COMMERZBANK
The bank at your side

Corporates & Markets

It’s not about the money

Peter Dixon
GLOBAL EQUITIES ECONOMIST
peter.dixon@commerzbank.com

The process of liquidity creation is increasingly less the preserve of central banks and ever more the result of actions in the wider financial system. In the wake of the shock posed by the 2008 Lehman’s bankruptcy, investors are less inclined to trust banks and their role in the monetary creation process. Developments in computing technology have enabled the rise of cryptocurrencies such as bitcoin which, its proponents claim, will eventually displace conventional money. These claims may be somewhat far-fetched, since it has yet to convince investors that it can replicate many of the functions of money. But the introduction of the blockchain technology, upon which bitcoin is based, represents a genuine revolution in the management of decentralised processing systems which has the potential to transform data management.

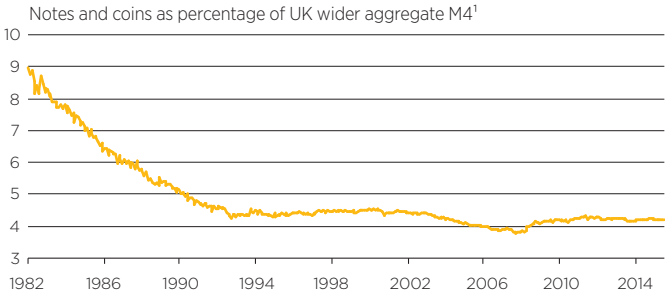
Money is as money does

Societies since ancient times have relied upon the exchange of goods and services to increase economic welfare. As economic systems became more sophisticated, increasingly complex transactions required the use of money as a medium of exchange, rather than barter. Money also took on the role of a unit of account which allowed goods and services to be priced in an appropriate manner. Moreover, as societies began to produce more than they could consume in any given period, it became necessary to find ways to store the surplus value. In this way, money became a means of storing wealth which could be consumed in future.

Monetary systems were originally based on a numeraire, with gold assuming this role from ancient times. Over time as institutional frameworks became stronger, societies became more accepting of fiat money – any money deemed by the state as being legal tender. By the 1970s the last remaining links between currencies and commodities in the industrialised world were severed, and in western economies today all the physical cash in existence is created by the central bank. But in a system of fractional banking, institutions are able to create loans which are a significant multiple of the value of funds deposited with them, secure in the knowledge that only a small proportion of their cash deposits will be called upon at any one time. As a result, cash today only makes up a small proportion of total liquidity – defined as cash and near-cash substitutes – in advanced economies (see Chart 1).

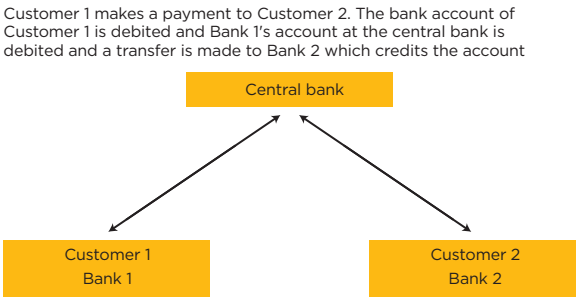
Although the concept of what we think of as money has changed over time, the process which facilitates payments between individuals is still recognisable as the system introduced in the 16th century. In effect, the financial system operates a ledger in which transfers between individuals are processed via clearing banks, in turn overseen by the central bank acting as the ultimate clearer (see Chart 2). Over the years, concerns have been expressed that central banks cannot be entrusted to maintain the value of money deposited in the financial system, due to their inability to get to grips with inflation, and this issue has become even more acute in the wake of the recent practice of quantitative easing (QE). Add to that the problems which resulted from high profile banking collapses in 2007 and 2008, and it is perhaps not surprising that investors are attracted by the idea of money which is not under the control of the banking system.

Chart 1: Cash is no longer king



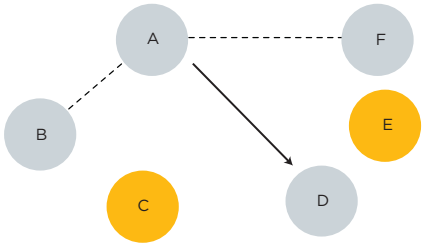
Source: Bank of England

Chart 2: Stylised representation of a conventional payments system



Source: Commerzbank Research

Chart 3: Stylised representation of a distributed payments system



Payments pass directly between users (A to D) but are verified by other users. New transactions are broadcast to 'miners' (B and F) and are added to the blockchain once verified, and other users (C and E) are informed.

Source: Bank of England, Commerzbank Research

It's less about the money and more about the blockchain
New technology has enabled the development of decentralised payments systems, which rely on encryption to maintain the ledger rather than entrusting it to a central entity. These new developments – of which bitcoin is the most widely known – explicitly rely on a community of mutually distrustful parties to ensure that the currency is not debased. In order to preserve the value of such currencies, their supply has to be limited and unlike conventional electronic money, which is created by the flick of a computer switch in the banking system, they are electronically 'mined'.

The supply of bitcoin can be expanded only by 'mining' new blocks which is designed to be a resource-intensive process, involving the solution of a complex random problem with a low probability of success. Once the 'puzzle' has been solved, the miner has to verify that they have title to the newly discovered block, which they do by creating a message which is then sent to the bitcoin network identifying the owner. This takes the form of a 'cryptographic hash function' which requires the miner to combine three inputs (a reference to the previous block, details of their candidate block of transactions and a special number called a 'nonce') and churns out a hash number which will determine whether the proof of work is accepted. Precisely because each of these transactions must confirm the integrity of the previous block all the way back to the initial transaction (or genesis block), this ledger can be thought of as a chain. Authenticating the so-called blockchain is computationally onerous, and because it relies on cryptographic methods it is near-impossible to falsify because it would require authenticating the chain all the way back to the genesis block.

It is this non-centralised nature of the ledger (the blockchain) which is the true innovation resulting from digital currencies. In the same way that the miners' verification process relies on encryption technology, so similar methods can be used to verify changes in bitcoin ownership arising from transactions between individuals (see Chart 3). The defining feature of a distributed payment system such as the blockchain is the manner in which consensus is achieved regarding proposed changes to the ledger. In conventional monetary systems, we have to trust the banking system to act in the best interests of participants and ensure that the ledger is maintained. Moreover, the keeper of the ledger (the central bank) has the ability to block certain types of transactions. But the blockchain offers a way around these constraints.

The Byzantine problems of cryptocurrencies
One of the most significant advances to come out of the adoption of blockchain technology is that it appears to have solved a long-standing game theory puzzle which has bamboozled generations of computer scientists – the Byzantine Generals problem. Cracking this problem offers an insight into how a decentralised currency system can operate. To get a handle on it, consider a thought experiment in which a group of generals (greater than two) are assumed to be outside a city, each with an army, and all want to invade the city. It is known that if at least half attack at the same time, they will be successful. But if they do not co-ordinate their plans to ensure they can muster the requisite number for the assault, they will be unsuccessful. They must thus collude in planning their attack, but the generals face three problems: they must (a) know whether their messages get through in the first place; (b) receive an acknowledgment indicating that the plans have been accepted and (c) verify that the information passed between them is true.

Computer scientists have struggled for 40 years to derive a network solution which will overcome all three of these problems but finally the blockchain appears to have managed it. Since the blockchain is arranged on a peer-to-peer basis, messages are transmitted to a user's immediate peers and the information disseminates quickly through the system. Thus, unless the user's connection is faulty, condition (a) is satisfied. The process of validating the blockchain outlined above satisfies condition (b).

Condition (c) has in the past proved more difficult to satisfy, but because the costs of generating a message are high (computationally onerous for relatively little reward), the costs of falsification are high. It is, of course, possible to falsify via collusion but because the system rewards those who maintain it (ie the miners) in the form of additional blocks, there is no reason why a majority of users should collude to produce an outcome which is sub-optimal[2]. In short, if we attach a cost to sending a message and ensure that only one person can send a message at a time, the authenticity of the blockchain is guaranteed.

Costs and benefits
From a systems perspective, the blockchain is a genuine revolution. In theory, therefore, it offers the possibility of eliminating many of the risks associated with the conventional ledger system. The most obvious of these is the credit risk resulting from the insolvency of an institution which owes huge sums to other parts of the financial system (as happened in the wake of the Lehman's bankruptcy). Another issue is liquidity risk in the event that a fundamentally solvent institution may not have the funds to process settlements that fall due (another problem which occurred as liquidity dried up in the wake of the 2008 banking shock). A third problem is operational risk, which may be the result of system failures such as IT.

Due to the fact that in a decentralised system transactions are conducted directly between individuals, there are no intermediaries to introduce credit and liquidity risk which are thus virtually eliminated. And since the technology is distributed across many users, operational risks are correspondingly reduced. However, one of the main risks faced by any financial system is fraud, which is not eliminated although its nature is likely to change markedly in a distributed payments system. Since agents do not have to disclose their identity when transacting in a decentralised system, there is less risk of identity theft. However, there is a greater risk of direct loss in the event that agents lose the private key which allows them to access their digital wallet. Any data lost in this way is not recoverable in a way that is possible when a password to a conventional online bank account is lost.

There may also be a bigger risk of systemic fraud in a distributed payments system. This might occur, for example, if hackers were able to gain access to a large proportion of the systems linked to the bitcoin network. It has been suggested that it may even be possible to hack into bitcoin mining networks by controlling less than 50% of the computing power, depending on factors such as their position in the network and the timing of when a hacker releases messages to the rest of the network. Anyone doubting the severity of fraud problems should recall the case of Mt.Gox, the exchange which at one stage was processing 70% of all bitcoin transactions. In 2014, it was closed down and subsequently liquidated following the discovery that 850,000 bitcoins belonging to investors had been stolen.

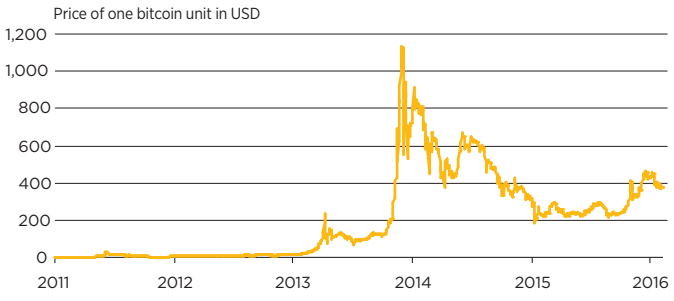
Subject to tackling these security issues, the distributed ledger system offers significant applications beyond the narrow confines of the payments system. It is theoretically possible, for example, that the existing financial market architecture in which securities are traded on exchanges, could be replaced with a decentralised system. Beyond the realms of finance, many systems which rely on digital record keeping could make use of this technology. For example, peer-to-peer file sharing networks could remove the need for centralised data storage across any number of applications. Some have even suggested that it could be used to create a more efficient system of voting, reducing the possibility of corruption and speeding up the process of tallying votes.

What of bitcoin?

But we end where we began, with the issue of money. After all, blockchain technology came into being in order to weaken the control of conventional institutions over other people's money. The process of mining for bitcoins, as we have demonstrated, is computationally arduous. Miners who discover new blocks are entitled to a reward of 25 bitcoins per block (prior to November 2012, each block yielded 50 coins and it is likely to halve again in 2017), subject to the constraint that the maximum number of bitcoins in existence is unlikely to exceed 21 million – a limit which it is anticipated will be reached in 2040.

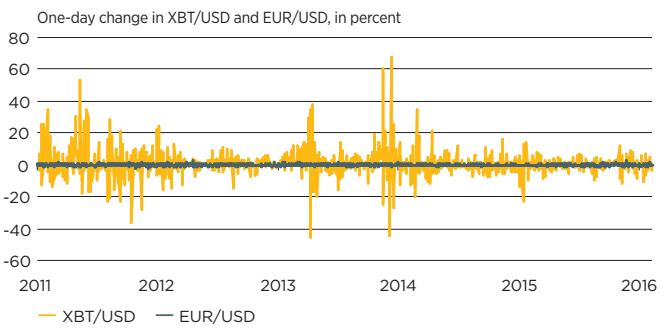
The extent to which bitcoin will displace other currencies is open to question. Although it has become more widely accepted as a medium of exchange, its use as a store of value depends very heavily on its stability. Chart 4 shows the extent of the swings in the price of bitcoin relative to USD whilst Chart 5 shows the one-day volatility compared to the EUR/USD exchange rate, and both are indicative of big fluctuations over the past five years. The huge increase in the value of bitcoin in 2013 was a speculative bubble driven by the fact that investors were concerned that its relative scarcity would send values rising over the longer term. As with any bubble, this soon collapsed as investors realised that many of the claims made for bitcoin were overblown.

Chart 4: The value of bitcoin has fluctuated sharply...



Source: Bloomberg

Chart 5: ...And it demonstrates high short-term volatility



Source: Bloomberg, Commerzbank Research

Indeed, distributed payment systems are unlikely to displace banks as legally trusted holders of money any time soon – after all, if you lose access to your electronic wallet, there is no-one to sue when things go wrong.

In addition, bitcoins will become ever harder to mine and the energy costs of providi ng enough computing power to mine the last few blocks may be way in excess of the return. Then there is the small issue that the currency supply is ultimately limited, which might eventually prove to be deflationary. In the round, the wider economic costs of bitcoin may be greater than the benefits which accrue to a relatively small number of adherents.

1 M4 Refers to different measures of money supply. Not all of them are widely used and the exact classifications depend on the country. M0 and M1, also called narrow money, normally include coins and notes in circulation and other money equivalents that are easily convertible into cash. M2 includes M1 plus short-term time deposits in banks and 24-hour money market funds. M3 includes M2 plus longer-term time deposits and money market funds with more than 24-hour maturity. The exact definitions of the three measures depend on the country. M4 includes M3 plus other deposits.
Source: FT.com/Lexicon.

2 In a system with n users, so long as n/2 are 'honest' the authenticity of the chain is technically guaranteed.

LAST WORD

The trials and tribulations of banks in the wake of the financial crisis have forced investors to think more carefully about the nature of money. The extent to which bitcoin and its many emulators will displace central bank issued money is moot: if it happens at all, it is a matter for the very long-term, and a move in this direction will likely only be triggered by a catastrophic failure of current arrangements. As bad as the events of 2008 were, the monetary system has coped – so far.
In the current 'lowflation' environment, there can be few complaints that central banks are eroding the value of money, even though returns on capital have been crushed by low interest rates, and matters might be different if central bank QE triggers a period of runaway inflation. But the bitcoin debate has sparked a genuine revolution with the introduction of the blockchain. In the years to come, even if bitcoin is relegated to a footnote in monetary history, blockchain technology is likely to still be with us, even if some of the claims currently made for it prove to be exaggerated.

Disclaimer

This document has been created and published by the Corporates & Markets division of Commerzbank AG, Frankfurt/Main or the group companies mentioned in the document ("Commerzbank"). Commerzbank Corporates & Markets is the investment banking division of Commerzbank, integrating research, debt, equities, interest rates and foreign exchange.

This is a financial promotion/marketing communication (together "communication"). It is not "investment research" or "financial analysis" as these terms are defined in applicable regulations and has not been prepared by a research analyst. The views in this communication may differ from the published views of Commerzbank Corporates & Markets Research Department and the communication has been prepared separately of such department.

This communication may contain short term trading ideas. Any returns or future expectations referred to are not intended to forecast or predict future events. Any prices provided herein (other than those that are identified as being historical) are indicative only, and do not represent firm quotes as to either size or price.

This communication is for information purposes only. The information contained herein does not constitute the provision of investment advice. It is not intended to be nor should it be construed as an offer or solicitation to acquire, or dispose of, any of the financial instruments and/or securities mentioned in this communication and will not form the basis or a part of any contract. Potential counterparties/distributors should review independently and/or obtain independent professional advice and draw their own conclusions regarding the suitability/appropriateness of any transaction including the economic benefit and risks and the legal, regulatory, credit, tax and accounting aspects in relation to their particular circumstances. Levels, bases and relief from taxation may change from time to time.

Any information in this communication is based on data obtained from sources believed by Commerzbank to be reliable, but no representations, guarantees or warranties are made by Commerzbank with regard to the accuracy, completeness or suitability of the data.

The past performance of financial instruments is not indicative of future results. No assurance can be given that any financial instrument or issuer described herein would yield favourable investment results.

This communication is intended solely for distribution to Professional Clients and/or Eligible Counterparties of Commerzbank. It is not intended to be distributed to Retail Clients or potential Retail Clients. Neither Commerzbank nor any of its respective directors, officers or employees accepts any responsibility or liability whatsoever for any expense, loss or damages arising out of or in any way connected with the use of all or any part of this communication.

Commerzbank and/or its principals or employees may have a long or short position or may transact in financial instrument(s) and/or securities referred to herein or may trade in such financial instruments with other customers on a principal basis. The information may have been discussed between various Commerzbank personnel and such personnel may have already acted on the basis of this information (including trading for Commerzbank's own account or communication of the information to other customers of Commerzbank). Commerzbank may act as a market maker in the financial instruments or companies discussed herein and may also perform or seek to perform investment banking services for those companies.

No part of this communication may be reproduced, distributed or transmitted in any manner without prior written permission of Commerzbank. This communication or the manner of its distribution may be restricted by law or regulation in certain countries. Persons into whose possession this document may come are required to inform themselves about, and to observe any such restriction.

By accepting this communication, a recipient hereof agrees to be bound by the foregoing limitations.

This communication is issued by Commerzbank AG and approved in the UK by Commerzbank AG London Branch, authorised by the German Federal Financial Supervisory Authority and the European Central Bank. Commerzbank AG London Branch is authorised and subject to limited regulation by the Financial Conduct Authority and Prudential Regulation Authority. Details about the extent of our regulation by the Financial Conduct authority and Prudential Regulatory Authority are available on request.

Italy: You should contact Commerzbank AG, London Branch if you wish to use our services to effect a transaction in any of the financial or other instruments mentioned in this communication.

Japan: Not for distribution in Japan

US: Not for distribution in United States

Canada: Neither Commerzbank AG nor any affiliate acts, or holds itself out, as a dealer in derivatives with respect to any Canadian person, in Canada as a whole or in any Canadian province, and nothing contained in this document may be construed as an offer or indication that Commerzbank is or stands ready to (in each case, with respect to a Canadian counterparty or within Canada) intermediate derivatives trades, act as a market-maker in derivatives of any kind, trade derivatives with the intention of receiving remuneration or compensation, solicit (directly or indirectly) derivatives transactions, provide derivatives clearing services, trade with a non-qualified Canadian party that is not represented by a derivatives dealer or adviser, or engage in activities similar to those of a derivatives dealer.

Commerzbank Corporates & Markets

Frankfurt
Commerzbank AG
DLZ Gebäude 2, Händlerhaus
Mainzer Landstraße 153
60327 Frankfurt am Main
Tel.: +49 69 136 44440

London
Commerzbank AG
London Branch
30 Gresham Street, London
EC2V 7PG
Tel.: +44 20 7623 8000