payments Strategy & Systems* 1: 54–66. https://www.ingentaconnect.com/content/hsp/jpss/2021/00000015/00000001/art00005.

Perkins, Joanna, and Jennifer Enwezor. 2016. “The Legal Aspect of Virtual Currencies.” *Butterworths Journal of International Banking and Financial Law*.

Perlman, Leon. 2019. “A Model Crypto-Asset Regulatory Framework.” *SSRN Electronic Journal*, May. https://doi.org/10.2139/ssrn.3370679.

Poncibò, Cristina. 2021. “Blockchain and Comparative Law.” In *Blockchain, Law and Governance*, 137–56. Springer.

Presthus, Wanda, and Nicholas Owen O’Malley. 2017. “Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency.” In *Procedia Computer Science*, 121:89–97. Elsevier B.V. https://doi.org/10.1016/j.procs.2017.11.013.

Rapoza, Kenneth. 2021. “In The DeFi Winter, ‘Stable Coins’ Looking Safer For Yield Investors.” Forbes. June 8, 2021. https://www.forbes.com/sites/kenrapoza/2021/06/08/in-the-defi-winter-stable-coins-looking-safer-for-yield-investors/?sh=7cd32cf37727.

Ripple. n.d. “Global Payment Solutions - Instant Processing | Ripple.” Accessed June 26, 2021. https://ripple.com/.

Rothbard, Murray Newton. 2012. *The Mystery of Banking*. Alabama: Ludwig Von Mises Institute.

Saiedi, Ed, Anders Broström, and Felipe Ruiz. 2021. “Global Drivers of Cryptocurrency Infrastructure Adoption.” *Small Business Economics* 57 (1): 353–406. https://doi.org/10.1007/s11187-019-00309-8.

Salvo, Mathew Di. 2019. “Why Are Venezuelans Seeking Refuge in Crypto-Currencies?” *BBC*, March 19, 2019. https://www.bbc.co.uk/news/business-47553048.

Seyfang, Gill. 2010. “The Euro, the Pound and the Shell in Our Pockets: Rationales for Complementary Currencies in a Global Economy.” *New Political Economy* 5 (2): 227–46. https://doi.org/10.1080/713687774.

Singh, Amritraj, Reza M. Parizi, Qi Zhang, Kim Kwang Raymond Choo, and Ali Dehghantanha. 2020. “Blockchain Smart Contracts Formalization: Approaches and Challenges to Address Vulnerabilities.” *Computers and Security* 88 (January): 101654. https://doi.org/10.1016/j.cose.2019.101654.

Skingsley, Cecilia. 2017. “How the Riksbank Encourages Innovation in the Retail Payments Market.” In *Annales Des Mines-Realites Industrielles*, 5–6. FFE.

SourceForge. 2021. “Best Crypto Lending (DeFi) Platforms - 2021 Reviews & Comparison.” 2021. https://sourceforge.net/software/crypto-lending-defi/.

Sovbetov, Yhlas, and Y Sovbetov. 2018. “Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero Journal of Economics and Financial Analysis.” *Journal of Economics and Financial Analysis* 2 (2): 1–27. https://doi.org/10.1991/jefa.v2i2.a16.

Taskinsoy, John. 2019. “Blockchain: Moving Beyond Bitcoin into a Digitalized World.” *Article in SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3471413.

Teichmann, Fabian Maximilian Johannes. 2018. “Financing Terrorism through Cryptocurrencies – a Danger for Europe?” *Journal of Money Laundering Control* 21 (4): 513–19. https://doi.org/10.1108/JMLC-06-2017-0024.

The Bank of England. n.d. “Bank of England: About Us.” Accessed March 20, 2019. https://www.bankofengland.co.uk/about.

———. 1969. “The Bank of England Note - A Short History.” London. file:///C:/Users/Kelly-Ann Coulter/Desktop/FEBRUARY 2019/the bank of england a short history.pdf.

Tokenlon. 2021. “Tokenlon Official Website | Trustless Token - to - Token Exchange, Based on the 0x Protocol.” 2021. https://tokenlon.im/.

Treasury Committee, House of Commons. 2018. “Crypto-Assets Twenty-Second Report of Session 2017-19 Report.” London. www.parliament.uk/treascom.

Treasury, HM. 2020. “Financial Services Future Regulatory Framework Review Phase II Consultation.”

Uniswap. 2021. “Uniswap | Home.” 2021. https://uniswap.org/.

Vadgama, Nikhil, and Paolo Tasca. 2020. “An Analysis of Blockchain Adoption in Supply Chains Between 2010 and 2020.” *UCL Centre for Blockchain Technologies* 3 (September).

Walch, Angela. 2019. “In Code (Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains.” https://doi.org/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198.

Wegberg, Rolf van, Jan Jaap Oerlemans, and Oskar van Deventer. 2018. “Bitcoin Money Laundering: Mixed Results?: An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin.” *Journal of Financial Crime* 25 (2): 419–35. https://doi.org/10.1108/JFC-11-2016-0067.

Wintermeyer, Lawrence. 2021. “After Growing 88x In A Year, Where Does DeFi Go From Here?” *Forbes*, May 20, 2021. https://www.forbes.com/sites/lawrencewintermeyer/2021/05/20/after-growing-88x-in-a-year-where-does-defi-go-from-here/?sh=2f0d70a274ce.

Wright, Aaron, and Primavera De Filippi. 2015. “Decentralized Blockchain Technology and the Rise of Lex Cryptographia.” *Available at SSRN 2580664*.

Yermack, David. 2015. “Is Bitcoin a Real Currency? An Economic Appraisal.” In *Handbook of Digital Currency*, 31–43. Elsevier.

Yi, Shuyue, Zishuang Xu, and Gang Jin Wang. 2018. “Volatility Connectedness in the Cryptocurrency Market: Is Bitcoin a Dominant Cryptocurrency?” *International Review of Financial Analysis* 60 (November): 98–114. https://doi.org/10.1016/j.irfa.2018.08.012.

# Discussion Paper #3

## Regulating Financial Innovation: DLT Potential and Promise for Financial Market Infrastructures (FMIs)

*Pavel Kulikov*

Researcher

Swiss Institute of Comparative Law (ISDC)

**Abstract**

The current worldwide banking and financial markets regulation updates are widely seen as an important milestone in the evolution of global financial stability and market confidence in a move forward to re-establish full global banking and efficient financial market functioning. Technology plays a unique role in this regulatory transformation becoming more and more observed in various spheres of increasingly digitized financial markets. It is seen more and more in everyday banking, central bank settlements, clearing and settlement of assets, trade of derivatives and many other fields. A persistent theme of this paper is the currently changing approaches to regulation of technological risks following a rapid transition to the wholesale level leveraging and mass-adoption of technologies on financial markets. Following an introduction to emerging technologies on the financial market, this paper looks at various factors behind currently changing regulatory paradigm, as well as blockchain's structure and promise for Financial Market Infrastructures (FMIs), including new and alternative settlement models which become available on DLT.

**Keywords**: DLT, FMI, Risk Regulation and Management, Dominant Design, 4 IR, Regulated Industries.

# Regulating Financial Innovation: DLT Potential and Promise for Financial Market Infrastructures (FMIs)

PAVEL KULIKOV[1*]

The current worldwide banking and financial markets regulation updates are widely seen as an important milestone in the evolution of global financial stability and market confidence in a move forward to re-establish full global banking and efficient financial market functioning. Technology plays a unique role in this regulatory transformation becoming more and more observed in various spheres of increasingly digitized financial markets. It is seen more and more in everyday banking, central bank settlements, clearing and settlement of assets, trade of derivatives and many other fields. A persistent theme of this paper is the currently changing approaches to regulation of technological risks following a rapid transition to the wholesale level leveraging and mass-adoption of technologies on financial markets. Following an introduction to emerging technologies on the financial market, this paper looks at various factors behind currently changing regulatory paradigm, as well as blockchain's structure and promise for Financial Market Infrastructures (FMIs), including new and alternative settlement models which become available on DLT.

**JEL codes: K20, K23.**
**Keywords: DLT, FMI, Risk Regulation and Management, Dominant Design, 4 IR, Regulated Industries.**

## I. Introduction

The first examples of leveraging technological solutions on the financial market go as far back as the 1850s, when the pantelegraph was invented.[2] Following the introduction of Quotron in 1960 – the first product allowing stockbrokers to receive up-to-the-minute prices for securities on a screen rather than on a printed ticker tape,[3] A revolutionary transition from physical to electronic trade of National Association of Securities Dealers Automated Quotations (NASDAQ) took place in 1971 significantly transforming the global stock market by abolishing fixed securities commissions significantly modernizing the preexisting IPO market.[4] Since that time, the role of technologies and innovations on the market has been constantly increasing in parallel to the computational power growth.[5] Innovative

[1*] Researcher at Swiss Institute of Comparative Law (ISDC), pavel.kulikov@unil.ch.

[2] In 1850s a device known as pantelegraph was invented by Giovanni Caseli. This was an early form of facsimile machine used predominantly to verify signatures in banking transactions by sending and receiving transmissions on telegraph cables. Being extremely slow, a sheet of paper with 25 words took about 108 seconds to transmit, the invention is widely considered to be the first step towards the financial services as we know them today https://en.wikipedia.org/wiki/Pantelegraph#:~:text=The%20pantelegraph%20(Italian%3A%20pantelegrafo%3B,device%20to%20enter%20practical%20service. (Last accessed on 21 July, 2020).

[3] https://en.wikipedia.org/wiki/Quotron (Last assessed on 21 July, 2020).

[4] The IPO market has been in existence in the US from 1935, long before the NASDAQ was formed. For an extensive overview of IPO performance from 1935 to 1972, *see, e.g.,* Gompres P. and J. Lerner (2003). "The Really Long Run Performance of Initial Public Offerings: The Pre-Nasdaq Experience" in *The Journal of Finance* Vol. 58 4, 2003.

[5] As transistors in integrated circuits (IC) become more efficient, computers become smaller and faster. In 1965, Gordon E. Moore, future co-founder of Intel, presented his scholarly paper titled "Cramming More Components onto Integrated Circuits" stating that the minimum costs for IC would fall dramatically in five years, and that a

technologies, such as digital identity[6], artificial intelligence[7], distributed ledger technology (DLT) and blockchains[8], smart contracts[9], among others, are often commonly referred to as "FinTech" or Financial Technologies. Described in broad terms, these are technological solutions enabling innovations for financial services and products on one of the most regulated parts of the global economy, - the financial sector. It is highly certain that application of these technologies, especially the cross-cutting, enabling technologies, such as DLT, would be beneficial for the market, where financial assets are traded, - financial market. The past decades have seen the vast majority of technological advances successfully contribute to the appearance of new business models on financial market, such as robo advisers[10] on the retail market. Development of innovations and technologies have also been behind a high-paced digitalization of traditional enterprises that provide financial services – financial institutions and, particularly, financial intermediaries, such as banks. According to Puschmann and Weber, digitalization of the banking sector went through the stages of: (i) internal digitalization, concentrating more on internal processes, such as portfolio management providing necessary automation of financial services, (ii) provider-oriented digitalization, mostly focused on standardization of processes for integration of core banking systems, and (iii) customer-oriented digitalization, which is characterized by the customer-centered approach including a more active application of IT advances, such as smart-phones and cloud computing systems.[11]

With technologies getting a more profound acknowledgement on the market, the public perception towards the associated risks is getting changed as well, requiring, in most cases, new approaches to evaluation of regulation, including risk management. It seems that this being one of the most important consequences of transition from nearly purely

---

sharp increase in the amount of components per circuit should be expected. In 1975 he formalised the concept predicting that the number of IC components would double every two years. This observation later became known as Moore's Law.

[6] *See* Arner D., D.Zetzsche, R.Buckley and J.Barberis (2018). *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, EBI Working Paper Series No. 28 (stating that there are four types of digital identity: (i) physical; (ii) legal identity; (iii) electronic identity; and (iv) behavioural identity, as well as there are two states as static and dynamic digital identity).

[7] *See* Guice G., D. Schaffner, E. Pagano and H.C. Rickhoff (2019). "Policymakers Focusing on Artificial Intelligence" in *The Journal of Robotics, Artificial Intelligence & Law*, Vol.2, No.2, March-April 2019.

[8] *See* De Filippi P. and A. Wright (2018) *Blockchain and the Law. The Rule of Code*. Harvard University Press. Zetzsche D, R. Buckley, D. Arner and A. Didenko (2019). "Liabilities Associated With Distributed Ledgers: A Comparative Analysis" in Madir, eds, *Fintech Law and Regulation,*Elgar FLP, 185-208

[9] *See* Clack, C., V. Bakshi, and L. Braine. (2016). *Smart Contract Templates: foundations, design landscape and research directions*, Position paper (Discussing practical contribution of relevance to financial institutions); Nick Szabo (1997) *Smart Contracts: Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY, [https://perma.cc/ZV4X-X8Y5] (proposing that many contractual clauses can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive – the basic idea of smart contracts) (last assessed on 07 September, 2020).

[10] See International Organization of Securities Commissions (IOSCO) (2017). *Research Report on Financial Technologies (Fintech)*, (observing that robo-advisers utilize algorithms to construct, manage and rebalance investment portfolios, typically using a pre-determined mix of exchange-traded funds (ETFs) to build low-cost, diversified, and liquid portfolios tailored to the investor's objectives). *See* also R. Weber (2019). Robo Advise, UFSP Jahrestagung, Zürich, 5. Juni 2019 (suggesting further possible qualification of robo advise by distinguishing between: (i) entrepreneurial or enterprise robo advise; (ii) fully automated or a hybrid one; and also qualifying it (iii) depending on the programs used by clients/intermediaries).

[11] Puschmann, T. and Weber, R. (2017). "Neuerfindung des Finanzsektors?" in *Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht* (SZW) 89 (1), 79–94.

voluntarily to a more systematic level of technology leveraging. Perhaps, another reason behind it is that prior to the crisis, financial innovations were viewed by industrialized countries solely as mitigating the associated risks instead of enhancing it.[12] However, innovation in financial products led to the creation of credit-linked instruments that generated high levels of leverage thus putting the financial system at great risk.[13] Alternative trading systems involving algorithmic trading and other types of high-frequency trading may have also been used abusively, which, in turn, resulted in systemic shocks.[14] On the positive side, though, advances in technology contributed to further advancement of liberalization of trade in financial services and simplified the cross-border operations.[15]

Prolific regulatory reforms implemented aftermath of the Global Financial Crisis (GFC) have caused some of the most dramatic regulatory changes and, nowadays, regulation of the financial market as well as financial institutions, which are, in other words, enterprises that provide financial services through performing the three main functions of: (i) transformation of financial assets; (ii) broker-dealer services; and (iii) asset management, represents more than a complex system of regulation with much of legislative and political debates involved. According to the functions mentioned above, it is common to distinguish between the following three types of financial institutions, which are active on the market: (i) financial intermediaries, (ii) investment firms and (iii) asset managers,[16] which are complemented with a special type of financial institution - Financial Market Infrastructures (FMI), whose relevance in ensuring the markets stability is particularly on the rise in the last decades.[17] Today, an idea, which is broadly shared, is that technologies could take hold in various fields of today's *complex financial market*.

## II. Technology in Finance - An Elementary Subsystem?

Financial markets originally were modelled as linear systems.[18] However, financial markets nowadays are increasingly global without a single point of control, unpredictable by means of nonlinear feedback effects arising from interactivities among market participants[19] and tend

[12] Brummer C. and M. Smallcomb (2015). "Institutional Design. The International Architecture" in *The Oxford Handbook of Financial Regulation*, 145. Oxford.
[13] Alexander K. (2012). "Market Structures, Technology and European Securities Regulation" in *Finanzmärkte Im Banne Von Big Data*, 33. Schulthess, Zurich.
[14] *Ibid*, 33.
[15] *See* Alexander K, Eatwell J., Persaud, A. and Reoch, R (2007). *Financial Supervision and Crisis Management in the EU*. European Parliament, Brussels, 37.
[16] See *generally* Fabozzi F., F. Modigliani, and F. Jones (2014). *Foundations of Financial Markets and Institutions*, Pearson, 4th Ed.; Busch D., G. Ferrarini, G.v Solinge (2019) *Governance of Financial Institutions*, Oxford.
[17] Ferrarini G and P. Sagato (2015). "Regulating Financial Market Infrastructures", in *The Oxford Handbook of Financial Regulation*, 568.
[18] But *see* Schwartz S. (2009). "Regulating Complexity in Financial Markets" in Washington University Law Review, Vol. 87, N2, 211-268 (pointing out that highly unlikely the efficient capital market hypothesis (EMH) and the random walk theory are validly describe markets for complex debt securities).
[19] *Ibid* (Schwartz, 2009) (When financial markets exhibit properties of a complex system, the ability to predict consequences, such as cause-and-effect explanations for market movements, is frustrated by nonlinear feedback effects arising from interactivities among market participants), citing Johnson N., Jefferies P. and Hui P. (2003). *Financial Market Complexity* 4. *See* also Hazen T (1991*), The Short-Term/Long-Term Dichotomy and Investment Theory: Implications for Securities Market Regulation and for Corporate Law*. 70 N.C. L. REv. 137; Bookstaber R. (2007). *A Demon Of Our Own Design: Markets, Hedge Funds and the Perils of Financial Innovation.*

towards self-organized behavior. There appears to be a convergence that the modern financial market represents an example of a complex system. This **complexity of financial market,** from my standpoint, can be better described as arising out of investor demand[20] and subsequently existing in a highly interconnected system of subsystems present on *the factor market,*[21] - market for financial assets. This *organized complexity* of the financial market, first of all, is attributed to the properties of its parts that initially look simple and the laws of their interpretation as not allowing to infer the properties of the whole. As *Herbert Simon* famously noted justifying frequency with which complexity takes the form of hierarchy: [22] "[I]n most systems in nature, it is somewhat arbitrary as to where we leave off the partitioning, and what subsystems we take as elementary. Physics makes much use of the concept of "elementary particle" although particles have a disconcerting tendency not to remain elementary very long. Only a couple of generations ago, the atoms themselves were elementary particles; today, to the nuclear physicist they are complex systems…[J]ust why a scientist has a right to treat as elementary a subsystem that is in fact exceedingly complex is one of the questions..". It is common to distinguish the following main types of complex financial markets: (i) formal stock exchanges; (ii) formal exchanges for futures and options; (iii) OTC markets; (iv) interbank deposit markets, foreign exchange markets and other money markets.[23] Some of the key regulatory deficiencies attributed to this complexity are *redistribution* and *excessive consumerism.*[24] Emerging technologies have particular promise and potential on these complex markets, as can be used, *inter alia*, for simplification of securities settlement and cross-border payments processing currently undertaken by the FMIs, financial market infrastructures intermediaries (FMIIs), *e.g* banks; and (iii) international financial market infrastructures (IFMIs), like Euroclear. As these are requiring, in its current mode, an increased reliance on a central ledger and higher level of involvement in managing the risks on behalf of the participants,[25] manifesting in high operational costs (OPEX). Mass-adoption of technologies of the Fourth Industrial Revolution (4IR) potentially could trigger an even larger than projected transition to a new taxonomy of regulation for financial institutions and the market itself. New technologies are enabling new concepts, systems and frameworks in finance, such as *(i)* Central Bank Digital Currencies (CBDC), which can be based on blockchain, but also on traditional computational architecture, *e.g.* "digital euro" (ECB, 2020); *(ii)* Smart Derivatives Contracts (SDC) aiming at application of smart contracts to the official documentation framework, such as that provided by the ISDA

[20] *Ibid* (referring to complexity in financial markets arising in response to demand by investors for securities to meet their investment criteria and their appetite for even higher yields as well as to facilitate the transfer and trading of risk to those who prefer to hold it, thus promoting efficiency).

[21] As generally being referred to as a place where the factors that are needed for production, such as labour and capital can be bought and sold; as opposed to *the product market*, which is a marketplace for the final goods and services.

[22] Herbert A. Simon (1962). "The Architecture of Complexity" in *Proceedings of the American Philosophical Society* Vol. 106, N6, 467-482.

[23] See generally Wood P. (2007). *Regulation of International Finance*, Sweet & Maxwell.

[24] Where *Redistribution* is a deficiency of regulation which involves a transfer of risk from individuals to financial firms willing to accept it effectively representing a hidden tax. *Excessive consumerism*, in turn, is a deficiency as the protection of consumer doctrine assumes that people are normally incompetent. *See* Wood P. (2007). *Ibid*, 32.

[25] Bank of International Settlements (BIS), Committee for Payments and Market Infrastructures (2017). *Distributed ledger technology in payment, clearing and settlement. An analytical framework*, 6.

or Swiss master agreement for OTC trades or *(iii)* Trading venues focusing on digital assets, such as *DLT Trading Facility.* Moving us closer towards achieving the new efficiency in analytic capabilities in finance, technologies also provide for data to be easily structured on blockchain, potentially advancing machine learning and hence improving the desired outputs.

It is predicted that in the foreseeable future the role of technology in finance would be exceeding the boundaries of an elementary subsystem, where its regulation would be designated to the market itself. The applications of technologies would not be mandatory limited to enabling new business opportunities fostering transparency and cost- and time-effective clearing and settlement mechanisms, e-money and digital payment services. It seems that future simplification and transformation of financial supervisory practices on the market is likewise within the reach of blockchains and other cross-cutting enabling technologies, commonly dubbed as the ABCD framework: Artificial intelligence ("AI"), Blockchain, Cloud and data ("Big Data"). As well as Machine Learning ("ML") and biometrics.

## III. Dominant Product Design on Financial Markets

The innovation lifecycle for financial technologies has now progressed from *fluid* towards a more *transitional* phase. As the figure 1 shows, the rate of product innovation in an industry or product class is highest during its formative years, the so-called the fluid phase, where within the rich mixture of experimentation and competition some center of gravity eventually forms in the shape of a *dominant product design*.[26] This is how *James Utterback* explains it in his monumental work "Mastering the Dynamics of Innovation":[27] "..[A] good example of the fluid phase is found in the yearly years of the automobile industry, when a bewildering variety of machines-including electric and steam-driven cars-emerged from the workshops of dozens of manufactures. Each hoped to capture the allegiance of the public with a novel new design and driver amenities; the great product variety of this period makes design innovation in the modern auto age seem sterile by comparison. During this fluid period of high product innovation, much less attention is given to the processes by which products are made, so the rate of process innovation is significantly less rapid".

[26] Utterback J. (1941), *Mastering the dynamics of innovation. How companies can seize opportunities in the face of technological change*, Harvard University Press, 1994 ed., 24. Further on *dominant design*: Utterback J. and W. Abernathy (1975), A Dynamic Model of Product and Process Innovation, 3(6) Omega.

[27] *Ibid* (Utterback, 1941) at xviii. Further on the topic: Utterback J. and W. Abernathy (1978). "Patterns of Industrial Innovation" in Technology Review, vol. 80, no 7, 40-47.

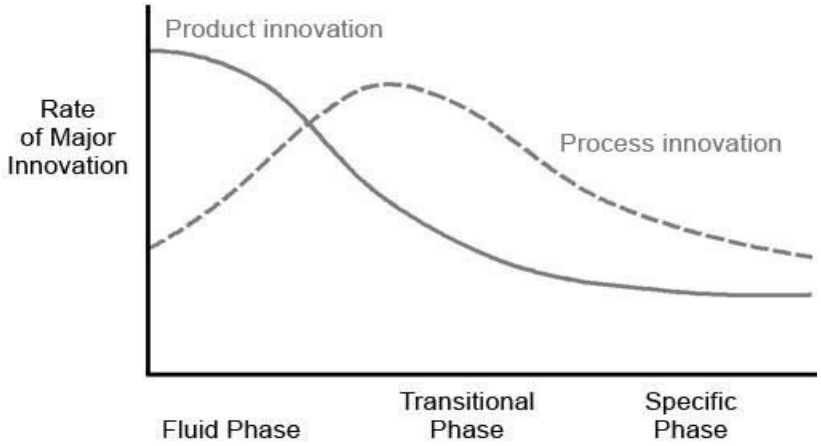



Figure1. The Dynamics of Innovation. Source: Utterback J. and W. Abernathy (1978)

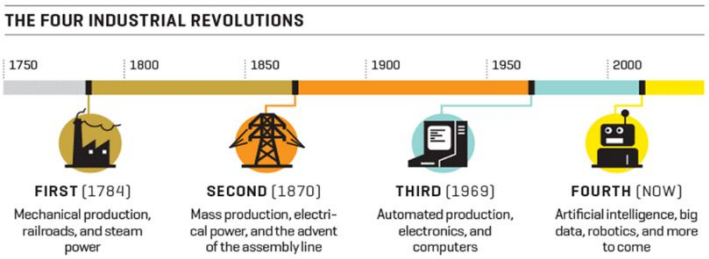
A dominant design as the landmark event for an industry (as hypothesized) has the effect of enforcing or encouraging standardization so that production or other complementary economies can be sought and perfected.[28] At the same time, it may not meet the needs of a particular class to quite the same extent as would a customized design, nor it is a dominant design necessarily the one that embodies the most extreme technical performance.[29] For example, the IBM PC, like the Model 5, offered the market little in the way of breakthrough technology, but it brought together familiar elements that had proven their value to users: a TV monitor, standard disk drive, QWERTY keyboard, the Intel 8088 chip, open architecture, and MS DOS operating system.[30]

As the ABCD framework of enabling technologies, used by FinTechs, TechFins[31] and RegTechs[32] is currently approaching the *dominant design* stage, their product design model is principally dictated by regulation, a pattern which is similar to most of the regulated industries, including the sector of finance,[33] I claim that new significance and rationale behind regulation on financial markets have now emerged, embracing acceleration of new forms of doing business on the market, - this trend becomes more and more commonly observed behind financial regulation in numerous countries. In Switzerland a new license category for trading venues focusing on digital assets was introduced - *DLT Trading Facility*,[34] effectively offering businesses to undertake both trade and post-trade activities under one license category (which differs significantly from the past regime where separate licenses were mandatory). The new license category also provides for access of both legal and natural persons to the trading facilities empowering them to run the OTF. What is interesting to observe in this trend, though, is the changing perception of the public towards the technological risks in conjunction with a close attention to possible negative externalities of

[28] *Ibid*, at 26, 32.
[29] *Ibid*, at 25.
[30] *Ibid*.
[31] See Zutzsche D, R. Buckley and D. Arner (2019). "The Rise of TechFins: Regulatory Challenges" in Madir, eds, *Fintech Law and Regulation,*Elgar FLP, 280-302. (defining TechFin as a technology company offering financial services and discussing, *inter alia*, the challenges that the shift from financial intermediary (FinTech) to data intermediary (TechFin) rises for incumbent traditional financial services institutions)
[32] See, *e.g.* Arner D., J. Barberis and R. Buckey, (2017). *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 (3) NW. J. INT'l L. & Bus. 371-414 (stating that "RegTech is a contraction of the terms regulatory and technology and it compromise the use of technology, particularly information technology, in the context of regulatory monitoring, reporting and compliance"), 373.
[33] See Dobrauz-Saldapenna G., D.Wirth (2016). «Five propositions for future success of Switzerland as a Financial Centre" in *Global Banking and Financial Policy Review,* 173-179.
[34] *DLT-Handelssystem*, a new proposed category of FMI under art.2 of the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Finanzmarktinfrastrukturgesetz, FinfraG), 958.1.

tech-enabled businesses by regulators (*e.g*. FINMA). The notion of Global Technology Risks (GTRs), which previously has not been an issue *en vogue*, is currently gaining pace, mandating changes to be made to regulatory approaches implemented worldwide. The general public, which generally tend to underestimate the risks stemming from voluntarily activities, as the utilization of technology has progressed from being purely voluntary, such as transferring bitcoins using blockchain more towards the wholesale level of tech utilization, *e.g.* Central Bank Digital Currency (CBDC) is becoming more and more aware of the upcoming risks requiring appropriate regulatory and supervisory response by regulators.

Risk assessment operating with categories of objective and subjective risks, generally helps regulators to avoid or minimize the related risks. At the same time, perceived (subjected) risk differs substantially from actual (objective) risk, as the former is usually under- or over- estimated in comparison to the latter. As human beings respond to hazards according to how they perceive it, understanding the perception of risk behind the regulatory paradigm for new technologies quickly becomes essential. As has been noted "[M]achines have altered the economics of the markets, and brought structural, sociological and psychological changes, which legal systems, whether modern or traditional, must take into account".[35] Undertaking effective risk-benefit trade-offs and, more generally, anticipating and adapting financial regulations to innovations, including enabling technologies, seems to require, first of all, a thorough understanding of the factors influencing regulatory decisions. Drawing on *Paul Slovic*,[36] I claim that there is a strong correlation between chosen regulatory approaches, including risk management framework development and how these technology risks are being perceived by the members of the general public. In accordance to the figure published in the *Science* journal in 1987, which became well-known and much cited worldwide, the location of known by that time to science 81 hazards on Factors 1 and 2 derived from the interrelations among 15 risk characteristics, such as: new or old risk; easily reduced or not; controllable or uncontrollable is provided (figure 3, p. 8). Mostly involuntarily, at this stage, the character of interactions with blockchain and other technologies,[37] collectively embraced under an umbrella of an actively ongoing the 4IR (Figure 2, p.7) significantly contributes to underassessing the associated risks. In accordance to *Chauncey Starr* research, the general public tends to accept risks from voluntary activities, such as skiing, that are roughly 1000 times as great as they would tolerate from involuntarily hazards (such as food preservatives) that provide the same level of benefits.[38] This paper argues that following transition to mass-adoption, wholesale level of technology leveraging,




[35]Zufferey J.B and M. Tschanz-Norton (1997). Regulation of Trading Systems on Financial Markets, 285.

[36] Slovic P. (1987). "Perception of Risk" in: *Science*, 236 (4799), 280-285. *See* also Slovic P. (2000). *The Perception of Risk*. Earthscan.

[37] Such as, advanced robotics, AI, autonomous systems, DLT (and various types of blockchains) and IoT. Kulikov P (2019). "Understanding the Digital Economy and the 4th Industrial Revolution: Focus on Law and Taxation", academic presentation at the *ISDC. Lausanne*, April 11, 2019 (on file with author).

[38] Starr C. (1969). "Social Benefits versus Technological Risk" in: *Science,* Vol. 165, 3899 (Sept. 19, 1969), 1232-1238.

overall demand for safety imposed by the society at large would be constantly increasing, at the same time, technology would be seen as less "sinister" risk in accordance to the increased scientific knowledge of its benefits. This would result in permanently challenging regulatory approaches to global risk and risk management agenda for emerging technologies in the future.

**Figure 2 - Location of 81 hazards on Factors 1 and 2 derived from the interrelationships among 15 risk characteristics. Each factor is made up of a combination of characteristics, as indicated by the lower diagram. Source: Slovic et al. (1985)**

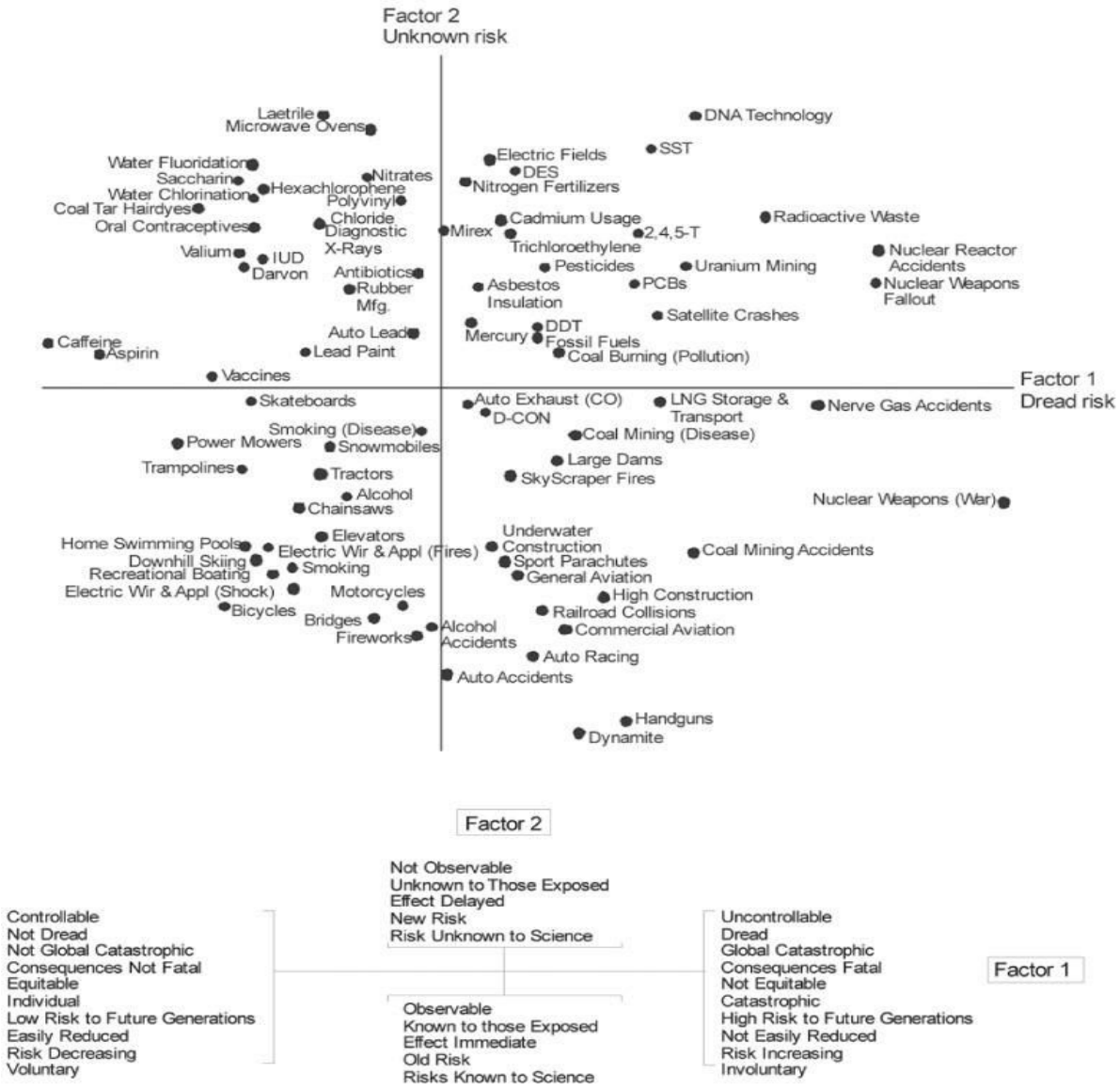



*Figure 3. Location of 81 hazards on Factors 1 and 2 derived from the interrelationship among 15 risk characteristics. Each factor is made up of a combination of characteristics, as indicated by the lower diagram. Source: Slovic 1987.*

In comparison to the past industrial revolutions, which **have not had a direct impact on banking and financial sector**, the currently unfolding 4IR has a direct influence and impact on the whole sector of global finance, which, as of today, is already one of the most

digitalised sectors of the global economy.[39] In the recent past, risk management issues related to technology on the market have been embraced under the category of operational risk, in turn recognized as one key form of financial risk, along with credit risk, market risk and legal risk. As a result of the rapid emergence of the 4IR, it is now widely believed that technology risks (including cyber security and data protection) should be seen as a separate form of risk, beyond the traditional operational risk categorization.[40] It seems that the deficiencies of the regulatory system with regard to Global Technology Risks (GTR) can be, at least to some extent, addressed by wider utilization of perception of risk studies in financial regulation. First, the concerns of the people should be the guiding principle for collective action (at least, as theorized in a democratic society). Secondly, any regulation ultimately involves and is based on risks trade-offs. Building financial regulations on rightly formed vectors of importance (when trading the risks) is effectively not possible without having a thorough understanding of these unchangeable vectors, which ultimately represent the peoples' willingness to undertake only a particularly determined set of activities. Thirdly, it is envisaged that more wider implementation of perception of risks in financial regulations would ultimately result in more quicker and effective identification of those points of concern when evaluating regulation, especially relevant in the current time of high demand to maintain business continuity under extreme stress conditions.

## IV. Evolution of the Regulatory Paradigm

### A. Systemic Risk and Transaction Costs

Regulation of technological advances in the post-crisis period with legislators choosing and applying one of the regulatory approaches or a combination thereof to ensure sound regulation of the market has quickly become one of the top issues on the global agenda. The approaches can be broadly described as following: (i) utilizing existing tools;[41] (ii) undertaking selective adjustments;[42] and (iii) introduction of new regulatory categories and mechanisms, such as those adopted in the US and being aimed at controlling the networks.[43] From a standpoint of a purely regulatory supervision of the market, it seems like a generally adopted view that regulators can take one of the following actions responding to a newly formed international agenda to foster financial inclusion as well as to public demand to support innovation, particularly digital financial disruption:[44] (i) stick to "doing nothing approach" resulting in permissive or *laissez-fair* depending upon whether current financial regulations apply to a particular business activity; (ii) taking on cautiously permissive approach based on forbearance, such as granting no-action letters, restricted licenses, special charters or partial exemptions for innovative firms, or established intermediaries testing new

[39] *Supra* note 36 (Kulikov, 2019).

[40] See, *e.g.* Buckley R., Avgouleas E. and D. Arner (2019) "Three Major Financial Crises: What Have We Learned?" in Arner D *et al*, *eds., Systemic Risk in the Financial Sector Ten Years After the Great Crash*, CIGI, Ontario Canada, 69.

[41] *E.g.* customer and investor protection aimed legislative provisions, rules on privacy, commodity exchange acts.

[42] E.g. DLT-Handelssystem, supra note 33.

[43] *E.g.* business license of virtual currency activities (BitLicense), issued by the New York State Department of Financial Services, - the NYDFS BitLicense regulatory framework. Regulations of the Superintendent of Financial Services, part 200: virtual currencies, 23 CRR-NY I 200 Notes.

[44] Zetzsche D., R.Buckley, J. Barberis, and D. Arner (2017), Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation, 23 FORDHAM J. CORP. & FIN. L. 31, 11-13.

technologies; (iii) fostering experimentation by instituting a regulatory sandbox or similar; and (iv) adopting a formal approach, in which existing regulations are reformed or new regulations are developed. Continued development of the DLT-powered products for financial market stakeholders, such as Corda,[45] would undoubtedly have a profound impact on the pace of legislative development in the foreseeable future, manifesting in numerous supervisory changes for internal (*domestic and foreign*) and external (*Euromarket*) markets. The financial services industry these days has a once-in-a-generation opportunity to reimagine and modernize its infrastructure to address long-standing operational challenges[46] and technologies are continuing to increasingly contribute to change both in terms of the pace of regulation and the approach to it. In 2019, the International Organisation of Securities Commissions (IOSCO) recognized technology, together with risk management and financial compliance, as one of the top priorities and challenges for efficient financial market functioning; in turn, it has prioritized its future work to be focused on digitalization, artificial intelligence and machine learning.[47] Although regulation of financial technology and automation has been on IOSCO's agenda since 2016, never before technologies commonly embraced under the umbrella of currently ongoing the 4 IR were recognized as a major challenge for the efficient markets.[48] Ensuring a fair, efficient and transparent market undoubtedly remains important; interactions between regulation of technologies and the objectives of financial market regulation are getting more and more evident. Technologies can potentially contribute to the appearance of new emerging notions of supervision and significantly contribute to shaping a new paradigm of financial market regulation. In considering various new aspects of it, it is worth noting with regard to the objectives of market regulation in particular, that protection of the market functioning doctrine as that closely aligned to the notion of investor protection (as both have emerged from the 1970`s), has also been formulated only recently.[49] Although many efforts in the financial markets regulation have traditionally been focused on the reduction of systemic risk and transaction costs, these notions might also be consequently challenged by the rise of technological advances. Emerging technologies can potentially be treated as a separate type of micro-level risk, raising some necessary questions as to whether some revisions to the doctrine of systemic risk should be made to reflect, *inter alia*, on technologies and blockchains significantly contributing to an increased interconnectedness of market players and appearance of negative procyclical related effects on the market.

B. Self-Regulation

[45] Corda blog (2018). What is Corda? (Last assessed on 10 September, 2020).

[46] *E.g.* DTCC (2016). Embracing Disruption. Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape (noting that current netting efficiencies could effectively preclude cost- and risk-application of the ledger model settlements, which anywise is only relevant for only 3% of trades going through the full settlement mechanism), 16.

[47] See Proceedings of the 44th IOSCO Annual Meeting, Sydney, 13-17 May 2019. *See* also report from the Chair of the IOSCO Board, IOSCO Annual Report (2018) https://www.iosco.org/annual_reports/2018/toc.html (last visited on Jan. 4, 2019).

[48] See Board Priorities - IOSCO work program for 2019, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD625.pdf (last visited on Jan. 4, 2020).

[49] *See* Zufferey J.B. (1994), Le réglementation des systems sur les marches financiers secondaries, FR, at 149-150.

The international dimension of the development of financial markets from the late 1960s onwards and their increasingly global and complex character witnessed since the 1980s has been complemented by rapidly evolving self-regulation standards and other "soft law" in the recent decades, mostly as a result of domestic regulation became increasingly inadequate for addressing the challenges of cross-border, international and global financial markets and institutions.[50] Legal doctrine has developed a new notion of law, commonly called soft law, describing something situated between law traditionally introduced by a legislator (hard law) and no law.[51] It is hard to disagree that upon certain conditions being fulfilled, soft law is even reaching a higher level of compliance than traditional "legalistic" law making.[52] For example, self-regulation currently embraces, in addition to corporate governance *per se*, questions such as internal audit and the system of compliance standards and various risk management rules, which are having a particular relevance for derivatives CCPs imposing more complex in comparison to securities CCPs risk management rules, margining and collateral management systems.[53]

In discussing the characteristics of soft law, *Rolf Weber* has concluded that following the principle of *subsidiarity*, (meaning that governments only intervene if the participants of the concerned community are not able to find suitable solutions themselves), soft law has partly also been an "escape" since the globalization of the financial markets has undermined the authority and control of regulators.[54] Following these characteristics, numerous risks of soft law are becoming apparent. Since the "legislative" process of developing self-regulatory rules is not always transparent and not every relevant group is necessary involved in it, it has no advantage of democratic legitimacy (in comparison to hard law) as it does not implicate a previous legislative process;[55] also, non-compliance to soft law does not necessarily trigger legal sanctions.

The most prominent example of soft law in international financial law setting is financial regulatory agreements, such as the 1988 Basel Capital Accord (Basel I), and its replacements (Basel II, III and IV (or 3.5.). Despite the importance of soft law in finance (mostly due to the above-mentioned agreements as these has long been seen as an irrevocable part of crises response),[56] the lack of self-regulation management practices was almost never considered as the factor important enough to play a major role in the global financial crises. As *Rolf Weber* has emphasized, soft law does not suffice for avoiding detrimental developments.[57] However, there also seems to be a broad consensus that inadequate due diligence in self-regulation of

[50] *Supra* note 31 (Arner D., J. Barberis and R. Buckey, 2017), 385.
[51] Weber R. (2012). Overcoming The Hard/Soft Law Dichotomy in Times of (Financial) Crises, *The Journal of Governance and Regulation*, Vol.1, Issue 1, 11.
[52] *See* generally *Ibid,* (Weber R, 2012); Weber R. (2010). *New Rule-Making Elements For Financial Architecture's Reform*, J.I.B.L.R. 2010, 25(10), 512-521 (although, pointing out that: "[S]pontaneous self-regulation is justified if it is more efficient than state law and if compliance with rules of the community is less likely than compliance with self-regulation").
[53] This firstly was relevant for the US markets only; draws on *Lee* (*2011, chap.1*).
[54] *Supra* note 50. *See* also Brummer C. (2011). *How International Financial Law Works (and How it Doesn't)*, 99 Geo. L.J. 257 (international financial regulation, though formally "soft", is a unique species of cross-border cooperation bolstered by reputational, market, and institutional mechanisms that have been largely overlooked by theorists).
[55] *Supra* note 50 (Weber, 2012), 13.
[56] But see *Supra* note, 53 (Brummer, 2011) (although international financial law is "soft" in terms of its formality, it can in practice be quite "hard").
[57] *Supra* note 50 (Weber, 2012) (On the one hand, the recent financial crisis has shown that soft law does not suffice to avoid detrimental developments; on the other hand, a straight call for hard law would not be able to manage the recognized regulatory weaknesses).

derivatives in America has played some role in the GFC development.[58] Though, it is important to point out that this argument is often misused to support a rather limited view on a structure of institutionalized FMIs as a necessary precondition for ensuring global financial stability.

Following increased complexity within the market (as defined previously in section I), among other fields of human interactions the world has seen the appearance of *new governance* mechanisms aimed at responding to continual changes of regulated society and knowledge. Viewing all solutions to problems as provisional, (with no exclusion for innovatory concept of MPBR, discussed hereinafter), these mechanisms and tools were characterized by implying a strong public role for supervision and enforcement.[59]

C. Standardization

International standardization in emerging technologies and blockchains, as a quasi-legal form of self-regulation, can be beneficial for the stimulation of innovation facilitating mass adoption of technologies in business processes on the market.[60]

A distinction is made between public and private regulations or standards and technical regulation is often delegated to private standard-setting bodies and is enacted both domestically and internationally by these bodies,[61] such as the International Organization for Standardization (ISO). As technologies are now approaching the dominant design stage (*see* hereinbefore, section III), it seems critically important to ensure effective transformation from private standards adopted by companies and industries towards more public level technical regulation (international standardization).

I claim that a lack of consistency in the standardization of **financial innovations**, especially during the early stages of their development is, first of all, grounded in complexity of the market (as discussed hereinbefore in section I) and the chosen by the private stakeholders innovation strategies, often resulted in creating negative effects, *e.g.* **"socially useless" innovations**. These strategies are following the general pattern of broadly utilized commercial innovations, such as A/C charges, character encoding and instant messaging and might involve *artificially accelerating the pace of innovation* for the purpose of achieving the product differentiation. This includes between previous generations of their own products and innovations, which is similar to the short term "planned obsolescence" through innovation strategy observed within, inter alia, consumer electronics (such as Apple iPhone) and academic textbook industries.[62] The second possible strategy constitutes *embracing*

[58] *Supra* note 16 (Ferrarini G and P. Sagato, 2015).

[59] See generally Trubek D. and L. Trubek (2006), New Governance & Legal Regulation: Complementarity, Rivalry, and Transformation, COLUM. J. EUR. L. Vol. 13.

[60] *See* generally Delimatsis P (2019), "When Disruptive Meets Streamline: International Standardization In Blockchain" in D. Kraus *et al*, eds, *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law,* 83-100 (In the case of actively evolving technologies like distributed ledger technologies (DLT) and blockchain, standardization, as a quasi-legal from of self-regulation, can be adequate way to create some tentative, non-binding norms and thus a common vernacular in a new landscape whereby "harder" forms of law may have undesirable results in terms of stifling innovation or creating unwelcome barriers to entry; citing Brunson N. and B. Jacobsson, 2000). *See* also Cotter T (2017), *infra* note.

[61] Cottier T. (2017), "Technology And The Law Of International Trade Regulation" in Brownsword R. *et al*, eds, *The Oxford Handbook Of Law, Regulation And Technology* 1018-1051, 1020.

[62] *See* generally Mishkin F. (1990), *Financial Innovation and Current Trends in U.S. Financial Markets* (National Bureau of Economic Research, NBER Working Paper No. 3323); Tufano P. (2003), "Financial

*complexity as an integral component* of a particular financial business model. Here, following higher profit expectations or regulatory arbitrage considerations, financial intermediaries are moving a substantial part of their business activities into new and relatively non-transparent instruments and markets.[63]

It remains to be seen to what extent international standardization initiatives (*e.g.* ISO/TC 307 Blockchain and distributed ledger technologies, launched in 2016) would be able to address numerous challenges, such as data governance,[64] which preclude effective leveraging of emerging technologies, inclusive of the DLT. Nevertheless, it should be noted that standardization is clearly not a real prospect for the next 10-20 years to come.

## *V.* The Blockchain Structure

As the blend of several existing technologies, including peer-to-peer networks, public-private key cryptography, and consensus mechanisms, blockchains are, in many ways, the "tamper-proof boxes" envisioned by Timothy May, one of the founding members of the "cypherpunk" movement more than thirty years ago.[65] In the absence of a uniform definition, for some it is a database, for others a register, or an open ledger of information.[66] Underlying blockchain is distributed ledger technology, which is, from my standpoint, can be better defined as an enterprise software code with elements of cryptography and distributed systems, which is subsequently used to create a database – a distributed ledger. One of the most prominent examples of application of distributed ledger in finance is Corda by R3.[67] Blockchain, as one type of distributed ledger, is effectively a sequence of blocks. In this it differs from any other distributed ledger, as the data on the blockchain is being recorded and stored in blocks, while this pattern is not necessarily followed in a distributed ledger. In comparison to other distributed ledgers, which do not use the *consensus mechanism*, blockchain is using cryptography relying on decentralization-enabled unstoppable code (which is also the main instrument in hands of those willing to exit the legal system).[68] Existence of the general agreement, in this or another form, between the users to ensure its functioning is necessary. Most commonly used types of this agreement to follow a particular type of computational logic or the so-called *consensus mechanism* are Proof of Work, which is both the most common and computationally intensive consensus mechanism; first developed in the late 1990s it requires that certain computers on the network solve computationally intensive mathematical puzzles to determine which party's block will be

---

Innovation" in Constantinides G. *et al*, eds, *Handbook of The Economics of Finance*; Awrey D. (2012), *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HBLR. 235.

[63] *Ibid* (Awrey D, 2012).

[64] *See, e.g.,* Depository Trust & Clearing Corporation (DTTC) (Feb. 2020). Security of DLT Networks. A Distributed Ledger Technology Security Framework for the Financial Services Industry (Last visited Apr 04, 2020).

[65] *Supra* note 7 (De Filippi and Wright, 2018), 1-2,13.

[66] Kraus D. and C. Boulay (2019). "Blockchains: Aspects Of Intellectual Property Law" in D. Kraus *et al*, eds, *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, 242.

[67] Corda blog (2018). What is Corda? (Last assessed on 10 September, 2020).

[68] Lindmark R. (2019). *#CryptoEthics Concepts: Decentralization-Enabled Unstoppable Code* [https://perma.cc/3824-JFQQ]

considered next block in the chain;[69] Proof of Stake; Proof of Burn; Proof of Authority; Proof of Capacity and Proof of Storage. Consensus mechanism ensures that while not being centrally maintained, blockchain remains highly resilient and tamper-resistant allowing to store data in a transparent and nonrepudiable manner and engage in a variety of economic transactions pseudonymously.[70]

With all the hype surrounding blockchain, what is usually left behind is the actual scope of its contribution to science. Among all of its initial characteristics described above, it seems that **only immutability**, as the data on blockchain can only be written, but not modified or deleted,[71] truly fulfills the requirements of novelty and originality. However, some authors believe that the new thing about blockchain is the nature of the consensus, arguing that "immutability and finality are simply properties that one hopes will be the outcome of the consensus mechanism in place",[72] which can be viewed as a doubtful proposition, as proof-of-work or PoW, the ground and most popular protocol behind blockchains' immutability, was created with a purpose to combat junk mail long before the appearance of blockchain.[73] Another argument to support considering immutability independently of protocol is that immutability can also be achieved out of using protocol (though, in this case it is called *weaker immutability)*. Any blockchain without the guarantee of immutability would be competing with Amazon AWS (web services/cloud computing platform), which is already much more user friendly and a thousand times cheaper.[74]

It is possible to distinguish between different DLT topologies, such as: public (unrestricted or open; decentralized); private (restricted or closed; centralized), also known as *consortia;*[75] mixed and federated blockchains. One of the most well-known examples of public blockchain is Ethereum consortium.[76]

Figure 5 shows the relationship between various blockchain topologies and implied distribution of control. The growing interest in research on blockchain governance has subsequently led to numerous multidisciplinary publications addressing various aspects of

---

[69] Bonneau J. et al. (2015). *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE Security & Privacy (Oakland)[https://perma.cc/R8GK-TF5Q] (describing the process of choosing the new block as being that simple: the first announced valid block containing a solution to the computational puzzle is considered correct. Upon hearing of it, other participants are meant to begin working to find a follow-up block. If an announced block contains invalid transactions or is otherwise malformed, all other participants are meant to reject it and continue working until they have found a solution for a valid block. At any given time, the consensus blockchain is the "longest" version).

[70] *Supra* note 7 (De Filippi and Wright, 2018), 2.

[71] The very premise of a public blockchain topology is immutability, where no modification is possible (provided that the fork is not created).

[72] Andolfato D. (2018). Blockchain: What Is It: What It Does, And Why You Probably Don't Need One. Economic Research Division of Federal Reserve Bank of St. Louis, USA.

[73] C. Dwork, M.Naor (1993). "Pricing via Processing or Combatting Junk Mail" in E.F. Bnckell (Ed.): *Advances in Cryptology - CRYPT0 '92*, LNCS 740, pp. 139-147. [https://perma.cc/C92A-RGJ7]

[74] Artamonov I. (2018) Does Ethereum-Classic has any significance in terms of Technology?, Quora [https://perma.cc/G2KL-5J5N].

[75] *Supra* note 78, 246.

[76] www.etherium.org (last assessed on 10 September, 2020).

measurement of the relationships between a particular trust model of blockchain and decision-making process,[77] - a topic essentially important for blockchain in finance.

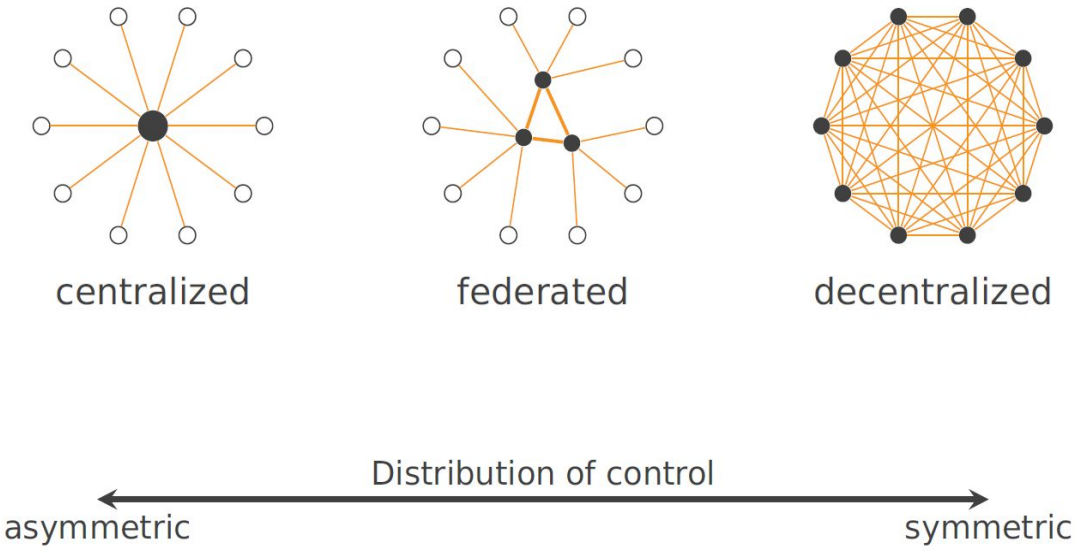



*Figure 5. Distribution of Control in Selected Style Topologies* *Source: Rainer Böhme (2019)*

[77] *E.g.* International Telecommunication Union (ITU-T) (2019). *Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework*.

## VI. DLT Potential and Promise for FMIs

### A) Introductory Overview

Financial market infrastructures (FMIs) are responsible for performing trading, clearing, settlement, depositing, as well as reporting and related functions (such as collateralization) on the market, commonly referred to as trade and post-trade processes. Trading is generally conducted on either regulated or "alternative" venues. Regulated (organized trading facility) venues are operated and/or managed by a market operator, which facilitates the bringing together of multiple third-party buying and selling interests in financial instruments in accordance with a set of non-discretionary rules that can lead to the formation of a contract in respect of the financial instruments that are admitted to trading under its rules and which is authorized and functions regularly,[78] *i.e.* it is a market operator (or a regulated market itself)[79] that manages a trading system, which is characterized by performing listings and self-regulation, as well as setting rules governing the conduct of subscribers. The most typical examples of regulated trading facilities are stock exchanges, futures and options exchanges. "Alternative" venues are typically electronic systems controlled by an approved market operator, which are often characterized by high trading speeds achieved by using technology. Typically, these are multilateral trading facilities (MTFs), termed as Alternative Trading Systems (ATSs) in North America[80] and Canada[81]. Trading on MTFs, in comparison to OTFs and systemic internalizers (see this section *infra*) is conducted in accordance with non-discretionary rules. Alternative trading venues are usually run by investment banks, such as UBS MTF for European Equities.[82]

Country differences in approaches to legal qualification of trading venues do exist. Swiss legal regime governing the trading venues, for example, identifies two types of trading venues: stock exchanges and the MTFs,[83] whereas under the EC legislation, three types of trading venues can be distinguished. In addition to stock exchanges and MTFs, the MiFIR and MiFID II[84] provided for inclusion of Organized Trading Facilities (OTFs) as one of the types thereof allowing trade in relation to bonds, structured finance products, emission allowances and derivatives. The main difference of OTFs in comparison to MTFs is that the former, in contrast to the latter, are matching the trades on a discretionary basis. However, similar to other "alternative venues", the OTFs are neither performing listing of securities, nor perform other functions usually attributed to regulated venues mentioned above. Systemic

[78] *See e.g.* Art. 4 (14) MiFID II (DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU). L 173/349.

[79] See, *e.g.* disposition of Art. 4 (13) MiFID II, *Ibid*.

[80] Rule 300 (a) Regulation ATS (17 CFR 242.300) under the Securities Exchange Act of 1934. The most widely known types of ATSs in America are: electronic communication networks, call markets, electronic trade matching, crossing networks, and dark pools.

[81] Art. 1.1. (a) National Instrument 21-101 Marketplace Operation (NI 21-101) and National Instrument 23-101 Trading Rules (NI 23-101). Except Ontario, where ATSs are defined in accordance to subsection 1(1) of the Securities Act, R.S.O 1990 c. S.5.

[82] https://www.ubs.com/global/en/investment-bank/multilateral-trading-facility.html (last assessed 11 September, 2020).

[83] Art. 26 (A) of Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) of 19 June, 2015. 958.1

[84] Art. 4 (24) MiFID II, *Supra* note 39 (Definition of OTF is given in Art. 4 (23).

internalizers (SIs) is yet another category that exist under the EC law. SIs had been considered as one of the three categories of trading venues before MiFID II was enacted.[85] Today SIs are rather counterparties on the financial market, which can be described, in broad terms, as investment firms executing client orders on their own account (in-house) on behalf of their accredited or wholesale customers outside the regulated market or MTFs, so long as the trades are executed on an "organized, frequent and systematic basis".[86] Trading on SIs, in most cases, involves displaying prices to one person only, lacking pre-trade transparency, that is why SIs are broadly considered as so-called "dark pool" operators.[87] This lacking transparency in their operations has been a subject of continuous attention from regulators worldwide for a number of years. In Europe, for example, SIs are subject to application of numerous transparency provisions under MiFIR,[88] which were further detailed in Commission Delegated Regulation.[89]

Additionally, all FMIs are subject to different regulatory regimes, therefore, it is common to distinguish between the following three broader groups of: (i) financial market infrastructures (FMIs), such as exchanges; (ii) financial market infrastructures intermediaries (FMIIs), *e.g* banks; and (iii) international financial market infrastructures (IFMIs), like Euroclear.

The Principles for Financial Market Infrastructures (PFMI) issued by BIS CPSS-IOSCO[90], is the main international standard-setting document aim to enhance the safety and efficiency in trade and post-trade services, to limit systemic risk and foster transparency and stability. PFMI identifies the following five types of FMIs with each of them playing a critical role in ensuring the integrity of the global financial markets:

1. PSs – Payment systems
2. CSDs– Central Securities Depositaries
3. SSSs- Securities Settlement Systems
4. CCPs- Central Counterparties
5. TRs- Trade Repositories.

[85] Three categories of trading venues (regulated markets, MTF and systemic internalizers) were introduced into the EC legislation in accordance to MiFID in 2004 (DIRECTIVE 2004/39/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC). OJ L 145, 30.4.2004.(No longer in force).

[86] *See* Alexander (2012), *Supra* note 12, at 35. For currently in force definition of "systemic internalizer", see Art. 4 (20) MiFID II. *Supra* note 90.

[87] On *SIs* managing "dark pools" of capital, *see* Kern (2012), *Ibid*. On increased transparency obligations of *SIs*, *see* European Securities and Markets Authority (ESMA) (2020). MiFIR Report On Systemic Internalizers In Non-Equity Instruments.

[88] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012. OJ L 173/84.

[89] Commission Delegated Regulation (EU) 2017/587 of 14 July on transparency requirements for trading venues and investment firms in respect of shares, depositary receipts, exchange-traded funds, certificates and other similar financial instruments and on transaction execution obligations in respect of certain shares on a trading venue or by a systematic internaliser. OJ L 87/387.

[90] BIS CPMI-IOSCO (2012). The Principles for Financial Market Infrastructures (PFMI).

Although, exchanges (and some other market infrastructures) were not explicitly included and governed by the PFMI, most of them, nonetheless, have to comply with the relevant principles thereof applicable to CSD or SSS in case they own or operate entities or perform functions of centralized clearing and settlement processes covered by the principles. Particularly, SIX SIS Ltd., as a systemically important CSD and operator of a securities settlement system has to comply with related PFMI principles regarding CSD and SSS.[91] (Swiss securities value chain represented on figure 6). Additionally, it is worth noting that national regulators may decide to apply some or all of these principles to those types of infrastructures, which are not formally covered by the PFMI.

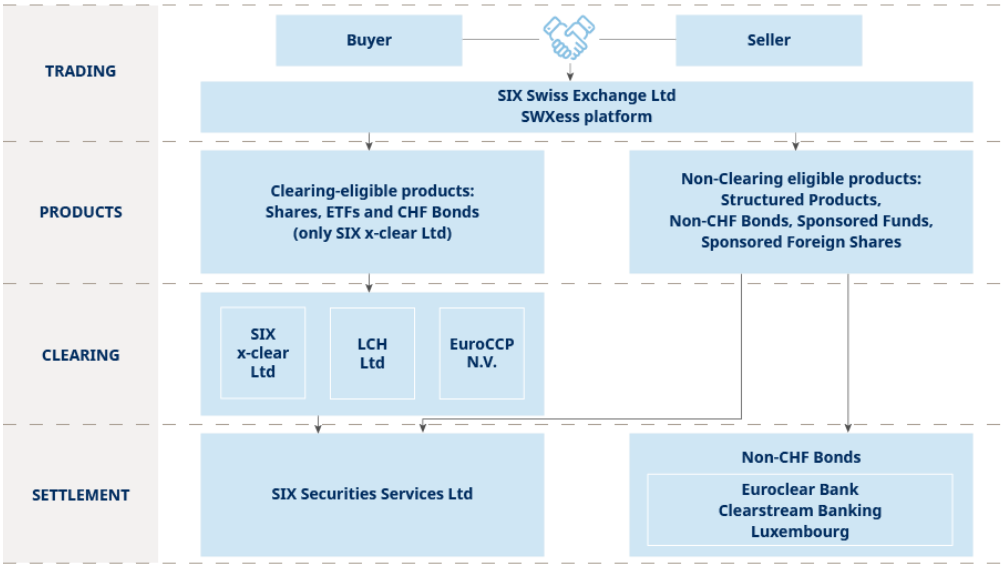



*Figure 6. Swiss Securities Value Chain* *Source: SIX*

B) FMIs Genesis

One of the early examples of the regulation of FMIs goes back to the end of the 19th century when a group of brokers organized the New York Stock and Exchange Board in 1817. Later, in 1865, the present title "The New York Stock Exchange" was adopted. From the early days its membership was limited, various rules of conduct were in place and it was within the boundaries of the Constitution[92] to regulate trading practices, necessary qualifications and stipulations for listings (Bernheim and Schneider, 1935). The regulatory system has been continuously evolving and, nowadays, regulation of FMIs represents more than a complex structure. An enhanced demand for listings, in conjunction with increased competition with domestic and foreign rivals has consequently induced in changes to exchanges' capital structure and fast-growing processes of their demutualization, pioneered by the Stockholm Stock Exchange and consequently spread all over the world. Since that time, numerous national and international mergers had occurred with the most notable being

[91] See *e.g.* SIX (2019). Disclosure of SIX SIS Ltd. Regarding The CPMI-IOSCO Principles For FMI In Accordance With "Disclosure Framework And Assessment Methodology".

[92] In 1925 the former Constitution and various rules of conduct (Resolutions) were transformed into a relatively compact Constitution, and Rules: *Constitution of the New York Stock Exchange – Rules Adopted by the Governing Committee Pursuant to the Constitution.*

the creation of SGX Singapore and merger of the NASDAQ with the OMX. Whereas the most recent example is all-cash tender offer for the operator of the Spanish stock exchanges (BME) made by the Swiss Infrastructure and Exchange (SIX) in the end of the last year in a bid to create one of the top European financial markets infrastructure group.[93] This acquisition has been finalized recently resulting in creation of the combined group which is now the third largest operator of financial market infrastructure in Europe by revenue.[94]

In modern times, the main trend in trading in securities is an increased reliance on "alternative types" of trading venues typically aiming at ensuring high trading speed via application of numerous sophisticated technologies and thus favoring high frequency trading. As the blockchain hype went down, many traditional trading venues, including exchanges and clearing houses are now started to consider DLT implementation, but in a rather different manner to that in the past, now no longer aimed at leveraging blockchain for building an entire complex system, but rather utilizing it as an extra layer to traditional infrastructure, as for securities lending. Some of these examples are discussed below.

C) Promise for Trade and Post-Trade Services

DLT can take hold in various processes in the securities industry value chain, including *pre-trade*, where research analytics and risk management is generally undertaken; *trade* with order entry into the trading system and its subsequent execution and *post-trade services* typically embracing services of clearing, settlement, custody and asset servicing, financing, accounting, administration, transfer, agency and also trustee and investor services.

According to the survey conducted by the World Federation of Exchanges (WFE) in 2016, the overwhelming majority of FMIs (21 out of 25 respondents), including SIX Stock Exchange, NASDAQ, Hong Kong Exchanges & Clearing Co. Ltd and Group Deutsche Börse, signaled that they were either investigating the applicability of DLT to their environment or actively pursuing DLT initiatives.[95] Numerous other reports has concluded that DLT could potentially bring numerous benefits to security markets, particularly, contributing to significant costs reduction and ensuring more efficient post-trade services while reducing the counterparty risks and enhancing collateral management practices.[96] The latest report produced by the European Central Bank (ECB) Advisory Group on Market Infrastructures for Securities and Collateral (AMI-SeCo) resolved that "DLT seems particularly "fit for purpose" for the post-trade processes, where sharing of a set of standardized information among different entities that are part of the securities chain is required, as it supports the set-up of a "single database", where information can be assessed

[93] SIX kündigt Barangebot für BME zur Schaffung eines europäischen Top-3 Finanzmarktinfrastruktur-anbieters an (18 November 2019) https://www.six-group.com/de/home/media/releases/2019/20191118-tender-offer-bme.html (last visited Nov. 18, 2019).

[94] SIX kauft Mehrheit an der spanischen Börse, Neue Züricher Zeitung (NZZ), June 11, 2020.

[95] World Federation of Exchanges (WEF) (2016). Financial Market Infrastructures and Distributed Ledger Technology, 4. (with respondents taking sharply different views on the DLT role in trade and post-trade business, some of the replies received pronounced that DLT has the potential to fully disrupt existing business models due to its pure technology replacement features).

[96] *E.g.* European Securities and Markets Authority (ESMA) (2017). The Distributed Ledger Technology Applied to Securities Markets; ECB AMI-SeCo (2017). The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration; Euroclear (2016), *Infra* note 74.

and exchanged by relevant actors, reducing administrative effort and manual intervention".[97] This is particularly relevant for OTC derivatives, as these might last for years, making the issue of management of counterparty credit risk a central function of the clearing process. However, it is still difficult to pin down whether these complex processes can be automated on blockchain not violating the rule of law, particularly, legal norms related to data privacy. Also, there seems to be a broad consensus that blockchain would not be able to increase the time-consuming processes of settlement on regulated FMIs, as the current T+2 cycle complexity was established, first of all, by market practices, financial industry laws and regulatory requirements and not by technical limitations.[98] Although, unprecedented volatility resulting from the COVID-19 pandemic has caused an increase in margin by more than 300 percent over historical averages providing an additional rationale behind work on DLT implementation for the Atomic T+0 target. For instance, the recent project launched by the Depository Trust & Clearing Corporation (DTCC) in 2020 – "Project Ion" explores new and alternative settlement models, leveraging the digitalization of cash and re-presentation of securities, and assesses a potential new accelerated settlement options provided by technologies (Figure 7, p.21).

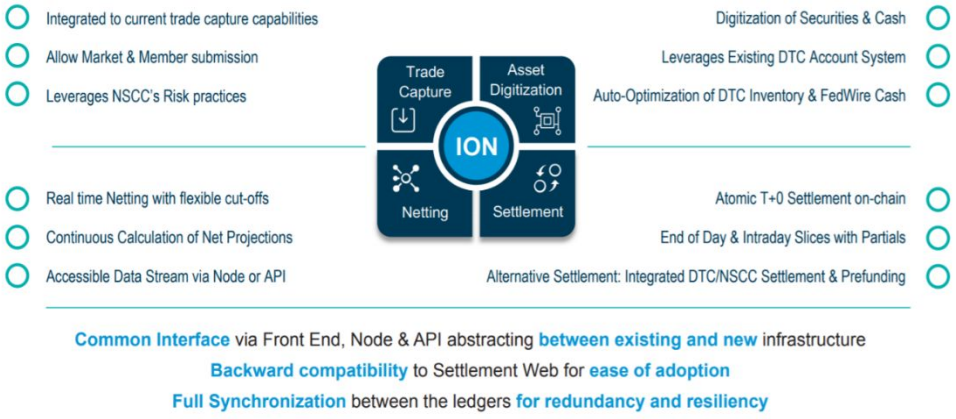



*Figure 7 Project Ion - case study* *Source: DTCC (May, 2020)*

Blockchain could be used to achieve the new normal efficiency on the markets. The legislative amendments recently undertaken in Switzerland,[99] Luxembourg[100] and

[97] ECB AMI-SeCo (2019). Potential use cases for innovative technologies in securities post-trading. (stating, *inter alia*, that private (restricted) DLT frameworks are more suitable for securities markets).

[98] See *e.g.* DTCC (2016). Embracing Disruption. Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape (noting that current netting efficiencies could effectively preclude cost- and risk-application of the ledger model settlements, which anywise is only relevant for only 3% of trades going through the full settlement mechanism), 16.

[99] During its meeting on 11 December 2020, the Federal Council brought into force, with effect from 1 February 2021, the parts of the DLT bill that enable ledger-based securities to be introduced (last visited Dec.15, 2020).

[100] Law No. 7363, amends the law of 01 August 2001 regarding circulation of securities http://data.legilux.public.lu/file/eli-etat-leg-loi-2019-03-01-a111-jo-fr-html.html (last visited Mar.15, 2019). Furthermore, on 27 July 2020, the Luxembourg's government presented a Bill of Law 7637 to amend the Law of 5 April 1993 on the financial sector and the Law of 6 April 2013 on dematerialised securities proposing the introduction of a new definition for "issuance account" in the 2013 Law (New par. 1 bis to art. 1 point 1 of Law of April 06, 2013). An issuance account (compte d'emission) would be defined as an account held by a settlement provider or central account keeper recording the dematerialised securities issued by an issuer.

Germany,[101] for instance, ensure that uncertificated (electronic) securities can be issued on and subsequently traded on blockchain. Nasdaq has enabled the first-ever private securities issuance documented with Blockchain technology back to 2015[102] and the World Bank Group has been issuing blockchain based bonds for its entire life cycle starting from 2018.[103] Numerous examples of leveraging it on top of traditional infrastructure, such as recently launched solution for collateral swaps in the securities lending market, HQLAx-Platform,[104] which aims at providing more efficient collateral management of high-quality liquid assets (HQLA), as in high demand under Basel III regulations, suggest that the new technologies and DLT can successfully contribute to significantly increasing legal certainty, therefore supporting new approaches to regulation of the market structures to address both: systemic risk and transaction costs.

As of today, there is no full-scale DLT system providing a full cycle of financial trades, so the real implications of DLT are not yet known.

While it is not clear yet if particular vulnerabilities associated with using DLT for trade and post-trade processes, *e.g.* issues of settlement risk and undertaking of swift amendments to smart contracts, such as needed under force-majeure circumstances would be tackled effectively, in accordance to existing rules and procedures the FMIs should clearly define the point at which settlement is final.[105] Taking into account distributed ledger's current technical features this can be highly problematic manifesting in legal uncertainties on the market.

## VII. Conclusions

It seems to be a pragmatic perspective to exclude mass adoption of permissionless blockchains in trade and post-trade cycles for securities over the next 20-25 years. Regarding permissioned blockchains, it largely remains to be seen as to what role the permissioned ledgers might play in the future and to what extent they would be capable of replacing traditional IT infrastructure. However, it is certain that DLT and blockchain have already influenced the complex financial markets by multiplying stakeholders' expectations regarding the scope and price of automation significantly contributing to the general shift from primary markets towards direct-access digital platforms. Incremental usage of ABCD cross-cutting enabling technologies in the capital market value chain, first of all, is now directly attributed to BigTechs' rapid expansion in the sector (*e.g.* through setting up the issuing venues) and could come with new risks and market failures.[106]

---

[101] Electronic Securities Act (Gesetz über elektronische Wertpapiere – eWpG-EE), draft published on 11 August 2020.

[102] Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology (December, 30 2015), (last visited Dec. 15, 2020).

[103] World Bank Prices First Global Blockchain Bond, Raising A$110 Million (August 23, 2018)

[104] Commerzbank, Credit Suisse und UBS führen erste Live-Transaktionen auf der Deutsche Börse/HQLAx-Plattform für Wertpapierleihe durch (03 December 2019) https://www.deutsche-boerse.com/dbg-de/media/pressemitteilungen/Commerzbank-Credit-Suisse-und-UBS-f-hren-erste-Live-Transaktionen-auf-der-Deutsche-B-rse-HQLAx-Plattform-f-r-Wertpapierleihe-durch-1690024 (last visited Dec. 03, 2019).

[105] Principle 8 of PFMI, *Supra* note 102.

[106] Further on the topic: Bank of International Settlement (BIS) (2019). *Big Tech in Finance: Opportunities and Risks. Annual Report*.

**A List of References**

Alexander K, Eatwell J., Persaud, A. and Reoch, R (2007). *Financial Supervision and Crisis Management in the EU*. European Parliament, Brussels.

Alexander K. (2012). "Market Structures, Technology and European Securities Regulation" in *Finanzmärkte Im Banne Von Big Data*, Schulthess, Zurich.

Andolfato D. (2018). *Blockchain: What Is It: What It Does, And Why You Probably Don't Need One*. Economic Research Division of Federal Reserve Bank of St. Louis, USA.

Arner D., D.Zetzsche, R.Buckley and J.Barberis (2018). *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, EBI Working Paper Series No. 28.

Arner D., J. Barberis and R. Buckey, (2017). *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 (3) NW. J. INT'l L. & Bus. 371-414

Awrey D (2011). *Regulating Financial Innovation: A More Principles-Based Proposal*, 5 BROOK. J. CORP. FIN. & COM. L. 273-315.

Awrey D. (2012), *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HBLR. 235.

Bernheim A., M. Schneider (1935). *The Security Markets, Findings and Recommendations of a special staff of the twentieth century fund*. New York.

Black, J (2001). *Decentring Regulation: Understanding The Role Of Regulation And Self-Regulation In A 'Post- Regulatory' World*, Current Legal Problems 54 (1).

Black, J. (2002) *Critical reflections on regulation*. CARR Discussion Papers (DP 4). Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, London, UK.

Bonneau J. et al. (2015). *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE Security & Privacy (Oakland).

Bookstaber R. (2007). *A Demon Of Our Own Design: Markets, Hedge Funds and the Perils of Financial Innovation.*

Brummer C. (2011). *How International Financial Law Works (and How it Doesn't)*, 99 Geo. L.J. 257.

Brummer C. and M. Smallcomb (2015). "Institutional Design. The International Architecture" in *The Oxford Handbook of Financial Regulation*, Oxford.

Buckley R., Avgouleas E. and D. Arner (2019) "Three Major Financial Crises: What Have We Learned?" in Arner D *et al*, *eds., Systemic Risk in the Financial Sector Ten Years After the Great Crash*, CIGI, Ontario Canada.

Busch D., G. Ferrarini, G.v Solinge (2019) *Governance of Financial Institutions*, Oxford.

C. Dwork, M.Naor (1993). "Pricing via Processing or Combatting Junk Mail" in E.F. Bnckell (Ed.): *Advances in Cryptology - CRYPT0 '92*, LNCS 740, 139-147.

Clack, C., V. Bakshi, and L. Braine. (2016). *Smart Contract Templates: foundations, design landscape and research directions*, Position Paper.

Cottier T. (2017), "Technology And The Law Of International Trade Regulation" in Brownsword R. *et al*, eds, *The Oxford Handbook Of Law, Regulation And Technology* 1018-1051.

De Filippi P. and A. Wright (2018) *Blockchain and the Law*. The Rule of Code. Harvard University Press.

Delimatsis P (2019), "When Disruptive Meets Streamline: International Standardization In Blockchain" in D. Kraus *et al*, eds, *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law,* 83-100.

Dobrauz-Saldapenna G., D.Wirth (2016). «Five propositions for future success of Switzerland as a Financial Centre" in *Global Banking and Financial Policy Review,* 173-179

Fabozzi F., F. Modigliani, and F. Jones (2014). *Foundations of Financial Markets and Institutions*, Pearson, 4th Ed.

Ferrarini G and P. Sagato (2015). "Regulating Financial Market Infrastructures", in *The Oxford Handbook of Financial Regulation.*

Gompres P. and J. Lerner (2003). "The Really Long Run Performance of Initial Public Offerings: The Pre-Nasdaq Experience" in *The Journal of Finance* Vol. 58 4, 2003.

Guice G., D. Schaffner, E. Pagano and H.C. Rickhoff (2019). "Policymakers Focusing on Artificial Intelligence" in The Journal of Robotics, Artificial Intelligence & Law, Vol.2, No.2, March-April 2019.

Hazen T (1991*), The Short-Term/Long-Term Dichotomy and Investment Theory: Implications for Securities Market Regulation and for Corporate Law*. 70 N.C. L. REv. 137.

Herbert A. Simon (1962). "The Architecture of Complexity" in *Proceedings of the American Philosophical Society* Vol. 106, N6, 467-482.

Korobkin R. (2000), *Behavioral Analysis and Legal Form: Rules vs. Standards Revisited*, 79 OR. L. REV. 23.

Kraus D. and C. Boulay (2019). "Blockchains: Aspects Of Intellectual Property Law" in D. Kraus *et al*, eds, *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law.*

Mishkin F. (1990), *Financial Innovation and Current Trends in U.S. Financial Markets* (National Bureau of Economic Research, NBER Working Paper No. 3323).

Nick Szabo (1997) *Smart Contracts: Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY.

Puschmann, T. and Weber, R. (2017). "Neuerfindung des Finanzsektors?" in *Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht* (SZW) 89 (1), 79–94.

Schlag P. (1986), *Rules and Standards*, 33 UCLA L. REv. 379.

Schwartz S. (2009). "Regulating Complexity in Financial Markets" in *Washington University Law Review*, Vol. 87, N2, 211-268.

Slovic P. (1987). "Perception of Risk" in: *Science*, 236 (4799), 280-285

Slovic P. (2000). *The Perception of Risk*. Earthscan.

Starr C. (1969). "Social Benefits versus Technological Risk" in: *Science,* Vol. 165, 3899 (Sept. 19, 1969), 1232-1238.

Tarbert H. (2020). *Rules For Principles And Principles For Rules: Tools For Crafting Sound Financial Regulation*, HBLR Vol.10, 6.

Trubek D. and L. Trubek (2006), *New Governance & Legal Regulation: Complementarity, Rivalry, and Transformation*, COLUM. J. EUR. L. Vol. 13.

Tufano P. (2003), "Financial Innovation" in Constantinides G. *et al*, eds, *Handbook of The Economics of Finance.*

Utterback J. (1941). *Mastering the dynamics of innovation. How companies can seize opportunities in the face of technological change*, Harvard University Press, 1994 ed.

Utterback J. and W. Abernathy (1975), A Dynamic Model of Product and Process Innovation, 3(6) Omega.

Utterback J. and W. Abernathy (1978). "Patterns of Industrial Innovation" in *Technology Review*, vol. 80, no 7, 40-47

Weber R. (2010). *New Rule-Making Elements For Financial Architecture's Reform*, J.I.B.L.R. 2010, 25(10), 512-521.

Weber R. (2012). Overcoming The Hard/Soft Law Dichotomy in Times of (Financial) Crises, *The Journal of Governance and Regulation*, Vol.1, Issue 1.

Wood P. (2007). *Regulation of International Finance*, Sweet & Maxwell.

Zetzsche D, R. Buckley, D. Arner and A. Didenko (2019). "Liabilities Associated With Distributed Ledgers: A Comparative Analysis" in Madir, eds, *Fintech Law and Regulation,*Elgar FLP, 185-208.

Zetzsche D., R.Buckley, J. Barberis, and D. Arner (2017), *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 FORDHAM J. CORP. & FIN. L. 3.

Zufferey J.B and M. Tschanz-Norton (1997). *Regulation of Trading Systems on Financial Markets,* Geneva.

Zufferey J.B. (1994), *Le réglementation des systems sur les marches financiers secondaries*, FR.

Zutzsche D, R. Buckley and D. Arner (2019). "The Rise of TechFins: Regulatory Challenges" in Madir, eds, *Fintech Law and Regulation,*Elgar FLP, 280-302.

Agency Guidance, International Standards and other Official Publications

Andrew Bailey, *Speech on the future of financial conduct regulation*, delivered at Bloomberg, London (Apr. 23, 2019)

Association of Foreign Banks (AFB), Futures and Options Association (FOA), International Capital Market Association (ICMA), International Swaps and Derivatives Association (ISDA), London Investment Banking Association (LIBA), Securities Industry and Financial Markets Association (SIFMA) (2017). *Follow-up Response to FSA Consultation Paper 06/19: Reforming Conduct of Business Regulation; and Consultation Paper 06/20: Financial Promotion and Other Communications.*

Bank for International Settlements, Oesterreichische Nationalbank (2019). *Materials of the Workshop Digital Currencies, Central Banks and the Blockchain: Policy Implications.*

Bank of International Settlement (BIS) (2019). *Big Tech in Finance: Opportunities and Risks*. Annual Report.

Bank of International Settlements (BIS), Committee for Payments and Market Infrastructures (2017). *Distributed ledger technology in payment, clearing and settlement. An analytical framework.*

BIS CPMI-IOSCO (2012). *The Principles for Financial Market Infrastructures (PFMI).*

Board Priorities – IOSCO work program for 2019.

Chair of the IOSCO Board (2018), *IOSCO Annual Report*.

Depository Trust & Clearing Corporation (DTTC) (Feb. 2020). Security of DLT Networks. A Distributed Ledger Technology Security Framework for the Financial Services Industry

DTCC (2016). *Embracing Disruption. Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape.*

DTCC (2016). *Embracing Disruption. Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape.*

ECB AMI-SeCo (2017). *The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration.*

ECB AMI-SeCo (2019). *Potential use cases for innovative technologies in securities post-trading.*

European Securities and Markets Authority (ESMA) (2017). *The Distributed Ledger Technology Applied to Securities Markets.*

*European Securities and Markets Authority (ESMA) (2020). MiFIR Report On Systemic Internalizers In Non-Equity Instruments.*

FSA (2007) *Principles-based regulation - Focusing on the outcomes that matter.*

International Organization of Securities Commissions (IOSCO) (2017). *Research Report on Financial Technologies (Fintech).*

International Telecommunication Union (ITU-T) (2019). *Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework.*

Proceedings of the 44th IOSCO Annual Meeting, Sydney, 13-17 May 2019.

SIX (2019). *Disclosure of SIX SIS Ltd. Regarding The CPMI-IOSCO Principles For FMI In Accordance With "Disclosure Framework And Assessment Methodology"*.

World Federation of Exchanges (WEF) (2016). *Financial Market Infrastructures and Distributed Ledger Technology.*

# About UCL CBT

The UCL CBT is the first centre globally to actively focus on blockchain-related research on the adoption and integration of Blockchain and Distributed Ledger Technologies into our socio-economic system.

The unique characteristics of the CBT at UCL provides a cross-sectoral platform connecting expertise and drawing knowledge from eight UCL departments centrally in one place. The CBT is a centre of excellence fostering open dialogue between industry players and sharing expertise and resources. It is a neutral think tank providing consultancy services to industry members, dedicated knowledge-transfer activities and cutting-edge in-house solutions.

For engagement outside of the academic world, the CBT's activities have been tailored to industry and policymakers' needs. The UCL CBT draws on its world-leading academic expertise to produce blockchain solutions for industry, start-ups and regulators. With a community of over 180 Research & Industry Associates and Industry Partners, it is the largest Academic Blockchain Centre in the world.

**Notable Work**

- The CBT released a report on the current adoption of DLT in global physical supply chains. The report featured an analysis of over 100 different projects taking place all over the world in the Grocery, Pharmaceutical and Fashion industries. Access the report here.
- The CBT is leading the Blockchain Technology for Algorithmic Regulation and Compliance (BARAC) project. This is the largest publicly funded blockchain project aimed at the public sector that will be defining feasibility guidelines to policymakers, industry and regulators by identifying problems and associated solutions with a bottom-up approach, built through case studies and proof of concept platforms. For this project, the CBT is partnering with the Financial Conduct Authority and the Singapore Monetary Authority and financial groups and Fintech companies like Banco Santander and R3.
- The CBT is a founding member of the Covid Task Force alongside The International Association for Trusted Blockchain Applications (INATBA) and the European Commission. The task force is convening key players in the global blockchain ecosystem to identify deployable technology solutions that address governmental, social, and commercial challenges caused by COVID. As well as identifying solutions, the Task Force will work to expedite their deployment.
- The CBT successfully funded nine research proposals that investigated topics including stable coin policy, smart contract innovation, blockchain economics and blockchain governance models. Research teams who were funded were made up of individuals from a variety of academic and industry organisations. Learn more about the projects here.
- The CBT launched the Block-Sprint hackathon to promote DLT innovation in the financial services sector. Over 160 individuals took part in the 2019 edition forming teams made up of industry practitioners, academics, and students. Learn about the winners and innovate ideas that were generated in the hackathon here.

# About the Discussion Paper Series

The *UCL CBT Discussion Paper is* published on a quarterly basis featuring the latest developments in the blockchain and DLT space. The aim of the discussion paper series is to share recent developments and state-of-the-art solutions on blockchain and DLT of researchers from an interdisciplinary background with the CBT community. All accepted submissions are available in the CBT paper database.

The submissions are circulated among the members of the UCL CBT Editorial Board, led by the Scientific Director so that the results of the research receive prompt and thorough professional scrutiny.

If you are interested in submitting a paper to be included in forthcoming editions, please visit our website here to see what the latest theme and criteria for submission are.

**UCL Centre for Blockchain Technologies**

http://blockchain.cs.ucl.ac.uk/

UCL Computer Science
Malet Place
London WC1E 6BT
United Kingdom

CBT