



The Advent of Crypto Banking

A New Paradigm for Central and Commercial Banking

A Perspective on Blockchain / Distributed Ledger Technology

November 2016

Contents

INTRODUCTION	1
1 MONEY'S EVOLUTION	2
1.1 CRYPTO INSTRUMENTS – THE NEW MONETARY INSTRUMENT	2
1.2 CRYPTO CURRENCIES – THE MOST FRICTIONLESS FORM OF MONEY	4
2 CENTRAL BANKING REIMAGINED	6
2.1 CENTRAL BANK ISSUED CRYPTO CURRENCY – THE THIRD FORM OF MONEY	6
2.2 BENEFITS FOR CENTRAL BANKS AND REGULATORS	6
2.3 SOVEREIGN BLOCKCHAINS – THE IMPENDING CENTRAL BANK PLATFORM	7
2.4 THE TRANSITION TO CRYPTO BANKING	9
2.5 A WORD OF CAUTION	12
2.6 THE IMPORTANCE OF REGULATORS	14
3 COMMERCIAL BANKS IN A NEW WORLD	15
3.1 THE BANKING DILEMMA	15
3.2 VALUE STORAGE	16
3.3 VALUE TRANSFER	16
3.4 VALUE PROVISION AND PROTECTION	17
3.5 TRUST IS HERE TO STAY	18
CONCLUSION	19
APPENDIX: CENTRAL BANK MANDATES AND TOOLS	21
DISCLAIMER	22

INTRODUCTION

The advent of the Information Age in the 1970s allowed humanity to progress into a world in which information could flow freely, unhindered by national borders, without the need for intermediaries such as post offices, libraries and universities. We have now entered an age in which not only information, but value can flow freely without the need for trusted intermediaries such as banks, deeds offices and Central Securities Depositories (CSDs). The technology that has enabled this digital peer-to-peer value-transfer revolution is called Distributed Ledger Technology (DLT) or blockchain¹.

Blockchain has captured the banking world's attention with its promise to improve transaction speeds and significantly reduce back-office processes and costs. However, the true ingenuity of blockchain is the creation of the **crypto instrument** – one of the most fundamental game changers in banking history. The birth of the crypto instrument allows us to question some of the basic assumptions of our current banking model and imagine a new system of banking – **crypto banking** – unfettered by obsolescent constraints. Removing these constraints allows us to envision the emergence of a new form of money (a central bank issued crypto currency), leading to a more stable financial system in which bank runs do not exist and deposit liabilities are anachronistic.

This paper aims to provoke deep introspection about our current fractional reserve banking system and the role of central and commercial banks within this system. We hope to contribute to the discourse of practitioners in central banking, commercial banking and the blockchain industry by examining some of the principles of money, value, banking and macroeconomics, and how blockchain may impact some of these principles. We believe that the greatest benefits of blockchain in banking will only be reaped once central banks issue their own currencies onto a blockchain. Such a step will allow other assets to be issued on the same blockchain and permit a plethora of use cases to come to full fruition. Central banks have a critical role to play in unlocking blockchain's tremendous potential.

This paper is structured in three parts:

- Part 1 – Money's Evolution
- Part 2 – Central Banking Reimagined
- Part 3 – Commercial Banks in a New World

This paper assumes a basic knowledge of blockchain².

¹ It should be noted that blockchain is a form of “distributed ledger technology” (DLT) and not all DLT architecture uses a chain of blocks to form distributed ledgers. Nonetheless, we use the term “blockchain” throughout this paper for purposes of simplicity.

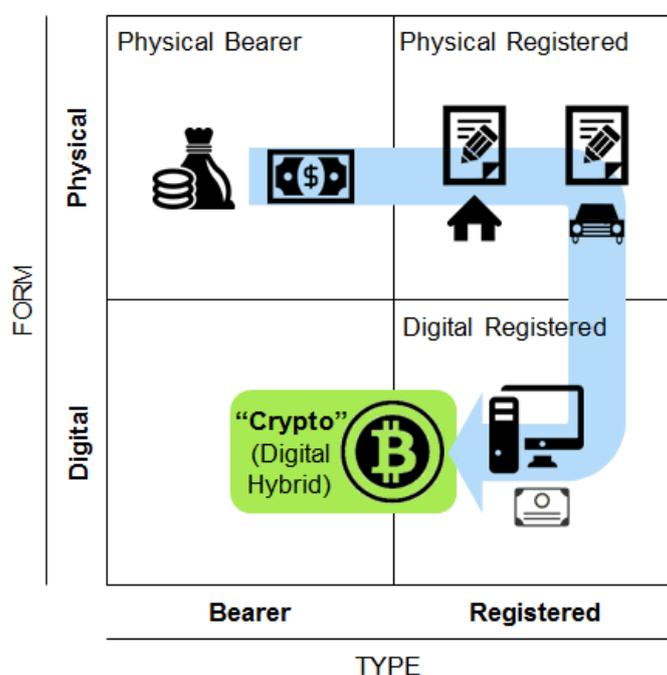
² For a 35 minute introductory video, please visit: <http://foundry.co.za/blog/blockchain-explained/>

1 MONEY'S EVOLUTION

1.1 CRYPTO INSTRUMENTS – THE NEW MONETARY INSTRUMENT

All monetary value in our society exists in one of two forms: bearer instruments or registered instruments. A **bearer instrument** is an asset that is assumed to be owned by the holder of the instrument, for which no transaction record is kept. An example is physical cash: it is not necessary to prove ownership of physical cash as the holder is the presumed owner. Society keeps no record of the transfer of ownership from one person to another. **Registered instruments**, on the other hand, are assets whose ownership is determined by referencing a ledger managed by a trusted institution (e.g., properties at the Deeds Office, bonds and equities at the CSD, or digital money in a bank account). While all assets can be categorised as either bearer or registered instruments, they can also be categorised as either physical or digital assets. Overlaying asset form (i.e., physical vs. digital) onto instrument type (i.e., bearer vs. registered) helps us understand the evolution of monetary instruments in society.

Figure 1: The evolution of monetary instruments in society



Physical bearer instruments were the first monetary instruments of human civilisation (e.g., animal hides, shells, salt, etc.), but communities came to realise that such forms of monetary value had their limitations. Land, for example, was an ineffective bearer instrument. If a hunter left his land and came back to find someone else standing on it claiming it for himself, one of two outcomes could result: the loss of the land to the new “owner”; or violence to resolve the dispute. Furthermore, there would be an incentive to remain on the land to maintain ownership and avoid any potential disputes. Neither of these outcomes is conducive to an advancing civilisation.

Thus, as communities developed, **physical registered instruments** emerged whereby the community collectively agreed on a trusted intermediary to keep the record of ownership (the source of truth) of a particular asset and update it on the community's behalf.

As computers became more widely adopted, many of these physical registered instruments migrated from physical to digital registers³. The birth of digital registers also gave rise to **digital registered instruments** – instruments that have no physical form, and are defined purely by an entry onto a digital register (e.g., a government bond or money in a bank account). Physical forms of value are easy to understand in this framework, while digital instruments are less intuitive.

A purely digital bearer instrument (e.g., a digital coin) cannot function as a monetary instrument due to the double-spending problem. Double-spending is the ability to spend a digital token of value more than once, as the act of spending it does not remove ownership from the spender. To understand this further, it is helpful to think of a photograph on a smartphone: the act of sending the photograph to others does not delete the photograph from the sender's phone. This poses a problem for anything digital that is meant to represent value. What is critically important in any monetary system is that when someone spends monetary value, he/she no longer has it. The ability to repeatedly copy and paste a digital token of value (the ability to double-spend it) reduces its scarcity and ultimately leads to its devaluation. To avoid double-spending digital monetary instruments, society has established trusted institutions (e.g., banks, deeds offices, CSDs) that ensure that when someone receives digital value, someone else must by definition no longer have it. This is a fundamental principle of our double-entry accounting system in which every debit must be equal to a corresponding credit.

In summary, three types of monetary instruments have been described:

1. Physical bearer instrument;
2. Physical registered instrument; and
3. Digital registered instrument.

These three instrument types were the only ones available until 2009. That year, Satoshi Nakamoto's seminal paper "Bitcoin: A Peer-to-Peer Electronic Cash System" combined advances in computer science, cryptography and game theory to develop what has now become known as blockchain technology. This technology has allowed the emergence of a fourth type of monetary instrument:

4. Crypto instrument

³ Physical registered instruments can thus be registered on either physical or digital *registers*.

The **crypto instrument** is a digital hybrid instrument with characteristics of both bearer and registered instruments: it's similar to a bearer instrument because the holder of a digital private key is the presumed owner of the value it controls, and it's also similar to a registered instrument because that value is recorded on a ledger (albeit a distributed one). The presence of both bearer and registered instrument characteristics are necessary for the existence of a crypto instrument. All assets issued onto a blockchain are crypto instruments.

1.2 CRYPTO CURRENCIES – THE MOST FRICTIONLESS FORM OF MONEY

The emergence of crypto instruments has allowed digital monetary value to be held without the need for a trusted intermediary for the first time in history. **Crypto currencies** – the most common type of crypto instrument today – such as Bitcoin, Ether, and many others⁴ demonstrate this fact. Anyone who owns crypto currency has a **unique private key** (akin to a password) that allows the owner (and only the owner) to mathematically “unlock” or spend the value at an associated public address (akin to an account number). The ledger that records the amount of crypto currency at any particular public address is maintained by a network of computers (called nodes) that run a consensus algorithm to ensure that they are all synchronised.

The ingenuity of this network of nodes working together to validate transactions (and reject any double-spending) is that the multitude of nodes ensures that there is no dependence on any single one to ensure the integrity of the ledger. This is a powerful concept – the way to remove a trusted intermediary is not to get rid of the intermediary, but to increase the number of intermediaries that are maintaining the same ledger so that trust in any particular intermediary is no longer needed. Dependence on any single intermediary reduces as the network grows, and indeed the term “intermediary” starts to become inappropriate and even inaccurate.

To understand the financial world's fascination with crypto currency and blockchain, we have to examine the nature of money. The traditional textbook definition of money refers to its three major functions in society: a means of exchange; a unit of account; and a store of value. Interrogating this further, however, it becomes apparent that all three functions relate to the concept of money representing value. After all, why accept money as a means of exchange for something else of value unless one believes the money has at least the value of what it was traded for? And a unit of account that measures the value of other products needs to possess value itself, otherwise it would be abandoned as a unit of account (as we have seen in any economy that has witnessed hyperinflation). So if the functions of money boil down to the value it possesses, what determines the value⁵ of money?

⁴ There are over 700 crypto currencies today.

⁵ There is much confusion about what value is and how it is derived. At the most fundamental level, value is what something is worth to someone. The price of any asset is determined at the interface between buyers and sellers who come together in a market-place (of any type – physical or virtual) to express their value of that asset in the form of bids and offers. However, it is impossible to think of the value of an asset without comparing it to another asset. Value is relative. We are socialised to think of value in the context of the most common asset in our societies – money. As such, when one is asked what the value of a cell phone is, most think of its value in terms of their local currency (Rands, USD etc.). But this is merely a product of being socialised to think of value in terms of money. The same cell phone has an exchange rate with mops, mangos and

Six characteristics determine how effectively money performs the functions mentioned above and in turn determine its value. These characteristics are:

1. **Durability** – if money is meant to store value and does not last long itself, it cannot function as a very good store of value;
2. **Portability** – to facilitate trade, money needs to be very portable, and costs associated with transferring it from one party to another diminish its function as money;
3. **Fungibility** – a unit of money should be exactly the same as any other unit, otherwise time and energy would be consumed in comparing tokens rather than promoting trade;
4. **Divisibility** – the smallest unit of money must be worth less than every other tradable asset, otherwise another token of money would need to be used to trade something worth less than the smallest unit of money;
5. **Scarcity** – the oversupply of any commodity brings its value down, and in the extreme case, where something is overly abundant, it cannot be used to trade for other scarce resources; and
6. **Acceptability** – money is accepted because the recipient believes it will be accepted by others when he/she wants to spend it. Without the belief that money will be accepted by others in the future, it would cease to be money.

Crypto currency is a better performing form of money (versus physical cash and digital money) in two significant ways: (1) It is more durable (it's backed up by many more servers across institutions than traditional digital money that is backed up only by the servers of an individual bank); and (2) it is more portable (as it is more seamless to move money on a single decentralised ledger than across different centralised ledgers). Money is supposed to be the most frictionless asset in society, and crypto currency is the most frictionless form of money to date.

match sticks, but it is more convenient to think of its price in terms of money as all other assets are priced in local currency which makes for more efficient comparisons and informed decisions. What is also crucial to understand is that there is a big distinction between a token and its value. An institution can control the issuance of its own token (whether it is a bond issued by a corporation or currency issued by a central bank), but cannot sustainably stipulate what the value of that token is. The market always decides the value.

2 CENTRAL BANKING REIMAGINED

2.1 CENTRAL BANK ISSUED CRYPTO CURRENCY – THE THIRD FORM OF MONEY

Currently, government money (e.g., USD, ZAR, GBP) can only be held in two forms: Physical cash (physical bearer instrument) or digital money in a bank account (digital registered instrument). Crypto currency is a **new form of money** that can be offered as a third form of central bank issued money beyond physical cash and digital money. We believe it is only a matter of time before central banks issue their own crypto instruments in the form of **central bank issued crypto currencies (CBCCs)**. Indeed central banks from Canada to China have expressed openness to blockchain and CBCCs.

While the term CBCC may scare some in the regulated space as “crypto currencies” have become associated with unregulated tokens of value, the term merely differentiates it from the digital money we have come to know that sits on commercial banks’ balance sheets as liabilities. Its name is derived from the cryptography that allows it to be a crypto instrument.

Just as no distinction is made between the value of a physical \$100 bill and \$100 in digital money that appears in an online bank account, so too would the value of \$100 in CBCC be the same as the first two forms of money. The currency would remain the same. Only the form would change. The emergence of CBCC would not change the money supply⁶ in an economy. The introduction of a third form of regulated money, CBCC, would replace another form of money to keep the money supply constant *ceteris paribus*. Just as one deposits a \$50 note at the bank which gets replaced by \$50 in an online bank account, so too would \$50 in CBCC have to replace some other form of money already in circulation. A central bank could easily set up a trust account to receive digital money (which it could take out of circulation) and issue a corresponding amount of CBCC to be sent to a wallet address of the digital money sender. In this way, the form of money as we know it could migrate from digital money to CBCC.

2.2 BENEFITS FOR CENTRAL BANKS AND REGULATORS

By migrating the predominant form of money in an economy to CBCC on a sovereign blockchain (more on sovereign blockchains in the next section), a central bank could observe in real time the transactions in an economy to better understand the velocity of money, and to gauge the health of the economy on a daily or even hourly basis. Once such a sovereign blockchain is created with a CBCC, other financial instruments such as bonds, equities, derivatives and even land and car registries could migrate to the same sovereign blockchain. This would allow the central bank to conceivably see the creation of all commercial bank assets in an economy

⁶ Money supply is defined as the total amount of monetary assets in an economy’s currency, the summation of physical notes and coins as well as digital money (the nuances of narrow and broad money definitions of M0, M1, M2 and M3 are not pertinent to the point at hand).

in real-time, including the categorisation of those assets (e.g., collateralised loans vs unsecured loans). Such transparency is invaluable to any central bank and would make decision-making more informed, timely and effective.

With a view of all transactions in an economy, anti-money laundering initiatives would be greatly enhanced. As it stands, payments from customers at a single bank are not always seen by the regulator as they are updates to that particular bank's ledger and do not get processed through a national payments system, making the historical flow of money difficult to track. In contrast, a sovereign blockchain would allow the movement of money to be traced through a historical path of transactions on a single decentralised ledger.

Tax collection could be revolutionised through the use of smart contracts on a blockchain. Tax could be collected at the point of transaction in real time, changing the entire system of tax collection from “after-the-fact collection” to “in-the-moment payment”. Imagine every payment to a retailer being automatically split at the time of payment such that 14% (value-added tax for example) would be paid directly to a government address with no inconvenience or cost to the customer or merchant. Such a system would significantly reduce the burden and cost of tax compliance for the merchant (as they would be paying their taxes automatically throughout the year) and improve collections for the tax authority.

This is just one example of how tax could be streamlined, but other examples abound – automated Capital Gains Tax when a vanilla asset is sold (the blockchain would have the history of what the asset was initially bought for and a smart contract could calculate the tax owed and pay both the seller and the tax authority in a single transaction); automated transfer duty on property sales, automated income tax payments when salaries are paid etc. The very notion of a withholding tax could become obsolete.

The blockchain would also allow the “codification of money”. Imagine a world in which the money paid into the account of the Department of Education could only be disbursed to accounts associated with schools or where money sitting in the government's social grant account could only be paid to accounts of individuals flagged as eligible to receive those grants. The combination of the codification of money and the transparency that the blockchain allows would go a long way in combatting corruption.

2.3 SOVEREIGN BLOCKCHAINS – THE IMPENDING CENTRAL BANK PLATFORM

Sovereign blockchains, as the name suggests, are blockchains that are established for a common currency area (usually a nation) under the jurisdiction of a single central bank. These blockchain networks are “permissioned” or “private” networks, in which nodes on the network need to be known and trusted. This is juxtaposed with “public” blockchains where anyone (i.e., untrusted parties) can download some software, establish a node and start participating in a particular blockchain network. The trouble with “public” blockchains

is that they are currently very expensive⁷ to run and slow to process transactions. These drawbacks are due to the untrusted nature of these public blockchains. Participants need to prove to one another that they have exerted effort in contributing to the network and are therefore eligible to be rewarded with fees and the issuance of the native currency of the blockchain (e.g., Bitcoins). The introduction of trust into a blockchain environment, making it “permissioned”, eliminates the burden of proof needed in a public environment, reducing costs dramatically and increasing transaction speed by several orders of magnitude⁸.

Central banks would be the moderators of these permissioned networks and would decide who would be permitted as nodes. It seems natural that the first nodes on a sovereign blockchain would be the banking institutions that central banks currently regulate, as these institutions are already well known to the central bank. In addition to selecting the trusted nodes, central banks would also issue the first asset on a sovereign blockchain: CBCC. Other asset classes would follow, but as money is the most common asset in an economy, starting with the issuance of money on a blockchain would facilitate a myriad of use cases.

The trusted nodes on the sovereign blockchain would perform a few functions:

1. Participate in the validation of transactions in the network (to prevent double-spending)⁹
2. Keep an updated record of the ledger and archive past transactions in a state system
3. Submit transactions to the network on behalf of others (i.e., their customers)

Establishing a sovereign blockchain with CBCC would provide tremendous benefit to an economy by reducing settlement times and costs for a banking industry (moving several institutions onto a single, yet distributed, ledger is powerful). Indeed, an economy’s payment system could eventually be replaced with a sovereign blockchain performing the role of a Real-Time Gross Settlement (RTGS) system.

The world is not yet ready for a permissioned supranational blockchain run by governments. Technology is not the impediment here, politics is. The nation-state is the largest organisational unit with a binding rule of law backed by an executive force. Humanity has attempted and achieved the unity of the family, tribe, city-state and nation, but has not yet established an international legislature, judiciary and executive force. Without this supranational structure supported by a community of federated nations, trust between nations would be difficult to secure and an international regulated blockchain would need to depend on a trustless consensus algorithm.

⁷ Most of them use proof-of-work consensus algorithms that can cost hundreds of millions of USD every year in the form of electricity consumption (as is the case with the Bitcoin network which is estimated to cost ~USD400m p.a. based on 2016 figures) let alone the hardware required. However, solutions such as Proof-of-Stake can bring the cost of public blockchain networks down significantly.

⁸ While the Bitcoin blockchain can currently process four to seven transactions per second, permissioned blockchains (depending on their architecture) can process well over tens of thousands of transactions per second.

⁹ There are several options of how this could happen, including: (1) a round-robin consensus algorithm; or (2) a single time-stamping service (with several fail-over services) that distributes time-stamped transactions to all nodes. Several remuneration models – from fee income to tax credits – could work to incentivise trusted nodes on a sovereign blockchain.

However, the recognition that some sovereign states could collude to bring down another state's economy by not validating their transactions (an ultimate form of economic sanctions) would dissuade any government from joining such a supranational network today. As such, a sovereign permissioned blockchain remains our focus for now.

2.4 THE TRANSITION TO CRYPTO BANKING

The establishment of a sovereign blockchain with CBCC opens up new possibilities for a completely new banking paradigm – a crypto banking paradigm. Central banks have started speaking more openly about broadening access to their balance sheets and CBCC on a sovereign blockchain would allow this. The sequence of issuing CBCC into an economy could be as follows:

1. **Slowly replace commercial bank reserves sitting with the central bank to CBCC.** This would ultimately transform current national payment systems into blockchain based RTGS systems;
2. **Migrate commercial bank liabilities to CBCC.** Private keys of the CBCC would be managed by commercial banks and therefore remain as liabilities to their depositors. Central banks could now see all transactions in the banking system (vs. interbank transfers only as is now the case). With control of the CBCC private keys, commercial banks would remain as credit originators, lending CBCC to create assets. Commercial banks would still need to keep their own ledger of liabilities;
3. **Allow non-banking institutions to hold their own private keys.** Such a move would allow the withdrawal of deposit liabilities from commercial banks and could impact liquidity and credit creation in the banking system if not managed carefully. To mitigate these risks, central banks could lend commercial banks a corresponding amount of CBCC as is withdrawn by non-banking institutions (more on the interest rate later). This would mitigate both liquidity risk and any threat to credit creation by the banks as the quantum of commercial bank liabilities would not be impacted. Only the funding source would change from non-banking institutions to the central bank.
4. **Allow individuals to hold their own private keys.** Again, this would allow further withdrawals of deposit liabilities from commercial banks. Central banks could again mitigate the impact on liquidity and credit creation by lending CBCC to commercial banks in an equal quantity to the withdrawals.

The above sequence of events raises some pressing questions: Why would non-banking institutions and individuals want to hold their own private keys? Wouldn't it be more risky to hold one's own private keys than to entrust them to a bank? Why would central banks want to go through so much effort to introduce a new form of money such as a CBCC on a blockchain? Let's look at these questions one at a time:

Why would non-banking institutions and individuals want to hold their own private keys?

A key characteristic of our current fractional reserve banking system is that banks engage in maturity transformation (accepting short-term liabilities and creating long-term assets). Depositor funds, therefore,

cannot all be withdrawn at the same time, otherwise a run on the bank would ensue. As such, a great deal of public confidence is required for any fractional reserve banking system to function. Runs on banks are not theoretical. While they can be mitigated by deposit insurance schemes, there is always credit risk against a bank holding money. The ability to hold the keys to one's own money eliminates this credit risk and removes dependence on the market's collective faith in a banking institution.

Wouldn't it be more risky to hold one's own private keys than to entrust them to a bank?

Yes it would be. And it is reasonable to think that private keys (especially those of individuals) could be managed by trusted service providers. But these service providers wouldn't necessarily need to be banks. The distinguishing characteristic of a bank (vs. other financial institutions) is that it can accept deposits. Managing keys is different to accepting deposit liabilities. Key managers may be more akin to asset managers (who can only do with assets what the owner allows) than banks. These service providers would conceivably have "currency-under-management" (similar to "assets-under-management" at investment management companies) rather than deposit liabilities and would therefore not be able to on-lend the "currency-under-management" as it would be off-balance sheet.

Why would central banks want to go through so much effort to introduce a new form of money such as a CBCC on a blockchain?

There are three main reasons:

1. It would give central banks much more insight, precision and control of the monetary policies they wish to implement;
2. It would create a much more stable financial system without the need for collective confidence in banking institutions, a world in which bank runs could not exist; and
3. It would bring down costs¹⁰ and promote increased financial inclusion.

Imagine a world in which banks are not deposit-taking institutions and the only source of funding for banks is  the central bank or through the issuance of bonds. As soon as a loan is made by a commercial bank, it would be "deposited" onto the sovereign blockchain and would essentially be a direct liability of the central bank. Such a system would require central banks to lend to commercial banks on an unsecured basis.

While we are currently accustomed to central banks lending money on a secured basis (i.e., in exchange for other highly-rated financial assets), there is no reason that central banks could not lend to banks on an unsecured basis. Central banks lending to commercial banks on an unsecured basis would add to the asset base in an economy, rather than liquidating debts (such as government bonds and mortgage-backed securities) as is currently done in quantitative easing programmes. But again, why would central banks want to do this? It

¹⁰ USD15-20bn per annum could be saved in banking infrastructural costs by 2022 according to Oliver Wyman.

ultimately boils down to central banks being the ultimate creators and destroyers of money in the economy. Right now, this is not the case.

Today, the role of money creation sits with commercial banks¹¹. As soon as they lend money, a new deposit is created and therefore new money is created in the economy. In a blockchain-enabled world, central banks could be the predominant lenders of CBCC to commercial banks on a matched basis (i.e., the term of the liability would be equal to the term of the asset created). The central bank would become the creator of money, and commercial banks would play a role of credit origination engines, passing on the money from the central bank to those they deem creditworthy.

The implication of this is that the central bank could have a funding curve that could be programmatically applied every time a commercial bank made a loan (i.e., every new asset created by a bank could be automatically funded by a matching liability term to the central bank at the funding rate for that tenor). A more stable narrow banking model would therefore be created. The funding curve could be used to implement monetary policy in a much more effective way as it would directly affect a much higher proportion of bank funding than it does today. The central bank could assign prudential limits to banks and monitor their non-performing loans (NPLs). Any bank that transgresses NPL limits on a sustained basis may lose their license (i.e., their right to receive funding from the central bank).

A fascinating result of this model is that while credit creation would continue in the same way as it does now, the major weakness of our current fractional reserve system would be avoided – even in times of a bank failure (i.e., the loans of a bank not being repaid causing the bank to become insolvent), not a single depositor's funds from the real economy would be affected. The concept of a “run on a bank” could be eliminated. This is because there would be no depositors in this system (remember, banks would not be depository taking institutions) as all funds would be held as a CBCC on the sovereign blockchain without being a liability of any commercial bank.

In this model, the impact of a bank failure (beyond capital losses for shareholders) would be the central bank not getting its loans to that bank repaid and more money remaining in the economy than anticipated. In such a situation, if too much money remains in the economy, the central bank could use some of its other tools (e.g., open market operations to sell some of its assets) to drain some liquidity out of the system (see Appendix: Central Bank Mandates and Tools).

This new model of banking - “crypto banking” - leads us to the question of the search for yield where money does not have to be a liability of a financial institution any longer. There are two key points to consider here: (1) A sovereign blockchain could be structured such that all CBCC attracts an interest rate (positive or negative) and

¹¹ Central banks can liquidate assets by taking an illiquid asset out of circulation and replacing it with digital money, but commercial banks are the institutions that create new money through the fractional reserve banking system.

could be controlled directly by the central bank¹²; and (2) Individuals and institutions could still be enticed to lend their money to financial institutions in search for yield – not as depositors but as bond-holders – but this would be a deliberate decision to take on credit risk for enhanced return. No one would be required to take on credit risk in this system, making the financial system more stable.

Financial stability of this system would be further enhanced once other assets start migrating to a sovereign blockchain (e.g., bonds, equities, mortgages and more). This would make a true Delivery-vs-Payment (DvP) transaction possible through atomic swaps¹³, and thus eliminate settlement risk from the system. Without settlement risk, capital costs would also reduce, bringing down both direct and indirect costs associated with settlement risk.

To recap, a sovereign blockchain with CBCC would greatly increase transparency¹⁴, reduce credit and settlement risk, increase the stability of a banking system and promote financial inclusion through lower costs. Central banks should welcome this with open arms.

2.5 A WORD OF CAUTION

Central banks today have a great challenge on their hands. Anaemic growth and inflation rates plague much of the world economy, government fiscal stimulation is hindered by burdensome public debt levels, and conventional monetary policy tools are being tested in a near zero (and even negative) interest rate environment in major economies. In an effort to fulfil their mandates to support sustainable economic growth, central banks have turned to unconventional monetary policy tools, introducing new money into their economies at unprecedented rates through the purchase of long-dated financial assets, and venturing into negative interest rate environments in order to stave off deflation. This could be dangerous.

Value has always existed in society. However, the unit of account (or measurement) of that value has often changed. It is critically important for anything that holds value to retain its characteristic of scarcity. Historically, money remained scarce as it was predominantly in the form of **commodity money** such as gold or silver. This money was limited in supply by virtue of the commodity's natural scarcity and limited rate at which new sources of the commodity could be mined. This element of scarcity was eroded slightly with the introduction of **representative money** – a token or piece of paper that was redeemable into a commodity (such as gold or silver). This is because representative money could be issued in excess of the underlying commodity reserves

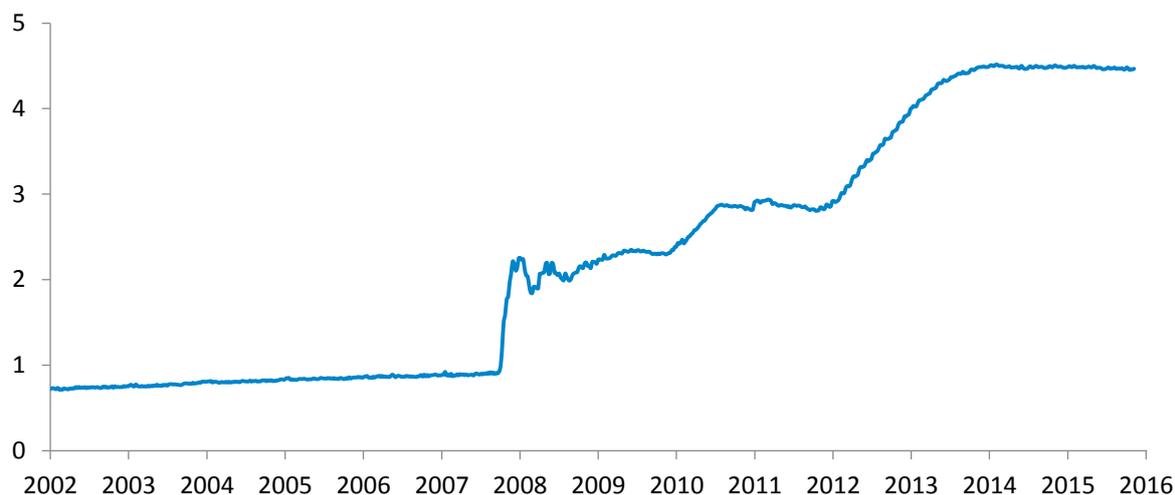
¹² In effect, a positive interest rate in this model would amount to increasing money supply and a negative interest rate would result in decreasing money supply.

¹³ An atomic swap is where two legs of one transaction are either both processed together or none of them is processed at all.

¹⁴ Increased transparency is often accompanied by worries about privacy. Just as it is in today's system, privacy will be a critical element of a blockchain-based financial system. However, regulators will want the ability to identify sources and destinations of funds (given due cause) for anti-money laundering / counter terrorist financing (AML/CTF) purposes. As such, participants on a sovereign blockchain would need to be validated (similar to Know-Your-Customer regulations today). Such identity validation is likely to be done by trusted institutions to the regulator, whose reputations will be determined by their record of maintaining the strictest standards of privacy for their clients. Advances in cryptography now allow a shared ledger that preserves privacy while still allowing the validation of transactions (e.g., zero-knowledge proofs).

(the gold standard was an example of representative money). But the constraint on scarcity was all but eradicated with the introduction of **fiat money** which had no recourse to any underlying commodity (as an example, the US abandoned the gold standard in 1971). Central banks now had a currency that had no backing to anything scarce, paving the way for money printing on the scale that we have seen in recent years.

Figure 2: Federal Reserve Balance Sheet, Total Assets (USD trillions)



Source: Board of Governors of the Federal Reserve System

With this ability to print currency at will, many major central banks are trying to raise the Consumer Price Index (CPI) through the injection of money into the economy (quantitative easing) in order to stimulate aggregate demand and economic activity. This new money, however, does not always find its way into the products and services that comprise CPI. Instead, this liquidity often makes its way into asset classes such as bonds and equities which have recently been reaching record highs – a bizarre situation given the uncertainty and placid economic growth around the world¹⁵.

Without success, several central banks pour more money into their economies hoping for a different outcome. It should be noted that central banks engage in policies to devalue their currencies against real goods and services every year (what we call inflation), to encourage spending rather than holding onto a depreciating asset (fiat currency). The challenge that central banks face is maintaining the public's faith in their currencies while trying to stimulate the economy.

While central banks have transitioned to currency whose supply is unrestrained and determined by a committee, non-government-backed crypto currencies have emerged, many of which have scarcity embedded into their

¹⁵ While it is noted that with decreasing interest rates (or discount rates) the net present value of cash flows increases, rendering equities and bonds more expensive, we have a bizarre situation in valuing assets in which the discount rate of cashflows seems to be playing a stronger role in valuations than the underlying fundamentals that determine those cashflows.

deterministic issuance algorithms (outside the control of a committee or an individual). This gives individuals and institutions the choice to hold value in a new asset class that is an appreciating asset (due to its scarcity).

While crypto currencies outside the government's ambit are still peripheral, their very existence and price in terms of fiat currency (Bitcoin is trading at ~USD730 per coin at the time of printing) should give pause to central banks to ensure they do not inadvertently undermine their own currencies through the implementation of certain monetary policies whose effectiveness may be limited. Central bankers have a great task to disprove those economists¹⁶ who claim that monetary policy stimulus can sometimes be compared to pushing on a string.

As CBCCs on a sovereign blockchain would make money more frictionless, careful consideration would need to be made regarding the implementation of existing monetary policies in a new paradigm. Just as an ice-skating rink promises a fast and frictionless experience, so too does it increase the potential for injury for those whose technique is not mastered. Central banks need to proceed with caution.

2.6 THE IMPORTANCE OF REGULATORS

It is fashionable in some parts of the crypto community to proclaim the end of regulation with the coming of blockchain. This is misguided. As a society we collectively choose to have regulators to ensure justice is upheld, and as the Economist recently noted: "Without justice, people will lose their trust in everything except for weapons." Laws, regulations and their enforcement are intended to protect and promote the best interests of society. We derive great benefit from these on a day to day basis. The fact that people can walk unarmed in society without fear of harm (for the most part) is testament to the liberties we enjoy from law and order.

However, humanity is suffering from a crisis of confidence in many of our public institutions and regulators globally. And so to say that we need regulation certainly does not imply that all regulation is good. Some regulations do not serve the best interests of society and as such should be abandoned. But we should not confuse bad regulation with the desire to eradicate regulation all together. Society needs laws and regulations and the ability to enforce them.

Regulators have an extraordinary opportunity and responsibility to nurture and shape this new crypto banking paradigm for the benefit of society.

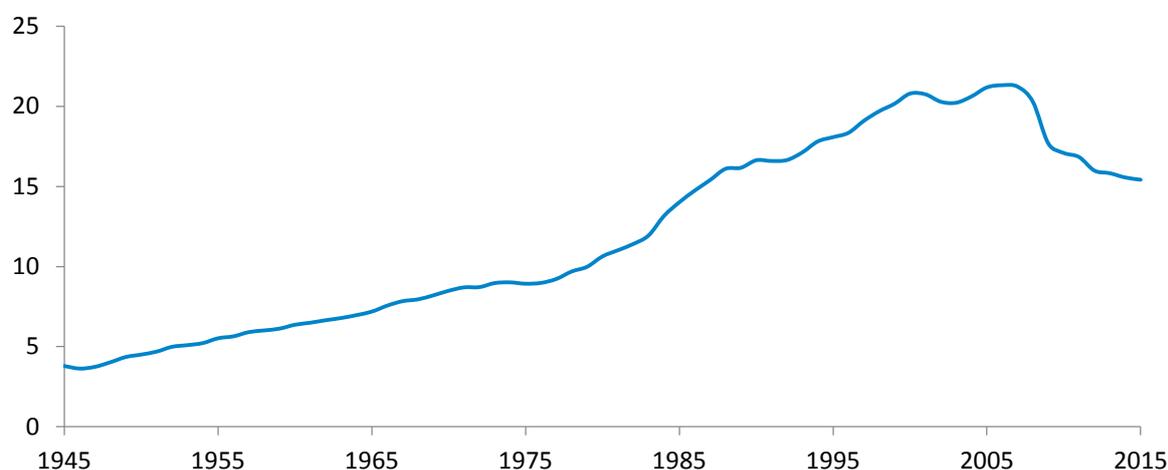
¹⁶ This phrase is often attributed to John Maynard Keynes, although it seems to have been first used by Congressman Alan Goldsborough in 1935.

3 COMMERCIAL BANKS IN A NEW WORLD

3.1 THE BANKING DILEMMA

In the early 1990s, postal services around the world faced a strategic dilemma with the birth of the Internet: (1) Ignore the new technology and continue with business as usual; or (2) Endeavour to understand it and adapt if required. The choices they made did not change the course of the Internet. However, those choices did dictate their survival and performance in a new paradigm where an additional, and more frictionless, form of communication was available to humanity. Their customers were no longer solely dependent on postal services for the delivery of written communication. Fast forward a couple of decades and hindsight tells the following story:

Figure 3: Pieces of mail handled by the US Postal Service¹⁷ (billions)



Source: United States Postal Service

Today, banks face a similar dilemma with the emergence of blockchain. Just as the Internet decentralised the flow of information and gave people another choice of how to communicate, so too has the emergence of the crypto instrument decentralised value and given people another option to store and transfer digital value without the need for a trusted financial intermediary. However, just as postal services haven't disappeared (and in fact certain parts of their business like parcel deliveries have prospered¹⁸), banks are not about to disappear either.

Blockchains will have many positive outcomes for banks, from reducing settlement risk and associated capital costs, to reducing costs associated with back office functions such as confirmations, reconciliations, and exceptions, to the possibility of reducing core banking system costs as the blockchain may replace much of the

¹⁷ The UK mail volumes show the same trend as the US with overall inland mail volumes declining by more than 4% p.a. from 2005 onwards.

¹⁸ Parcel deliveries in the UK grew at a rate of 4.1% p.a. from 2005-2012.

need for a banking general ledger in the future. However, far from being complacent, banks need to reflect on the core services they offer their customers and anticipate how to adapt their models to thrive in a new financial paradigm. Fundamentally, banks are in the monetary value business and provide four core services¹⁹ to their customers:

1. Value storage (e.g., deposits, custody services)
2. Value transfer (e.g., payments, FX, bonds, equities, commodities)
3. Value provision (e.g., debt or equity)
4. Value protection (e.g., insurance or derivatives)

3.2 VALUE STORAGE

What many do not realise is how high the proportion of digital money is in our economies (93% of ZAR is digital and 7% exists as physical notes and coins²⁰). All of this digital money must be placed with trusted banking institutions at the moment. There is, in fact, no other way to currently store this digital money outside a trusted and regulated institution. Commercial banks have the exclusive right to store digital government currency for the public.

The issuance of CBCC would lead to the decentralisation of value storage. This is significant because if an individual or institution can manage their own private key and therefore control their own CBCC at little to no cost, they have a disincentive to deposit their money with a bank if bank charges are anywhere above zero. Furthermore, as mentioned previously, any commercial bank deposit carries credit risk against that institution. So the choice of holding a CBCC removes credit risk for deposit holders, further disincentivising them to deposit money with a commercial bank. Holding CBCC directly on a sovereign blockchain would be akin to holding money directly with the central bank (and thus being protected against any possible run on a commercial bank). All these factors could adversely affect commercial bank funding and a bank's endowment of non-interest bearing liabilities. In the extreme case, bank deposits could become an anachronism. The role of commercial banks could start to change from custodians of funds to custodians of private keys.

3.3 VALUE TRANSFER

In addition to affecting bank deposits (value storage), blockchain will impact the global payments industry (value transfer). Globally banks earn ~40% of their revenues from payments, representing a USD1.7tn revenue stream²¹. This lucrative industry has already attracted technology firms (e.g., Google, Apple, Facebook) as well as a host of other start-ups (e.g., Stripe, Venmo, WeChat) which have started to disrupt the space without the use of blockchain. Blockchain technology has the potential to disrupt these disruptors. To understand this

¹⁹ Banks also provide advice across all four core services.

²⁰ As a percentage of M3 money based on South African Reserve Bank data.

²¹ McKinsey & Company, 2015. "Global Payments 2015: A Healthy Industry Confronts Disruption."

better, it is necessary to take a fundamental look at the payments industry to understand how it is currently being disrupted. This is happening in one of two main ways:

1. A wrapper on top of the current payments plumbing (e.g., Apple Pay, Google Wallet)
2. A single centralised platform that benefits from network effects and scale (e.g., M-Pesa, PayPal)

The “wrapper” model aims to ease the user experience by using technologies such as Near Field Communication (NFC) instead of swiping credit cards. However, the back-end is still built on credit card rails – i.e., a credit card is required to sign up to these services. The “platform” model also seeks to ease user experience and has been most successful on a platform like M-Pesa from Kenya. Instead of requiring credit card details, M-Pesa requires accounts to be pre-funded with cash. As long as enough people have a SIM card with Safaricom (the telecom operator that provides the M-Pesa service) users find value in the platform which enjoys the network effect and is self-reinforcing. All mobile money on the M-Pesa platform is backed 100% by Safaricom deposits in several Kenyan commercial banks. When transfers are made on the M-Pesa platform, M-Pesa just updates its ledger that contains all M-Pesa account balances. However, this model is limited by how many people can be signed up to the platform and is generally constrained by national borders. PayPal is a single centralised platform that has transcended the national border, but still remains dependent on traditional banking models and credit card rails.

Ultimately, payment systems currently rely on updating several different ledgers at different institutions and ensuring that those ledgers reconcile. If a central bank decides to institute a sovereign blockchain and migrates account holders’ digital money (sitting on commercial bank ledgers) to CBCC, a single (although distributed) ledger is created for an entire economy. This can reduce costs for the financial system significantly as there would be no need for reconciliation of payments as most payments would move to a single blockchain-based ledger.

Regarding FX, we anticipate a much more streamlined payment process in the future where a cross-border payment will be as easy as sending a cross-border email. We believe there will be a network of sovereign blockchains that host CBCCs managed by central banks for each currency zone²². In such a scenario, exchanges straddling these blockchains would be the means by which FX payments are transacted seamlessly. As long as there are different currencies around the world, price discovery is imperative between currencies and multiple exchanges will compete to provide this service.

3.4 VALUE PROVISION AND PROTECTION

While the two above mentioned core services of banking – value transfer and value storage – will be most impacted by blockchain in the foreseeable future, the last two core banking services – value provision and value

²² We also believe that non-government backed crypto currencies are here to stay and that the future will be a network of both sovereign and non-sovereign blockchains.

protection – will not be immune to change. As the financial ecosystem migrates onto blockchain and customers have control over their own data and assets, blockchain may provide a means for individuals to expose their data²³ (e.g., 12-month transaction history) to credit algorithms that offer a matching service with providers of capital. Moving into the world of smart contracts will help manage risk; for example, margin calls for derivatives could be made every five minutes instead of every 24 hours.

3.5 TRUST IS HERE TO STAY

Although there will be threats to business models of trusted financial intermediaries as they currently stand, the need for trusted intermediaries will certainly not disappear. The advent of blockchain has led to voices proclaiming trust between parties in a financial system is no longer needed. As Nakamoto noted in the Bitcoin white paper: “What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.”²⁴ With blockchain algorithms that have been designed to achieve consensus among untrusted nodes (like the Bitcoin protocol), such voices seem to be vindicated. However, such algorithms are effective only for digital assets. These assets are born, live and potentially die in a digital universe.

We live in a physical world and when digital tokens that represent physical assets (e.g., houses, cars, diamonds, art etc.) are issued onto a blockchain, there is a need to verify that these digital tokens are in fact backed by the physical assets they claim to represent. It is, however, economically inefficient to verify everything for oneself. The need for verification reintroduces the need for a trusted intermediary. For example, when blockchains are used to capture events that will trigger the release of funds (e.g., trade finance applications), the parties that are capturing the events at each step of the process will need to be trusted. Think of a smart contract that will hold an importer’s funds in escrow until a digital bill of lading is issued onto a blockchain by the carrier to indicate the goods have been shipped by the exporter. The importer needs to trust that the carrier is not in cahoots with the exporter.

More and more references to “escape hatches” in smart contracts have been made in light of some of the recent challenges the blockchain community has experienced. In effect, these escape hatches provide for an emergency exit in case something goes wrong with the code of a smart contract. The question then becomes: “Who can invoke these escape hatches?” If the escape hatch can be triggered by some but not all, trust is invested in those who have the right to trigger. And if the escape hatch can be triggered by all, immutability is sacrificed and a blockchain ceases to be a blockchain. As such, the very notion of an “escape hatch” assumes the existence of trust in a system.

²³ This is already happening in the non-blockchain space with directives such as PSD2 that require API integration into financial institutions and giving customers more control over their own data.

²⁴ Nakamoto, Satoshi (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System.”

CONCLUSION

Just as the unfettered flow of information revolutionised human interaction with the coming of the Digital Age, so too will the possibility of unconstrained flow of value transform human trade and industry. Blockchain has given birth to the crypto instrument, a hybrid of a digital bearer instrument and a digital registered instrument, the most frictionless form of value that has ever existed.

For the very first time, digital assets can be held in custody by the owner of the asset, without relying on a trusted party such as a financial institution. We foresee a third form of fiat currency (after physical cash and digital money), a central bank issued crypto currency (CBCC), which will soon be established on sovereign blockchains across the globe. These blockchains will be multi-asset ledgers onto which bonds, equities, derivatives, contracts and a plethora of other records can be registered.

We believe central banks will embrace CBCCs as a new form of money as it will significantly enhance their ability to understand their economies, reduce systemic risks, and facilitate more effective transmission of monetary policy throughout the economy. A remarkable outcome of the issuance of a CBCC on a sovereign blockchain would be the elimination of bank runs – a feat that cannot be overestimated for financial systems. A more stable banking system can be envisioned, discarding some of the dangers of a fractional reserve system without sacrificing its benefits.

The codification of money – programming conditions for the use of funds in a particular transaction – will go a long way in combating graft in business and government alike. Only once CBCCs are issued onto sovereign blockchains, can the full might of this new technology redound to central banks and their economies. Much responsibility rests on the shoulders of central bankers to ensure humanity sees the benefits of this technology sooner rather than later.

While many have hailed the end of trusted intermediaries in financial systems due to the emergence of blockchain, this view is misinformed. Trusted parties will not disappear, but their roles will certainly change. We anticipate trusted intermediaries having “currency under management” (which would not be deposit liabilities) as well as managing the link between physical assets and their digital representations on blockchains.

Just as post offices do not generate the content they transport and their traditional business models were impacted by the introduction of a new decentralised communication mechanism, banks too do not generate most of the funding for the assets on their balance sheet (banks are the most highly leveraged institutions in society) and the introduction of a new decentralised value transfer and storage mechanism will affect traditional business models.

CONCLUSION



Commercial banks today need to consider their future roles in the four core services of banking: (1) value transfer; (2) value storage; (3) value provision; and (4) value protection. There is no doubt that the way these services are performed will change. We stand at the threshold of a new epoch in financial services.

We welcome your thoughts, comments and feedback.

Farzam Ehsani – Leader of Blockchain Initiative

- farzam.ehsani@rmb.co.za
- +27-11-282-1565

Acknowledgements

Coenie Beyers – Blockchain Engineer

Peter Munnings – Blockchain Technical Lead

APPENDIX: CENTRAL BANK MANDATES AND TOOLS

The mandate of all central banks consists of maintaining monetary and financial stability through a combination of price stability (i.e., a targeted inflation rate), sustainable growth, full employment and sustained confidence in the currency²⁵. Central banks aim to achieve these mandates through the implementation of monetary policy tools (leaving fiscal policy to other institutions of government). These monetary policy tools include:

- **Discount rate for window lending** – the rate central banks charge commercial banks for short-term borrowings;
- **Open market operations** – the buying and selling of securities to influence interest rates (quantitative easing falls into this category as it aims to bring down long-term interest rates by buying long-dated assets such as government bonds and/or collateralised securities such as mortgage-backed securities);
- **Reserve ratio requirements** – stipulating the cash reserve requirement of commercial banks to either restrain or encourage credit creation (and therefore money supply) in the economy; and
- **Forward guidance** – the attempt to influence interest rates by signalling to the market what the central bank intends to do with future actions.

Central banks deploy these tools to influence the behaviour of commercial banks and thereby try to control factors such as inflation, economic growth, asset bubbles, and unemployment rates indirectly through commercial banks. As such, monetary policy tools are blunt instruments. They depend on data that is obtained through reports from commercial banks that are out of date by the time they arrive and, like all reports, are prone to inaccuracies. As described in this paper, in a crypto banking world with sovereign blockchains and CBCC, central banks could have much more insight into their economies and improve their control and transmission of monetary policies.

²⁵ Central banks have slight variations in mandate

DISCLAIMER

This research has been written by the Found^{er}ry blockchain team at FirstRand Bank Limited (“the Bank”) (acting through its Rand Merchant Bank Division). Whilst all care has been taken by the Bank in the preparation of the opinions and forecasts and provision of the information contained in this report, the Bank does not make any representations or give any warranties as to their correctness, accuracy or completeness, nor does the Bank assume liability for any losses arising from errors or omissions in the opinions, forecasts or information irrespective of whether there has been any negligence by the Bank, its affiliates or any officers or employees of the Bank, and whether such losses be direct or consequential. Nothing contained in this document is to be construed as guidance, a proposal or a recommendation or advice to enter into, or to refrain from entering into any transaction, or an offer to buy or sell any financial instrument.

This communication is not intended nor should it be taken to create any legal relations or contractual relationships.

FirstRand Bank Limited is listed on the JSE and Namibian Stock Exchange and is an Authorised Financial Service Provider under South African law. FirstRand Bank Limited is authorised and regulated by the South African Reserve Bank. In the UK, FirstRand Bank Limited is authorised by the Prudential Regulation Authority and is subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of FirstRand Bank Limited regulation by the Prudential Regulation Authority are available from us on request.