bitt

White Paper

Central Bank Digital Currency Issuance

Contact:

Roland Haggins	roland@bitt.com
Oliver Gale	oliver@bitt.com
Gabriel Abed	gabriel@bitt.com
Simon Chantry	simon@bitt.com

Table of Contents

Executive Summary

Page 4

Physical Currency in a Digital World

Page 5

Historical Developments

Page 5

Currency Issuance

Page 6

Global Central Bank Digital Currency (CBDC) Developments

Page 8

A Digital Financial Ecosystem

Page 11

Encouraging Economic Growth

Page 14

Technology Overview

Page 15

Blockchain Technology

Page 15

Security

Page 16

How secure transactions take place

Page 16

Advanced Inter - Network Protocol

Page 18

Central Bank Multilateral Clearing Facility

Page 19

How Secure CBDC Issuance Takes Place

Page 20

Conclusion

Page 22

References

Page 23

Executive Summary

Innovations in the financial sector that provide an efficient means to make and receive payments can positively affect the long-term growth of economies. Technological developments in the payments system that are designed to reduce costs and inefficiencies could provide the environment necessary for unhampered economic growth. In an age of digital communication, it is not possible to conduct electronic transactions using physical notes and coins issued by a central bank. As such, many central banks around the world are currently researching the economic impact of a digital currency issuance to the public. Without central bank intervention, electronic transactions will continue to be facilitated by a fragmented system of legal tender substitutes, namely privately issued e-money and credit cards which are not part of the money supply. The current system of e-money limits the central bank's ability to control the money supply, lowers seigniorage income, decreases reserves, decreases international monetary control and changes the money multiplier.

By issuing digital currency, a central bank can solve the problem of not having a legal tender to securely, efficiently and uniformly be the medium of exchange in electronic payments settings. In effect, a central bank digital currency solves the problem of inefficient physical notes in much the same way that physical notes solved the problem of cumbersome precious metals.

This paper elaborates on how innovations by central banks issuing a digital currency, can increase efficiency, stimulate economic growth and solve a number of problems in the payments system today. Central banks around the world have approached the issuance of a digital currency from many different perspectives, these are explained and the most viable solution is presented.

Physical Currency in a Digital World

Historical Developments

Methods of payment have developed from primitive barter systems, to precious metal coins, to banknotes, to national fiat currency. Each of these advancements has brought about an increase in efficiency, ease of payment and economic productivity. In the famous 1776 book referred to as the Wealth of Nations, Adam Smith who many regard as the father of modern economics, described human nature as having “a propensity to truck, barter and exchange”. According to this view, to find an efficient means to trade appears to be embedded into the cycle of human activity to ensure the survival of the species. At the heart of this innovation is currency, the basis of trade. The historical developments of currency show evidence of the first metallic coins emerging at some point in the 7th Century BCE. Paper bills emerged some time later in China during the Tang Dynasty (618-907 C.E.) and in Europe during the 17th century. Physical notes are still the most ubiquitous form of currency on the planet. However, in an increasingly digital world, physical currency presents a set of challenges that can easily be solved through a digital transformation of currency. The challenges of physical currency include:

- The inability to transact in ecommerce and digital settings.
- The recurring cost of printing and coining physical currency.
- Security and risks of theft in transportation and storage.
- Logistical challenges and costs of transporting physical cash.
- Limitation during transactions where both parties must be present.
- Time consumption to count physical cash.
- The circulation of counterfeit currency.
- Physically damaged currency requiring removal from circulation.
- Challenges tracking tax evasion and money used for illicit purposes.
- Bacterial, fungal and virulent contamination of paper notes and coins.

- Environmental impact of printing and coining physical currency.

Purpose

Over the past decade we have seen rapid technological advances including the advent of cryptocurrencies, blockchain and distributed ledger technology. The result is that the technology now exists for central banks to resolve the challenges of physical fiat currency with the issuance of secure, efficient and stable digital currency.

Currency Issuance

Currency issuance is well known to be one of the primary functions of a central bank. The entire financial system of a country has to have a stable supply of legal tender to accommodate the ever-changing volume and variety of financial instruments, institutions and markets.

The volume and composition of this legal tender should adjust to the dynamic requirements of the economy. Accordingly, the central bank of a country may be granted,

i. The sole right to issue currency (including that of the government of the country)
ii. A monopoly of issuing legal tender bank notes.

According to the Bank of England, “legal tender has a very narrow and technical meaning, which relates to settling debts. It means that if you are in debt to someone then you can’t be sued for non-payment if you offer full payment of your debts in legal tender” (bankofengland.co.uk, 2017).

Most legal tender issued to the public by central banks is in the form of physical notes and coins, which means that electronic transactions cannot be performed using central bank issued currency. As a medium of payment, central bank legal tender should facilitate payments immediately, conveniently, securely and cheaply. Clearly this is not the case in an increasingly digital world where in addition to being cumbersome, physical cash represents a real burden on the environment. The private sector has innovated to meet the demand for digital payments by introducing privately issued e-money, mobile money, credit cards and a variety of other forms of digital money. The result is a frictional, fragmented combination of private e-money systems that act as a digital substitute for legal tender.

This existing system of e-money limits the central bank's ability to control the money supply, lowers seigniorage income, decreases reserves, decreases international monetary control and changes the money multiplier. With distributed ledger, blockchain technology and central bank digital currency (CBDC), this will end as central banks can instantly determine the size, distribution, and value of the money supply at the stroke of a button. By issuing CBDC, a central bank can solve the problem of not having a digital legal tender to securely, stably and uniformly be the medium of exchange and store of value in an electronic setting.

In effect, CBDC solves the problem of inefficient physical notes in much the same way that physical notes solved the problem of cumbersome precious metals.

Global Central Bank Digital Currency (CBDC) Developments

A number of central banks including the Central Bank of Canada, the People's Bank of China, the Bank of England, Sveriges Riksbank and the European Central Bank have published or are conducting studies to determine the benefits of issuing a digital legal tender. The Eastern Caribbean Central Bank and Central Bank of Barbados are also investigating the benefits of issuing their own digital currencies. While none of these central banks have formally issued a digital currency (CBDC) equal to that of their current fiat money, they have expressed interest in creating one in the future.

In many cases, central banks do not have the capabilities to issue a CBDC and this is a key reason for central banks to establish public-private partnerships with financial technology companies who not only have expertise in this area, but who are able to educate and train central bank staff to manage this process internally. Upon examining the costs and benefits associated with issuing a CBDC, central banks listed a number of characteristics that the digital currency would require in order to be successful. For instance, it would need to be considered a liability on the central bank's balance sheet just like traditional fiat money, the two currencies (physical and digital) would be interchangeable and the supply of the CBDC would be based on existing monetary policies. This means the CBDC would follow the same legal precepts that make a physical currency possible. Research from the Central Bank of Canada raised questions associated with the use of the CBDC including, the technology platform that would be used and the verification system required for secure access. The Central Bank of Canada has begun conducting experimental trials with CBDC but this has not yet been released to the public.

Ecuador is among the first countries to unveil their version of CBDC with their "Sistema de Dinero Electrónico" (electronic money system). There are two main weaknesses of this system. Firstly, it does not use distributed ledger technology but is effectively an electronic wallet issued to the public. Secondly, the balance held in the wallet must correspond to actual physical cash held at the central bank. The system can be used for person to person transactions or to make payments with vendors who use the system. It is controlled by the Central Bank of Ecuador which allows users to activate, deactivate and troubleshoot accounts via mobile devices, webpages and designated help desks throughout the country. Users load their accounts with money simply through deposits made at machines, online or through tellers. The electronic money system was designed to expand banking services to the underbanked population, as it gives them alternative

ways to store their cash, however it also offers cost saving opportunities to the government. Traditionally, Ecuador spends on average USD $3 million a year to exchange deteriorating and old currency for new notes. This cost could be completely eliminated if the e-money currency scheme reached ubiquity. Unfortunately Ecuador's electronic money system has failed to achieve the envisaged number of users to date. This has been attributed to legislation which leaves CBDC at risk, and the lack of confidence from banks into the security of the scheme at the central bank level.

According to reports, the West African Economic Monetary Union (WAEMU) is expected to have a legal digital tender issued by the Banque Regionale de Marches (BRM). The issuance will begin in Senegal then expand to Cote d'Ivoire, Benin, Burkina Faso, Mali, Niger, Togo and Guinea-Bissau and will operate under e-money regulations established by the Banque Central des Etats de l'Afrique de 'Ouest (BCEAO).

The Bank of England conducts ongoing research into the advantages and disadvantages of issuing CBDC. For example, the 2016 Staff Working Paper No. 605 from the Bank of England, explains the advantages of CBDC including, reduced transaction costs, increased competition for deposit accounts and a reduction in counterparty risks through peer to peer transactions. The UK Financial Conduct Authority (FCA) granted the financial technology company, Tramonex, Electronic Money Institution (EMI) status to start a blockchain based digital currency in the UK. This development could help the Bank of England further research and determine how they would approach a distributed ledger or blockchain based CBDC issuance.

During November 2016, the Government of India announced the demonetisation of all Rs. 500 and Rs. 1,000 banknotes, as a bold move to tackle black money, corruption and counterfeit notes used by terrorists. In December 2016, a report commissioned by the Minister of Finance of India presented by the Committee for Digital Payments made a number of recommendations to improve the digital payments system in India. Addressing the benefits that could be achieved if the government of India pursues a CBDC issuance, the report states: "instantaneous settlement of transactions, reduction of costs of cash, ability to provide a more comprehensive and unified source of credit history and reduction in instances of tax avoidance. The most significant benefit however, is that the technology makes it extremely difficult to counterfeit, and more importantly enables the central bank to detect the existence of counterfeit currency on a real-time basis."

As noted previously, the private sector has already innovated to meet the demand for digital payments by developing a vast array of fragmented private e-money and mobile money systems, which in many cases are not interoperable. To address the need for a digital currency for settlement use, BNY Mellon, Deutsche Bank, ICAP and Santander have collaborated for the creation of the Utility Settlement Coin, an asset-backed digital currency. Through the use of blockchain technology, intervention by central banks in

these areas could provide much needed efficiency, monetary stabilization and removal of friction from the payments system as a result of physical cash.

A Digital Financial Ecosystem

Blockchain technology has the ability to "fight corruption and to deal with failures of governance and governments and rule of law all over the world."

David Cameron,
Former Prime Minister
of the United Kingdom.

There are a growing number of alternative cryptocurrencies like Ethereum, that have similar attributes to the Bitcoin Blockchain. However, since 2009, the Blockchain technology platform that underpins Bitcoin has been tried, tested and found to be the most secure and decentralised public distributed ledger. Any apparent inefficiencies or time lags in settlement can be addressed by advanced inter-networking protocols that allow for micro-transactions, containing specified amounts of CBDC stored in metadata on the blockchain, to be settled instantly off the blockchain, but with the confidence of on-chain enforceability. This means transactions occur securely, seamlessly and in a stable robust digital ecosystem.

For this reason, the decentralised cryptocurrency Bitcoin, provides the framework for the technology infrastructure that makes it possible for a central bank to issue a secure, efficient and immutable digital currency. By issuing CBDC, the central bank can significantly increase seigniorage, reduce its overall costs and gain superior control over monetary policy.

However, it is important to note that CBDC does not replace physical notes and coins, but rather complements them in an increasingly digital society where physical

currency payments are on the decline. This is analogous to the manner in which email complements traditional postal methods and has increased the efficiency of conducting business over the past two decades. Technology that enables rapid payment services to large sections of the population has been advancing at a fast pace to deliver robust, secure and convenient payments solutions. These digital payment solutions allow for services to be delivered at lower costs, affording greater scalability and ease of access.

There are several advantages to a central bank issued digital currency:

Increased Seigniorage: Seigniorage is the profit a central bank makes from issuing legal tender. Typically, it is assumed that central banks do not pursue a profit objective per se, but they are presumed to contribute to the efficiency, stability, and competitiveness of financial markets. This includes reducing taxpayer burden where possible. With CBDC issued into the economy, the central bank can save on the costs associated with printing physical notes and coins. CBDC will potentially provide over 90% cost savings in comparison to the cost of printing, transporting, securing and distributing physical notes and coins. This will allow the central bank to retain greater seigniorage. In large economies, such as India for example, according to the 2016 report by India's Committee on Digital Payments, CBDC could enable the central bank to achieve an annual saving of up to INR 21,000 crores (USD $3.2 Bn) on the associated costs of physical currency. In addition, the reduction of physical payments and increase of electronic payments through the introduction of a CBDC provide the opportunity for increased seigniorage.

Efficiency: Technology has been advancing at a fast pace to deliver robust, secure and convenient payment solutions. For example, due to the platform agnostic nature of CBDC, features such as instant utility bill payment can be achieved through multiple platforms built and operated by various entities. CBDC can benefit consumers by allowing funds to transfer more efficiently and less expensively. This technology allows for services in the economy to be delivered at lower costs, affording greater ease of access and scalability. In addition, the blockchain platform can be used for an efficient system of global clearing and settlement.

Secure Non-counterfeitability: Cryptographically produced and secured, CBDC cannot be counterfeited. There will be a fixed amount of CBDC in circulation that the central bank issues and no other entity has the ability to add or remove CBDC; the process is reliant on the fundamentals of public-private key cryptography. Since CBDC transactions are verified by a consensus protocol on the blockchain, the problem of double spending is eliminated.

Auditability: The central bank can track digital transactions to an unprecedented level with superior accuracy, in comparison to physical currency transactions that are anonymous and more susceptible to illicit use. The new levels of transparency mean that Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) measures will become more robust, as will the Government's ability to gain revenue from previously

evaded taxes, which in some countries amounts to over 20% of GDP. Since transaction data is stored on the blockchain, and can be verified with certainty through the proof of work consensus mechanism, government issued CBDC enables greater auditability over existing physical currency while ensuring greater integrity of transaction data.

Monetary Policy: Central bank trust and credibility can be enhanced through a modernised monetary transmission system with CBDC that will allow the central bank to access a new way of implementing monetary policy to efficiently and systematically balance the economy. For example, the Bitt Inc. Central Bank Issuance Management Panel software is designed to allow central banks to issue, distribute and recall currency. The interface provides real-time detailed reports on transaction activity including, number of transactions, speed of transactions and velocity of money. This will enable central banks to accurately monitor the effect of monetary policy and make adjustments at inflection points to promote economic stability and growth. The technology infrastructure is platform agnostic, fully customizable, interoperable and upgradeable to suit the needs of respective central banks. In the same way, old notes are taken out of circulation, CBDC will be no different. The ability to upgrade the CBDC platform for more secure, efficient, lower cost and feature rich CBDC will form the basis of meeting the requirements of rapid technology developments and innovations.

Interoperability: Where there is a growing number of fragmented private e-money systems, one single digital instrument namely CBDC, issued by the central bank will solve the interoperability problem by being available for use in all instances where digital cash is required. This enables central banks to preserve their function as the sole issuer of national CBDC in the digital realm.

Financial Inclusion: Traditionally, banks have had prohibitive costs and requirements for products and services that exclude some of the most vulnerable in society. CBDC will enable access and provide usage of a broad range of affordable, quality financial products and services that the most vulnerable in our society will be able to utilize, namely the unbanked and underbanked.

Encouraging Economic Growth

"Digital financial services lower the cost and increase the security of sending, paying and receiving money."

Dr. Leora Klapper,
Lead Economist at the World
Bank Development Group

Governments and central banks can use this technology to solve a number of problems in the payment system today.

In traditional payment systems, fees are taken by third-party intermediaries for their role in facilitating and processing payments. This results in higher transaction costs. A relevant example of this is the Merchant Discount Rate (MDR) which vendors have to pay to accept digital payments on electronic payment channels such as Visa or MasterCard. Especially in developing countries, these fees are often perceived as high in relation to the value of goods sold. This renders it financially prohibitive for many micro, small and medium-sized enterprises (SMEs) to offer electronic payment solutions which in turn can limit business growth.

This is a key area where using CBDC with central banks and banks can create a more cost effective, efficient banking system. The technology infrastructure can settle payments in a purely peer-to-peer manner using distributed ledger technology. This means that merchants will be able to accept payments quickly and securely and consumers will be able to conduct peer-to-peer payments in the same manner.

Since payments are settled directly between parties, they can be settled with greater speed and transparency than with conventional systems, thus improving liquidity constraints. This gives banks and financial institutions the ability to maximise efficiencies and move into innovative payment mechanisms through a more digital approach to finance. A McKinsey Group study posited that the widespread adoption of a digital approach in payment systems globally could boost the GDP of emerging economies by USD $3.7 trillion by 2025. Within this, nearly two thirds of the forecasted increase would stem from increased productivity of financial and non-financial businesses, and governments, as a result of digital payments. The remaining third would be aligned to financial inclusion of the unbanked and SMEs. This perspective is supported by a working paper from the Bank of England which found that a CBDC issuance of 30% of GDP, against government bonds, could permanently raise the UK's GDP by as much as 3%.

Further, economists have identified that an efficient payment system reduces the cost of exchanging goods and services, and is critical to interbank and capital market functions. The improved efficiency of transactions with CBDC innovation can generate economic benefits. A reduction in costs in the payments system creates an incentive for participants to exchange more frequently. In contrast, an inefficient, weak payment system may negatively affect the stability and growth of the economy, through the inefficient use of financial resources, increase in risk and losses for market participants.

Technology Overview

Blockchain Technology

Blockchain is the underlying technology for Bitcoin, which is best known for its ability to enable peer-to-peer transactions on a decentralised network, it is a secure messaging system built on internet protocols. Instead of relaying emails, texts, or web pages, the Bitcoin network processes value-transfer messages or transactions. This network is a major example of an emerging category of money known as cryptocurrency; a fusion of cryptography and finance. Bitcoin solves the problem of double-spending, identification, authentication, and financial inclusion on the Internet without a central authority, an innovation made possible by a system known as public-key cryptography.

A distributed ledger is a digital record of information in a database that is replicated, synchronized and shared across each node on a network. The distributed ledger records all individual entries into groups or “blocks”, these blocks are then appended together in sequential order. The result of this process could be considered a chain of blocks often referred to as the “blockchain”. Each block of the decentralised database is constructed using public key cryptography or asymmetric cryptography and contains the digital signature of the previous block. Originally designed to support the Bitcoin cryptocurrency, the Bitcoin Blockchain infrastructure also supports a limited scripting language that can be used to store metadata. Bitt Inc. uses a protocol that enables the attachment of metadata to distributed ledger transactions for the issuing and exchange of immutable CBDC. The specific characteristics of distributed ledger technology, namely its unprecedented security, immutability, non-counterfeitability, efficiency of transfer, and robustness make its application clear to central banks for the foundation of a CBDC issuance infrastructure.

Security

Distributed ledger technology achieves unprecedented security and immutability properties, through the use of secure asymmetric cryptography techniques and through the use of a strong consensus mechanism. The consensus mechanism combined with the public nature of the ledger and asymmetric cryptography create immutable properties. The integrity of a central bank's digital currency monetary base can be ensured on the blockchain through its use of cryptographic SHA-256 hash functions, implemented in a 'Merkle Tree' structure. The transaction information for the central bank issued digital currency is bundled into 512 bit message blocks. Each block is run through a cryptographic function to output a hash, which is an alphanumeric string of characters much shorter than the original message. The output hash is a direct function of the message block, meaning that if one character alone in the 512 bit message block were different, the function would output a completely different hash pointer. Each hash contains information of one of the transactions in the message block and is timestamped to certify its existence at a specific time, with each timestamp containing the previous timestamp in its hash. A separate hash function is generated for every 512 bit message block, upon which pairs of hashes are then passed through the hash function to create 'hashes-of-hashes', in a process that is repeated until a final 'root hash' is achieved at the top of the Tree. Through repeating the hash function to create a 'hash-of-hashes', central banks can be assured of the integrity of the CBDC monetary base at all times by checking the original root hash. If even one fragment of transaction data had changed, it would not match and would be promptly identified as a false transaction. In addition, the hash pointers tied to transaction data serves as an index for the transaction history, enabling integrity and auditability of the CBDC monetary base. The multisignature and cold wallet hard air gapped systems make for impenetrable and computationally impossible reverse engineering of key pair generation.

How secure transactions take place

The authentication of the CBDC is based on the digital signature that accompanies the message. This is akin to the watermark on a central bank paper note, except it provides

irrefutable real-time proof that the digital currency was issued by the central bank, based on the premise of public key cryptography. Every holder of CBDC will possess a public and private cryptographic key. The public key could be likened to an address which enables other users to communicate with it (i.e. transact, sign contracts etc.). The private key is essentially a secure password that only its owner or the holder of the CBDC knows. If the holder of CBDC sends a transaction message, a digital signature is generated using the private key and the message. Authentication occurs when the public key is used to verify that the holder of the paired private key sent a message. The digital signature enables network nodes to verify that the sender is really the holder of the CBDC's private key. The function of the digital signature is hence to enable the network to verify the authenticity of CBDC contracts or transactions, and prevent fraud and impersonation.

Once the digital signature of the CBDC transaction is authenticated, it is grouped together with other authenticated transactions into a block. This forms the first block of the blockchain.

An additional level of security prevents fraud and potential double spending. The order of transactions in the distributed ledger is established, cannot be manipulated and must be proved authentic. Each block is encrypted using a cryptographic hash function and can only be read after it is decrypted. This is challenging due to the strength of the encryption and extensive computational power that is required for decryption. To ensure the network agrees on a single history of the order in which transactions occurred, without the existence of a trusted third party, a cryptographic technique called a Merkle 'hash tree' is used.

Information regarding transactions is grouped into bundles and run through a mathematical algorithm to create an alphanumeric string of characters much shorter than the original amount of data. Each hash contains the digital information of one of the transactions in the block and is timestamped to certify its existence at a specific time, with each timestamp containing the previous timestamp in its hash. A separate hash is generated for each transaction in a block, upon which pairs of hashes are then passed through the hash function to create 'hashes-of-hashes', in a process that is repeated until a final 'root hash' is achieved. The hashing process enables the easy identification of any changes made to the data within the transactions of a block by rerunning the process and cross-checking with the original 'root hash'. Hashes can then be used as a means to index and verify the large amounts of data generated through transaction histories

as even if only one character of the input data is changed, the hash generated will be a completely new alphanumeric string.

Advanced Inter-network protocol

While originally designed to support the Bitcoin cryptocurrency, the Bitcoin Blockchain infrastructure also supports a limited scripting language that can be used to store metadata on to transaction information. The advanced inter-networking protocol is a permissioned distributed ledger that has the additional security of the permissionless Blockchain ledger. This protocol allows Bitt Inc. to fulfil a fully functioning CBDC issuance based on blockchain technology. The protocol can be used by central banks to house data pertinent to CBDC on top of any cryptographic transaction data, thereby ensuring forward compatibility and exchange of its CBDC with other digital currencies. This layer connects central bank requirements with end-users, to provide the economic data, connect to AML and KYC identity solutions, privacy and the architecture for a scalable payments infrastructure.

It is important to note that although Bitt Inc. has at this time focused on the Bitcoin Blockchain, this strategy and method is blockchain and distributed ledger agnostic, being fully interoperable with other decentralized and centralized databases. The technology infrastructure is fully upgradeable and continues to adapt with technological advances to maintain consistency, robustness and maintain interoperability in the future.

Advanced inter-networking protocols enable operations to be completed across multiple distributed ledgers. This can be harnessed by central banks to enhance the capabilities of their CBDC infrastructure, ensuring the interoperability of its CBDC amongst ledgers used by other institutions or payment providers. This will be highly relevant for international foreign exchange transfers using a central bank issued digital currency. In addition, the advanced inter-networking protocol allows for microtransactions, containing specified amounts of CBDC stored in metadata on the blockchain, to be settled instantly off the blockchain, but with the confidence of on-chain enforceability. The ability to distribute nodes geographically that may run different software implementations, combined with full data duplication across the decentralised database network provides a real-time settlement system with strong defenses against physical events and cyberattacks. Through

enabling the instant settlement of transactions that would take up to an hour to be fully verified on the blockchain, central banks can scale the CBDC monetary base without hinderance to meet growing user demands.

Central Bank Multilateral Clearing Facility

The properties of distributed ledger and blockchain technology can assist the role of central banks in global payment systems. Distributed ledger based CBDC can significantly reduce or eliminate counterparty risk for CBDC transactions. A global distributed ledger network provides the attributes of a global settlement system that is resilient, robust and secure. A 2016 consultation paper from the Bank of England highlights three contexts where distributed ledger technology can be applied:

- As a platform for core RTGS settlement.
- As a platform for externally-managed securities settlement delivery versus payment or foreign exchange payment versus payment services that require access to central bank money.
- As a platform for a possible future digital currency that might need to interoperate with RTGS.

Inter-Central Bank Currency Agreements:
Two central banks both issuing a fully interoperable blockchain based central bank digital currency, can settle funds transferred from one digital currency concurrently with funds transferred from another. Likewise, eliminating counterparty risk, banks holding accounts at the central bank can seamlessly conduct cross-border payments in real time through the central bank with central bank digital currency. These technological developments lead the way for new bilateral currency agreements, and the internationalization of currencies that previously suffered from low demand in foreign exchange markets.

How Secure CBDC Issuance Takes Place

There are a number of different models that describe how a CBDC issuance may take place in an economy. It is important to note, that the CBDC characteristics and method of issuance are fully customisable according to the individual specifications or preference of the CBDC issuing authority. Bitt Inc. recognises the that the issuance model chosen will impact mobile operators, financial institutions and all participants of the economy. For this reason, Bitt Inc. welcomes discussion from central banks, financial institutions, mobile operators and the general public in this regard.

Below are two approaches to consider:

The first approach involves the central bank issuing CBDC reserves for selected financial institutions. The CBDC would be transferred to the financial institutions who would use it for lending and settling transactions. Banks would then issue their own interoperable private digital currencies, which would be used by their customers. Physical currency would remain in circulation indefinitely and bank customers would be able to exchange their physical currency for CBDC. This approach allows for the fractional reserve system to function in much the same way.

The second approach makes use of Digital Cash Accounts (DCAs) which are a type of account facilitated by banks and financial technology firms but held at the central bank, as opposed to banks. Traditionally, only banks or building societies were able to hold accounts at the central bank. This limited competition in payment account services as payment service providers (PSPs) were reliant on the banks for accounts, who in turn set high rates to disadvantage the PSPs from competing.

Since DCA account funds are held by the central bank and owned by the account holders, even if the DCA facilitator were badly managed and faced bankruptcy, the DCA holders' funds would be inaccessible for seizure by the DCA facilitator, thereby offering safety and redundancy features comparable to those of a Trust. Potentially, funds held in the DCAs would be recorded as liabilities on the balance sheet of the central bank, and therefore would be balanced by equivalent assets in the form of perpetual zero coupon bonds issued by the government for the sole purpose of 'backing' the issuance of the digital cash.

Furthermore, establishing CBDC monetary policy will strengthen and stabilize the financial system while reducing bank systemic risk. With a CBDC, the credit creation process would remain much the same with the exception that banks could issue loans without accepting deposits as all CBDC will be held by central bank in DCAs. The central bank would provide banks loans in CBDC, who would then provide these funds to creditworthy customers. Even if a financial institution failed, no depositors funds would be affected as all CBDC would be held in central bank DCAs.

This second approach would provide the central bank with unprecedented real-time transparency, auditability and the ability to have greater control over monetary policy.

The legal precepts that make a digital legal tender issuance possible are the same legal precepts that enable a central bank to issue a physical currency. This requires taking the precepts of the law in the respective country that allow for physical legal lender issuance and amending them to include currency in a digital format. The result is that the sole issuer, the central bank, would be additionally able to issue a known amount of digital fiat currency to be put into circulation.

Conclusion

From taxes to social welfare benefits, the governments of the world cumulatively receive and disburse trillions of dollars to and from their citizens. A digital transformation of this flow of money is a strategic shift from the dependence of physical cash to a more efficient, secure and lower cost, electronic payment system. Through harnessing the potential of blockchain technology it is possible for central banks to safely and securely issue a digital legal tender currency.

Digital legal tender issued by a central bank to the public, has the potential to modernise the financial system of any economy, thereby ushering in the establishment of a strong payment and settlement framework with unprecedented opportunities for economic growth. This technology advancement can allow for seamless inter-central bank digital currency transfers. A central bank digital currency (CBDC) issuance can also enable a central bank to achieve greater seigniorage and interoperability of its currency, whilst simultaneously increasing the reach of its monetary policies and broadening financial inclusion.

In order to make CBDC issuance a reality, governments must recognise the benefits and opportunities that it affords. Legislation pertaining to legal tender and to the power of a central bank to issue and maintain its legal tender monetary base, should be amended to include legal tender in a digital form. In turn, for these milestones to be reached, further education into the properties and benefits of blockchain technology for CBDC issuance, must reach a government and policy making level. It is recommended that governments prudently engage in pilot projects and proof of concept experimentation, using a phased approach within controlled environments, to deploy, test and assess the feasibility of suggested implementations.

Bitt Inc. welcomes discussion from central banks, financial institutions, mobile operators and the general public on the areas of this paper.

References

Aschenbeck-Florange, T. (2014, February 05). Regulation of Bitcoins in Germany: First comprehensive statement on Bitcoins by German federal financial supervisory authority (BaFin). Retrieved February 19, 2017, from Bitcoin Magazine, https://bitcoinmagazine.com/articles/regulation-bitcoins-germany-first-comprehensive-statement-bitcoins-german-federal-financial-supervisory-authority-bafin-1391637959/

Banco Central Do Brasil. (2013, October 09). SPB (Sistema de Pagamentos Brasileiro) The Brazilian Payments System Law 12,865. Retrieved February 19, 2017, from Banco Central Do Brasil, https://www.bcb.gov.br/Pom/Spb/Ing/InstitucionalAspects/Law12865.pdf

Bank of England (2016) 'The macroeconomics of central bank issued digital currencies', Staff Working Paper, (605), pp. [Online]. Available at: http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf (Accessed: 6th March, 2017).

Bank of England, A new RTGS service for the United Kingdom: safeguarding stability, enabling innovation (September 2016): www.bankofengland.co.uk/markets/Documents/paymentsystem/cp160916.pdf

Barrdear, J., & Kumhof, M. (2016, July). Staff Working Paper No. 605 The macroeconomics of central bank issued digital currencies. Retrieved February 19, 2017, from Bank of England, http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf

Cawrey, D. (2014, May 01). How Auroracoin is Forcing Digital Currency Discussion in Iceland. Retrieved February 19, 2017, from CoinDesk, http://www.coindesk.com/auroracoin-forcing-digital-currency-discussion-iceland/

Central banks should lead on digital currency, PBOC's fan says (2016, September 1). Bloomberg News. Retrieved from https://www.bloomberg.com/news/articles/2016-09-02/central-banks-should-lead-on-digital-currency-pboc-s-fan-says

Committee on Digital Payments. (2016). Medium Term Recommendations to Strengthen Digital Payments Ecosystem. Available: http://finmin.nic.in/reports/watal_report271216.pdf. Last accessed 27th Feb 2017.

Deutsche Bank . (2016, August 24). Utility settlement coin concept on blockchain

gathers pace. Retrieved February 19, 2017, from Deutsche Bank, https://www.db.com/newsroom_news/2016/medien/utility-settlement-coin-concept-on-blockchain-gathers-pace-en-11661.htm

Digital currencies: International actions and regulations. (2017, January). Retrieved February 19, 2017, from Perkins Coie, https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#Australia

Dinero Electrónico - Servicio de Rentas Internas del Ecuador. (2016). Retrieved February 19, 2017, from Servicio de Rentas Internas del Ecuador, http://www.sri.gob.ec/web/guest/dinero-electronico

ECB. (2015, February). Virtual currency schemes – a further analysis. Retrieved February 19, 2017, from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

ECurrency mint limited and Banque Régionale de Marchés launch new digital currency in Senegal (2016, November 4). Business Wire. Retrieved from http://www.businesswire.com/news/home/20161103006949/en/eCurrency-Mint-Limited-Banque-R%C3%A9gionale-De-March%C3%A9s

Edu.bankofengland.co.uk. (2017). What is legal tender? | Bank of England Knowledge-Bank - The economy made simple. [online] Available at: http://edu.bankofengland.co.uk/knowledgebank/what-is-legal-tender/ [Accessed 28 Feb. 2017].

Electronic Money. (2017). Retrieved February 19, 2017, from Central Bank of Ecuador, https://www.bce.fin.ec/en/index.php/electronic-money-system

Fung, B. S. C., & Halaburda, H. (2016, November). Central Bank Digital Currencies: A Framework for Assessing Why and How. Retrieved February 19, 2017, from Bank of Canada, http://www.bankofcanada.ca/wp-content/uploads/2016/11/sdp2016-22.pdf

Gautham. (2016, November 16). Sweden to have its own digital currency by 2019. Retrieved February 19, 2017, from Bitcoin News, http://www.newsbtc.com/2016/11/16/sweden-digital-currency-2019/

Higgins, S. (2016, November 28). German Central Bank Tests Blockchain Trading Prototype.

Retrieved February 19, 2017, from CoinDesk, http://www.coindesk.com/german-central-bank-blockchain-trading/
Hofverberg, E. (2015, May 20). Sweden: Tax authority publishes guidelines for income tax on Bitcoin mining, suggests prohibition of Bitcoin use in waste and scrap metal transactions. Retrieved February 19, 2017, from Library of Congress, http://www.loc.gov/law/foreign-news/article/sweden-tax-authority-publishes-guidelines-for-income-tax-on-bitcoin-mining-suggests-prohibition-of-bitcoin-use-in-waste-and-scrap-metal-transactions/

Hofverberg, E. (2014, August 12). Iceland: National digital currency Auroracoin launched. Retrieved February 19, 2017, from Library of Congress, https://www.loc.gov/law/foreign-news/article/iceland-national-digital-currency-auroracoin-launched/

Junta de Regulación Monetaria Financiera. (2016, August 29). Resolución No. 274-2016-M. Retrieved February 19, 2017, from http://www.juntamonetariafinanciera.gob.ec/PDF/resolucion274m-2016.pdf?dl=0

Kristof, A. (2015). National Cryptocurrencies. In Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data (pp. 67–79). Retrieved from http://aksitha.com/Big%20Data%20Technologies/Big%20Data/HANDBOOK%20OF%20DIGITAL%20CURRENCY%20-%20Bitcoin,%20Innovation,%20Financial%20Instruments,%20and%20Big%20Data%20%5B2015%5D.pdf

Library of Congress. (2014, January). Regulation of Bitcoin in Selected Jurisdictions. Retrieved from http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

McKinsey Group (2016) Digital Finance For All: Powering Inclusive Growth In Emerging Economies, : McKinsey Group.

Rosenfield, E. (2015). Ecuador becomes the first country to roll out its own digital cash. Available: http://www.cnbc.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html. Last accessed 15th March 2017.

Shin, L. (2016, June 16). Canada has been experimenting with A digital fiat currency called CAD-COIN. Forbes. Retrieved from http://www.forbes.com/sites/laurashin/2016/06/16/canada-has-been-experimenting-with-a-digital-fiat-currency-called-cad-coin/#6d4091ed1b0c

Smith, Adam. Wealth of Nations, edited by C. J. Bullock. Vol. X. The Harvard Classics. New York: P.F. Collier & Son, 1909–14; Bartleby.com, 2001. www.bartleby.com/10/

UWI TV, & King, D. (2017, February 10). UWI SUNY symposium - “crisis in correspondent banking in the Caribbean” Retrieved from https://www.youtube.com/watch?v=I9OurFk0qx-s&feature=youtu.be&t=8169

Young, J. (2017, February 12). UK government grants permission to issue Blockchain-Based currency. Retrieved February 20, 2017, from The Coin Telegraph, https://cointelegraph.com/news/uk-government-grants-permission-to-issue-blockchain-based-currency

