
***WSIS Forum 2018 OUTCOME DOCUMENT***

**Template for Submission of Executive Summaries for**

**Thematic/Country Workshop/ Action Line Facilitation Meetings/ Interactive Sessions/ High Level Dialogues/Publication Releases/Briefings**

**Deadline: Thursday 22 March, 2018**
***Exception: For sessions on Friday 23 March, please send at the latest 2 hours after the session***
*Please note that the WSIS Forum 2018 Outcome Document will be released on the* ***23rd of March***
*(the last day of the Forum)*

1) **Title of your session**
   Central Bank Issued Digital Currency: Interoperability and Security Challenges
2) **Name of Organization/s organizing the session**
   International Telecommunication Union (ITU)
3) **Relevance with the WSIS Action Lines – please specify the Action lines C1 to C11**

The Session is relevant to Action lines C5 "Building confidence and security in the use of ICTs" and C6 "Enabling environment". The session discussed the challenges which Central Banks face with regards to the regulatory, interoperability and security for digital currency. The developments at international level in developing standards for Central Bank issued digital currency and its characteristics and requirements for interoperability and security were also addressed.

4) **Key achievements, announcements, launches, agreements, and commitments (these will be reflected in the press release and Outcomes Document of the WSIS Forum 2018)**

5) **Main outcomes highlighting the following:**

   I. **Debated Issues**

   This session considered the differences between cryptocurrencies and Central Bank issued digital currency (CBDC). The session provided a broad perspective of the main challenges facing central banks in issuing digital currency from an interoperability, policy and regulatory and cybersecurity perspective. It is anticipated that the technology for CBDC could be used across all economies.

   Some of the key points from the presentations are summarized below:

- Dr Daniel Reiss, Visiting Member of Secretariat, CPMI, Bank for International Settlements gave an introduction and overview on "Central Bank Digital Currencies: what is it about?". CBDC are digital currencies which are issued by central bank authorities, and are a new instrument besides banknotes and coins, and bank reserves. CBDC have applications in (wholesale) payments among the financial industry, as well as in retail for individual payments.

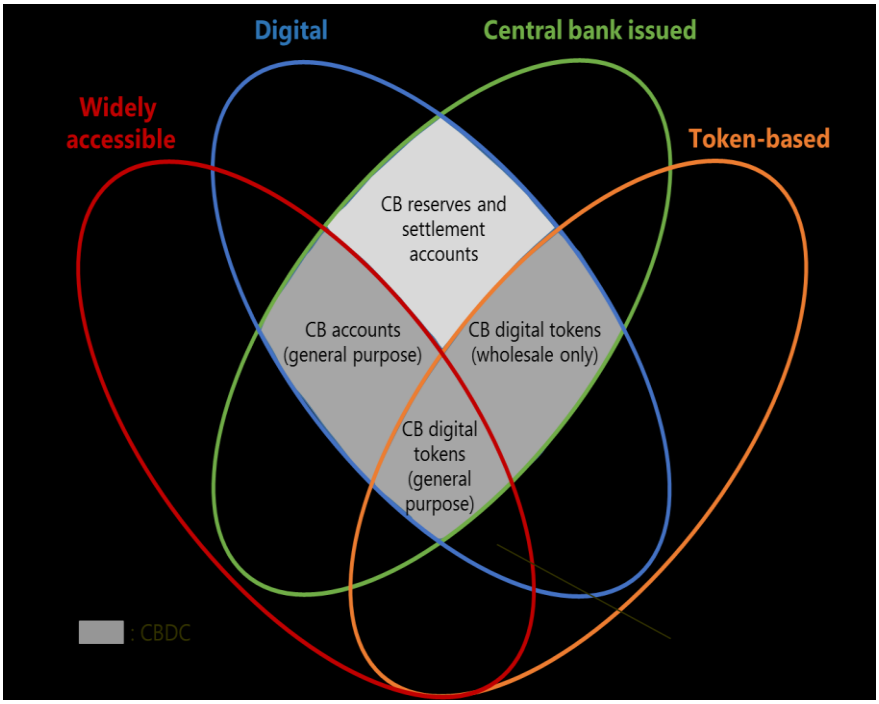


Figure 1: Money Flower (Source: Bech and Garratt, BIS Quarterly Review, September 2017, adapted by CPMI-MC report (2018)).

Central Bank Issued Digital Currency (CBDC) is potentially a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks. CBDC is at the centre of the money flower (See figure 1). The taxonomy distinguishes between three forms of CBDCs (the dark grey shaded area). Two forms are token-based and the other is account-based. The two token-based versions differ first and foremost by who has access, which, in turn, depends on the potential use of the CBDC. One is a widely available payment instrument that is primarily targeted at retail transactions but also available for much broader use. The other is a restricted-access digital settlement token for wholesale payment and settlement transactions. They are referred to as (central bank) general purpose token and (central bank) wholesale token. Private digital tokens (general purpose) in Figure 1 above include crypto-assets and currencies, such as bitcoin and ethereum.

Central Bank issued Digital Currency can be implemented by different technologies such as distributed ledger technology for example. There are various design choices for a CBDC, including: *access* (widely vs restricted); degree of *anonymity* (ranging from complete to none); operational

*availability* (ranging from current opening hours to 24 hours a day and seven days a week); and *interest bearing characteristics*. CBDC is different from cryptocurrencies as it is issued by the Central Bank and not by private entities like Bitcoin.

A number of important questions are to be answered such as on resiliency and efficiency of CBDCs, but also on interoperability with other digital payment systems, privacy, counterfeiting and avoidance of double spending, and aspects addressing policy, credit and investment. Open questions are which potential CBDC provide for innovations, their seamless integration, and trust. In the majority of countries, CBDCs do not imply crowd-out cash or less cash.

- Dr Klaus Loeber, European Central Bank, considered "Central Bank Digital Currencies - Risks and Implications". He gave insightful explanations of CBDCs along with a taxonomy showing the relationship of digital currencies with physical currencies and digital deposits. He pointed out a number of roles and responsibilities of central banks when issuing CBDC where central banks act as payment operators.

  Some of the design considerations and implications for central banks are:

  - **Availability.** Currently, access to digital central bank money is limited to central bank operating hours, traditionally less than 24 hours a day and usually five days a week. CBDCs could be available 24 hours a day and seven days a week or only during certain specified times (such as the operating hours of large-value payment systems). CBDC could be available permanently or for a limited duration.

  - **Anonymity.** Token-based CBDC can, in principle, be designed to provide different degrees of anonymity in a way that is similar to private digital tokens. A key decision for society is the degree of anonymity vis-à-vis the central bank, balancing, among other things, concerns relating to money laundering, financing of terrorism and privacy.

  - **Transfer mechanism.**The transfer of cash is conducted on a peer-to-peer basis, while central bank deposits are transferred through the central bank, which acts as an intermediary. CBDC may be transferred either on a peer-to-peer basis or through an intermediary, which could be the central bank, a commercial bank or a third-party agent.
  - **Interest-bearing.** As with other forms of digital central bank liabilities, it is technically feasible to pay interest (positive or negative) on both token- and account-based CBDCs. The interest rate on CBDC can be set equal to an existing policy rate or be set at a different level to either encourage or discourage demand for CBDC. Both non-interest bearing and interest bearing accounts could be used for retail or wholesale payment transactions. The payment of interest would likely enhance the attractiveness of an instrument that also serves as a store of value.

- **Limits or caps.** Different forms of quantitative limits or caps on the use or holdings of CBDC are often mentioned as a way of controlling potentially undesirable implications or to steer usage in a certain direction.

There are technical issues such as standardization and cyber risks, as well as economic issues and acceptance issues, regulatory, policy, and legal questions, and issues of cross-border. The CPMI Working group has been investigating the implications of digital innovations and of cryptocurrencies. He outlined the key elements of CBDC, and some optional design features. He highlighted several implications of CBDCs, and provided key findings from an analysis which concluded that elementary questions deserve an answer when designing digital currencies.

- Dr David Wen, Chairman, ITU-T Focus Group Digital Currency, including Digital Fiat Currency (ITU-T FG DFC) presented the current situation of the new "ITU-T Focus Group on Digital Currency including Digital Fiat Currency (FG DFC)" which was established in May 2017, and which builds upon the experiences and results of the former ITU-T Focus Group on Digital Financial Services (FG-DFS). With the example of Swedish e-Krona, CBDCs are not intended to replace physical currencies, but are actually complementing them. The Focus Group DFC is exploring the digital fiat currencies, with perspectives contributed by People's Bank of China, and Bank of Canada, and is looking into the ecosystem, along use cases, requirements and architectures, towards the opportunity for achieving interoperable, international DFC systems while considering issues of governance, interoperability, security, and counterfeiting. The second meeting of FG-DFC will be held in July 17-20 in New York City, United States.
- Dr Bruno Huttner, QKD Expert, ID Quantique introduced "Quantum threats and possible solutions for blockchains and digital currencies". The role of cryptography is to protect the digital currencies. He showed concerns that in a not too distant future, current cryptography might not be so secure anymore due to anticipated threats from quantum computers. He explained quantum computers as a novel approach which are fundamental different and potential much more powerful in their operations upon qubits than classical binary computers. Fears are that digital signatures schemes and other current public-key crypto primitives could be compromised by the power of quantum computers which are expected to become practical likely in a some years from now while some uncertainties exist with regards to the future security of other crypto primitives. He offered quantum-safe methods such as quantum key generation, quantum-resistant algorithms, or quantum cryptography as new tools to mitigate the threats. He concluded by calling for crypto agility such as designers of digital currency systems are recommended to take into account already now any future disruptive changes in crypto technologies and be able to adapt to the raising threats.

- Mr Paul Neubecker, CFO, HX Foundation and Hybrid Network remotely presented "Interoperability, Security and Privacy on Distributed Systems". He compared CBDC with public block-chains, with respect to privacy, to interoperability, and to security, where he explained the similarities but also the limitations of each technology. He concluded that each technology has trade-offs, but also that the technologies can be used complementary.

## II. Quotes

Commercial banks could lose **customer information** whereas Central Bank Issued Digital Currency may allow central banks to obtain better real-time data on economic activity: Klaus Loeber, European Central Bank

New digital currency should implement **crypto agility: Bruno Huttner, ID Quantique**

## III. Overall outcomes of the session highlighting

- **Various design choices and different forms of CBDC are possible with different implications for payment systems, monetary policy transmission as well as the structure and stability of the financial system**
- **CBDC raises old questions about the *role of central bank money*, direct *access to central bank liabilities* and the *structure of financial intermediation***
- **CBDC could bring potential *benefits* to payment and settlement systems, but could also pose *risks and challenges* – need to compare with existing or enhanced payment and settlement solutions**
- **The risk on cyber-security caused by the quantum computer will become real in the next few years. The quantum computer will break all public key signature schemes and would be a threat to hash function as well.**
- **As such digital currency solutions based on distributed ledger technology, needs to be made quantum secure.**
- **Interoperability of distributed ledger technology implementations of central bank issued digital currency with existing web infrastructure and other DLT's will be key for such deployments. Currently, in order to transfer from BTC to ETH, a trusted 3rd party is required resulting in fees and excessive value extraction. There is also need to develop a universal identity solution for eKYC.**

## IV. Main linkages with the Sustainable Development Goals

Mobile money and other digital financial services are becoming one of the main telecommunication/ICT success stories for socioeconomic development of many nations, especially in developing countries. The use of mobile phones for mobile financial services offers opportunities to enhance growth and development. In the meantime, mobile financial services can provide benefits to the telecommunication/ICT industry by making it the indispensable infrastructure for future financial services for everyone. Many Central Banks including the Federal Reserve Bank of United States, Bank of England, and People's Bank of China have all stated that they are researching and working on a central bank issued digital currency. Implementations of DFC using different technology and are in different phases of deployment. Like fiat currency in paper form that played a key role for financial inclusion for the past centuries, and continuing doing so, a digital fiat currency must also be accessible by all citizens of a country and could be a catalyst to accelerating interoperability in digital financial services and further help in bridging the financial inclusion gap and provide more financial stability. This would ultimately help in enhancing socio economic growth and more transparency in managing government funds disbursement and control over counterfeiting money.

## V. Emerging Trends related to WSIS Action Lines identified during the meeting

## VI. Suggestions for Thematic Aspects that might be included in the WSIS Forum 2019

**Please complete this document and send to Matthew L. Greenspan, Matthew.Greenspan@itu.int AND Gitanjali Sah, Gitanjali.Sah@itu.int**