ZURICH

Topical Thoughts
January 2022

Cryptocurrencies are here to stay

Central banks will likely launch their own digital currencies

"The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."

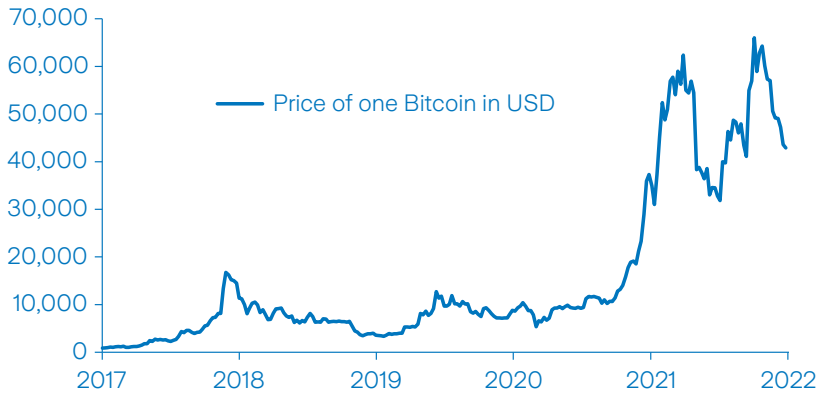
Satoshi Nakamoto

Cryptocurrencies have moved into the spotlight of global financial markets. While much will depend on future regulation, cryptocurrencies are here to stay and related applications are likely to be disruptive for many areas of finance. Central banks see the potential of the new technology and are under pressure to develop their own digital currencies.

With a total market capitalisation of about USD 2.2tn and a daily trading volume of more than USD 100bn cryptocurrencies have moved into the spotlight of global financial markets. Despite the ascendance of thousands of new cryptocurrencies Bitcoin remains the leading coin by market value, making up almost half of the total market capitalisation.

Investors' enthusiasm for Bitcoin and other cryptocurrencies has cooled down, but the overall interest and disruptive potential remain high. After a steep rise and a substantial correction over the past two years Bitcoin's value has increased tenfold since the beginning of 2020, reaching an all-time high in October last year, before falling back recently. This is probably a good moment to take a step back and have a more fundamental look at the drivers behind the recent hype and the disruptive potential of cryptocurrencies, including their potential impact on sovereign currencies and the development of central bank digital currencies (CBDCs). Though neither private nor digital money are really new, cryptocurrencies, and in particular the technology behind them, do offer interesting and potentially disruptive new applications.

The price of Bitcoin has soared



Source: Bloomberg

Front cover image source: iStock

Source: iStock

Cryptocurrencies share some of the characteristics of money

Money has come in many different forms over the course of the centuries. Shells, corals, cocoa beans, gold, gems and paper money have been used as a store of value, a medium of exchange and a unit of account – the three main functions of money. What all these forms of money have in common is the trust to be able to exchange it against something of value in the future. Historically, this trust was based on the supply of these units of exchange being limited and not easily be falsified.

While protection against forgery of most historical forms of money was inherent in its physical form, the value of modern paper or digital money is guaranteed by the central bank that stands behind the currency. A central bank controls the supply of money and sets up the institutions to validate, execute and supervise transactions.

Bitcoin and other cryptocurrencies share some characteristics of money in that they are difficult to falsify and their supply is limited. But rather than relying on physical scarcity or prudent central banks, they use technology to deliver these features. If cryptocurrencies become successful in delivering the main functions of money, their usage could potentially become challenging for existing payment systems and central banks.

Cryptocurrencies don't rely on central authorities

As Satoshi Nakamoto, the presumed pseudonymous person who developed Bitcoin, wrote in the fundamental Bitcoin white paper, a major motivation to create a new digital cash system was to lower transaction costs by introducing a mechanism that does not rely on financial institutions. Linked to this was the desire to financially integrate the millions of people without access to banking and payment services, particularly in emerging markets.

A key property of most cryptocurrencies, including Bitcoin, is that they don't rely on a central authority to limit supply and validate transactions. Transactions and ownership are controlled by decentralised consensus, which is reached if a majority of network participants agree on a specific ownership structure. In the case of Bitcoin, the basis for the decentralised consensus is the 'proof of work'.

Bitcoins are mined to validate new transactions

All Bitcoin transactions that have been executed and validated in the past are stored in a publicly accessible ledger called the blockchain. A new Bitcoin transaction is basically a public message to the Bitcoin network that ownership of a Bitcoin unit (or part of it) is transferred from an existing owner to a new one. As soon as the network participants receive the details of the new transaction the validation process begins.

First, the blockchain is consulted to confirm whether the sender of the Bitcoin unit is actually the legitimate owner. Once confirmed the transaction is combined with a batch of other new transactions to form a new block. Before the new block can be added to the blockchain to legitimise all the included transactions the network participants will initiate the process of providing the proof of work.

The proof of work consists of solving a mathematical problem over and over, slightly changing the input until a pre-defined result is reached. Crucially, the result of the calculation changes in a completely unpredictable manner as the input is changed. The only way to find the correct answer is by trial and error.

This cumbersome process is called mining and requires a lot of computing power and energy. The miner who first solves the problem sends out the correct solution to the whole network. Other participants will now validate the proof of work. By construction, the validation is much simpler and faster than solving the initial problem, a bit like with a Sudoku game. Once the proof of work is validated and approved by a majority of other network participants the miner who first solved the proof of work is rewarded with a number of Bitcoins and the block with the new transactions is added to the blockchain. These transactions are now part of the public ledger and the process recommences with the next set of new transactions.

The proof of work must be difficult and cumbersome in order to avoid any ex-post manipulation of the blockchain. If someone wanted to manipulate a past transaction that person would not only have to change the block in question but all of the following blocks as well in order to achieve the decentralised consensus with regard to the fraudulent block. Given how difficult it is to find the correct solution this is basically impossible.

New cryptocurrencies try to overcome Bitcoin's flaws

The proof-of-work concept cryptographically puts Bitcoin on a sound basis, but it limits its usefulness as a medium of exchange. The number of transactions that can be executed in a reasonable amount of time is already a significant bottleneck although the number of transactions is still only a fraction of what more traditional clearing systems can handle.

In addition, the proof-of-work concept, by definition, uses a lot of computing power and therefore energy resources, which further limits the widespread adoption of Bitcoin. Therefore, even if price volatility falls and acceptance increases over time, Bitcoin is unlikely to be the cryptocurrency of the future.

With these flaws in mind other cryptocurrencies have been created to overcome Bitcoin's deficiencies, trying to provide a sound framework for the future use in transactions. Currently there are thousands of cryptocurrencies although only a handful of them have a relevant market value. Some of them use different approaches to validate ownership and transactions to reduce the use of resources needed to run the network.

Do cryptocurrencies have value?

The total market value of global cryptocurrencies is about 2.2 trillion USD as of January 2022. But where do cryptocurrencies get their value from? Unlike gold, a cryptocurrency such as Bitcoin does not have a long history as a store of value and unlike traditional currencies there is no widespread use of cryptocurrencies to buy goods and services.

However, in an increasing number of cases cryptocurrencies are used as a means of payment within a specific network. Ether, the second most important cryptocurrency by market value, is a good example for this. Ether is the digital currency you need when using the Ethereum network, which offers you a wide range of applications in the digital world. Simply put, if you travel to a foreign country you will need the local currency while you will rely on Ether if you make use of the Ethereum network. Cryptocurrencies can therefore have some value as means of payment, although this is unlikely to be the main driver of current market valuation.

Market value of crypto currencies surges

Source: Coingecko

The proof-of-stake concept and decentralised finance create new investment opportunities

Given the above-mentioned massive use of computation power for the proof-of-work concept, many cryptocurrencies use other approaches to validate transactions or intend to do so in the future, like Ether. One such approach is the proof-of-stake concept. Simply put, instead of trying to crunch a difficult mathematical problem to create a consensus on the current state of a blockchain, the proof-of-stake mechanism relies on validators having large stakes in a cryptocurrency. On cryptocurrency exchanges like Binance owners of a cryptocurrency can lock in all or part of their crypto assets for a pre-defined period of time to be used for so-called staking. By doing so, cryptocurrency owners commit all or part of their holdings to participate in the process of transaction validation and thus support the operation of the network. For this, they get rewarded by an attractive return, particularly given the current low-yield environment.

In addition to staking, there are a growing number of decentralised financial functions like loans and swaps to provide liquidity to the system and earn attractive yields. Decentralised finance thus provides an alternative to simply speculating on price movements of a cryptocurrency.

Nevertheless, while some cryptocurrencies may have an inherent value as a means of payment on a specific network, and many provide additional investment returns, they may still suffer from large price swings caused by speculative flows making them less appealing as a store of value.

Stablecoins are much less volatile as they are linked to other assets
Stablecoins are a category of cryptocurrency that was created to overcome the issue of massive volatility that plagues many cryptocurrencies and may deter potential investors and future users. Stablecoins get their inherent value and enjoy lower volatility because they are linked to another asset or currency. Some stablecoins, like Tether or the Binance dollar, are backed by the US dollar. By linking their price to the value of the US dollar these cryptocurrencies benefit from the stability of the global reserve currency, significantly lowering their price volatility.

However, stablecoins that are linked to a traditional currency are not fully decentralised as their fate is now bound to a fiat currency and the central bank that manages the supply of that underlying currency. In addition, one needs to be sure that there is enough collateral to cover the full value of the outstanding coins.

Alternatively, some stablecoins are backed by other cryptocurrencies so as to remain fully decentralised and independent from fiat currencies. Because the underlying cryptocurrency can be volatile (like Ether or Bitcoin) these stablecoins are overcollateralised to keep their price as stable as possible. While the price of a crypto backed, overcollateralised stablecoin will be less volatile than its non-stable peers, it will probably still experience more volatility than a stablecoin backed by a traditional currency or asset.

Regulation and technology will shape the future of cryptocurrency
Looking forward, while decentralised cryptocurrencies have some practical applications that give them inherent value, they still suffer drawbacks that limit their potential for everyday use, most notably excessive volatility, limited transaction capacity, and dependency on vast computer power. Stablecoins try to circumvent some of these constraints but, in the process of doing so, create new challenges, both around the management of reserves and regulation. It therefore remains to be seen whether there will be widespread demand for private cryptocurrencies and if their use will become challenging for existing payment systems and central banks. This will depend both on technology and on regulation, which are expected to evolve rapidly in the coming years. Indeed, issuance of cryptocurrencies is rising exponentially, along with the capacity to handle transactions, spurred by stiff competition between blockchains and new demands from an increasingly digital economy. And although governments and regulators initially took a hands-off approach towards cryptocurrencies, they are now responding, with bans on cryptocurrencies in some regions and a heightened focus on how to regulate the emerging sector without stifling innovation in others.

While competition is normally considered a good thing, privately distributed and decentralised cryptocurrencies risk generating more fragmented payment networks with less interconnectivity, where the central bank has limited ability to guarantee resilience or act as a lender of last resort during times of crisis. Were cryptocurrencies to gain significant traction, the role of central banks and their ability to promote economic and financial stability is consequently brought into question.

Central banks are developing their own public digital currencies
In parallel with the developments around blockchain technology and private cryptocurrencies, central banks are accelerating work on their own digital currencies, or central bank digital currency (CBDC). In doing so, they are exploring solutions that have been developed by the crypto industry, including the blockchain technology. CBDCs differ markedly from private cryptocurrencies in one important aspect though. While private cryptocurrencies are issued by a private entity and therefore do not represent a claim on central bank money, CBDCs would be fully backed by the sovereign. Currently, cash has a special role to play, as it is the public's only direct access to central bank money. CBDCs would essentially be cash, but in a digital form, thereby broadening and digitising access to central bank money.

While initially hesitant, central banks are taking this step for a variety of reasons, including the challenge posed by private cryptocurrencies, the declining use of cash, and potentially also as a way to deal with the constraint of the zero lower bound (ZLB) to interest rates. Though only a few CBDCs have been fully rolled out, CBDC pilots have been launched to test concepts in many regions and the next few years are likely to see rapid progress, including around cross-border payments.

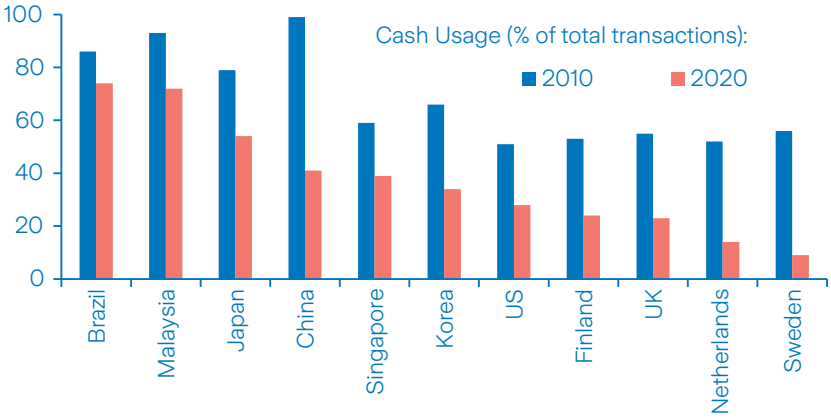
Central banks respond to the disruptive potential of stablecoins

While Bitcoins and other non-asset-backed crypto currencies have disadvantages that make them less useful as currency, most notably excess volatility, the emergence of stablecoins appears to have been a trigger for central banks to accelerate their own work in this area. They are less volatile, so could potentially be more broadly accepted and used as a means of payment. Stablecoins issued by big tech companies would additionally benefit from huge network effects, so could quickly achieve size and coverage if successfully rolled out, both within and across national borders. Facebook, for example, had a network of around 2.9 billion monthly active users – almost one third of the global population.

Stablecoins are, however, still facing challenges, particularly around governance and management of data and reserves and, above all, regulation. Indeed, developments around the Diem stablecoin, which is the Facebook backed digital currency project, where progress has slowed partly due to regulatory challenges, testify to this. In addition, although stablecoins are linked to an underlying asset, they are still susceptible to market runs and price volatility, especially during a crisis period. While these issues pose near-term challenges, it is not inconceivable that some privately issued stablecoins will eventually emerge as a complement to public money.

If such a stablecoin were to be linked to traditional currencies, it would essentially be an extension to the current monetary system, with central banks retaining their ability to control and stabilise the value of money. Conventional payment providers could, however, still be disrupted, and payment systems could become more fragmented. If, however, a non-fiat-currency-backed stablecoin is proven successful in delivering both stability and ease of use, it would pose a threat to sovereign currencies, and potentially undermine the role of central banks. Given this, it is not surprising that central banks are under pressure to develop their own digital currencies.

Physical cash is becoming obsolete in a digital world



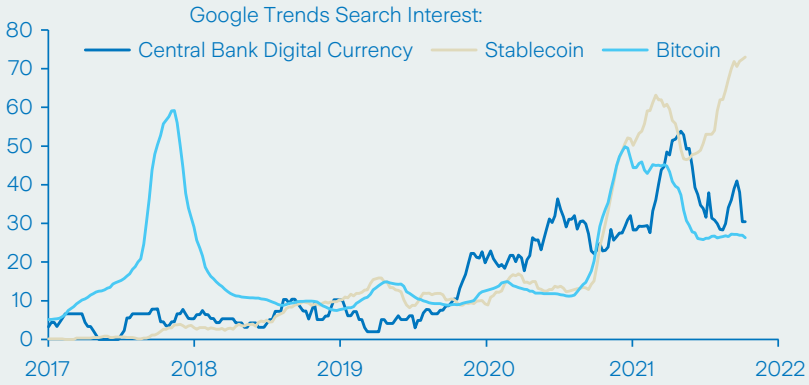
Source: McKinsey

The threat of cash becoming obsolete

Even in the absence of cryptocurrencies, however, the existing monetary system is at risk of becoming obsolete, given the move to a digital society. Cash usage is falling at a rapid pace following payment innovations, a switch to e-commerce and the Covid crisis. Recent data collated by the Bank for International Settlement and the Bank of England show that in the UK, 60% of payments were made using cash in 2008 but this had fallen to less than 30% in 2018 and is projected to fall to 9% in 2028. In Sweden, which is one of the countries that has seen the sharpest cash decline, it now accounts for less than 2% of GDP and half of retailers anticipate that they will not accept cash as a means of payment by 2025.

The trend towards cash-less societies reduces the public's access to a risk-free asset (cash) that also serves as a means of payment. As a result, in future financial crises, when demand for risk-free cash surges and confidence in financial institutions plummets, a lack of readily available physical cash could amplify recession forces. As payment systems have evolved, central banks need to consider whether a new type of central bank money should be invented to better suit evolving needs. The competition from private crypto currencies makes this more urgent.

Crypto and digital currency interest broadening out



Source: Google Trends
Note: Weekly maximum search interest normalised to 100, chart shows 12 week moving average

CBDCs as a potential way around the zero lower bound

Yet another reason for why central banks may be interested in CBDCs is the existence of a zero lower bound (ZLB) on interest rates. The ZLB prevents central banks from cutting rates below a certain level and arises because of the existence of physical cash. When faced with negative interest rates, the public has the option to store physical banknotes (at a cost) as an alternative to being charged a negative interest rate on a deposit account. As a result, policy rate cuts into deeply negative territory are likely to be counterproductive, as they could lead to deposit flight (if banks pass on negative rates to the deposit holders) or a hit to bank profitability (if banks instead absorb negative rates in lower margins). For a long time, the ZLB was a theoretical concept, which few anticipated would ever impact real world policy making. The past decade changed that and central banks are being challenged by their inability to cut rates further.

If central bank money goes fully digital, the option of storing physical cash is removed, making it possible for central banks to cut rates further into negative territory without causing issues for the banking system. CBDCs could therefore offer a way around the ZLB, which is important if current efforts to raise long-run nominal interest rates fail to deliver.

As central banks are not expected to abandon physical cash completely, deterrents need to be built into the system to reduce the potential for the public to switch out of CBDC into cash when interest rates are negative. There are various proposals, including a transaction cost for converting CBDC to cash.

Central bank digital currencies may pose a challenge to traditional bank deposits

Sovereign issued assets are attractive as they are backed by the sovereign. As with physical cash, CBDCs would essentially be risk free (other than for inflation), while bank deposit accounts (or commercial bank money) are subject to credit risk which could materialise if a bank becomes insolvent. There is therefore a risk that the public will choose to hold CBDCs instead of conventional bank deposits, particularly during times of crisis. The challenge is to design a CBDC that is useful and relevant but, at the same time, avoids disruptions for the broader financial sector.

Focus is currently on a two-tier system, where banks and other intermediaries hold custody accounts, distribute CBDCs across the economy, and provide services for the public. While banks would maintain their role as financial services providers, this setup does not resolve risk around the substitution of CBDCs for bank deposits.

There are different approaches to reducing this risk, including capping the amount of CBDC that an individual can hold, or applying a penalty, in the form of less favourable interest rates, on the CBDC. However, these approaches risk creating a complex and less efficient system, which undermines the usage and the usefulness of CBDCs, and potentially gives an advantage to private cryptocurrencies. There is a fine balance that needs to be established.

CBDC pilots have been launched, with further developments expected

Given the potential risks, it is encouraging that a range of approaches are being tested by global central banks, both around distribution (eg whole-sale vs retail), access (account or token based) and authority (decentralised or centralised).

Financial institutions would play an important role in the wholesale/platform approach, where distribution of a CBDC would be managed through regulated intermediates such as banks but potentially also tech companies. But there are alternatives to this. One solution sidesteps intermediaries and allows the public to directly access CBDCs from the central bank, similarly to how banks and other counterparties can access central bank reserves today. Another solution would be to involve cryptocurrency issuers to provide CBDCs in a decentralised manner using blockchain technology, but where the cryptocurrency is fully backed by central bank reserves. A range of pilots are ongoing, in developed as well as emerging economies.

While central banks are, by definition, leading the way on CBDCs, they are hugely dependent on the private sector to drive innovation and provide the technology that is needed to make CBDCs successful. Because of this dependency, a complete ban on private cryptocurrencies is unlikely – at least at this stage of development.

Conclusion

What is clear is that cryptocurrencies and in particular, the underlying technologies, are here to stay. Central bank digital currencies also look like a near certainty, given the declining use of cash and the evolving needs in a digital economy. What is less certain is how the regulatory framework will evolve and this will be key for future developments and potential disruptions.

The real threat to public money and the ability of central banks to promote economic and financial stability is if a non-fiat-currency-backed stablecoin is proven successful in delivering both stability and ease of use. The question then becomes whether governments will outlaw successful private currencies, or whether regulation will be so harsh, that it removes all advantages of a private currency. Given what is at stake, we suspect this may be the case.

However, even if regulation in some regions prevents private cryptocurrencies from becoming widely used, they can still provide competition to sovereign money. One example of this is that countries that currently outsource their money supply by pegging their currencies to a safe-haven currency now have the option to do so against a cryptocurrency. To date, only one country (El Salvador) has legislated to adopt a cryptocurrency as legal tender, but more could potentially follow. What ultimately matters is whether trust in technology can replace trust in strong currencies and the institutions that go with them.

Like cryptocurrencies, central bank digital currencies can also be disruptive. Were they to be rolled out on a broader scale, they have, for example, the potential to relax the zero lower bound on interest rates. We are probably still a few recessions away from this potentially becoming reality, but once the zero lower bound is gone, there is nothing that guarantees a zero (or mildly negative) floor on interest rates. This would have material implications for interest rates, the savings industry, and the financial sector more broadly.

By contrast, if the current rise in inflation proves to be more persistent than expected, this could lead to investors and savers increasingly favouring cryptocurrencies with limited supply, such as the Bitcoin, over fiat currency. One question is whether competition from cryptocurrencies could, at some stage, become sufficiently material so as to influence (likely in a hawkish direction) central bank policy.

Finally, whether cryptocurrencies become widely used or not, it appears that banks and other financial intermediaries will face new challenges, both from cryptocurrencies and from CBDCs. Central banks will need to carefully consider this in their quest for digital currencies, and the financial services industry must ensure its business models evolve in a changing environment.

Disclaimer and cautionary statement

This publication has been prepared by Zurich Insurance Group Ltd and the opinions expressed therein are those of Zurich Insurance Group Ltd as of the date of writing and are subject to change without notice.

This publication has been produced solely for informational purposes. The analysis contained and opinions expressed herein are based on numerous assumptions concerning anticipated results that are inherently subject to significant economic, competitive, and other uncertainties and contingencies. Different assumptions could result in materially different conclusions. All information contained in this publication have been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Group Ltd or any of its subsidiaries (the 'Group') as to their accuracy or completeness.

Opinions expressed and analyses contained herein might differ from or be contrary to those expressed by other Group functions or contained in other documents of the Group, as a result of using different assumptions and/or criteria.

The Group may buy, sell, cover or otherwise change the nature, form or amount of its investments, including any investments identified in this publication, without further notice for any reason.

This publication is not intended to be legal, underwriting, financial investment or any other type of professional advice. No content in this publication constitutes a recommendation that any particular investment, security, transaction or investment strategy is suitable for any specific person. The content in this publication is not designed to meet any one's personal situation. The Group hereby disclaims any duty to update any information in this publication.

Persons requiring advice should consult an independent adviser (the Group does not provide investment or personalized advice).

The Group disclaims any and all liability whatsoever resulting from the use of or reliance upon publication. Certain statements in this publication are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by other factors that could cause actual results, developments and plans and objectives to differ materially from those expressed or implied in the forward-looking statements.

The subject matter of this publication is also not tied to any specific insurance product nor will it ensure coverage under any insurance policy.

Zurich Insurance Company Ltd
Group Investment Management
Mythenquai 2
8002 Zurich

173008079 (01/22) TCL

ZURICH