Teneo
The Global CEO Advisory Firm

Cryptocurrency Payments

Will cryptocurrencies provide viable alternative payment mechanisms?

Teneo Insights
February 2022

Introduction

Cryptocurrencies are frequently talked about synonymously with payments, but is that correct? Can cryptocurrencies form the basis of viable payments mechanisms? Could they in the future? What forms of payments could they be beneficial for?

This is a subject that has no doubt formed the basis of many PhD theses. Here, we try to distil the key points into a few pages which the layperson can understand.

In doing so, we make no apologies for sticking to the mainstream definitions and mechanisms and ignoring the many variations which prove exceptions to those rules and can make the discussion overly complicated. Similarly, for any metric associated with cryptocurrencies, there is a wide range of answers, depending on sources and dates. We have not verified the metrics used as we are interested in the orders of magnitude rather than precise figures to make the observations below.

As the cryptocurrency world is both relatively new and rapidly evolving, there is as yet no definitive lexicon; different authors use subtly different definitions. In the appendix, are listed the definitions used in this article (drawn from a range of sources).

Background

The hype to-date has largely revolved around unbacked cryptocurrencies as an asset class dominated by Bitcoin and a handful of other tokens. Speculators buy them, hold them and sell them.

Focus has been on how their value against a fiat currency has performed, much like a commodity. But by their very name, cryptocurrencies are seen by some as a currency. As their whole existence relates to transactions and records of transactions, it is difficult not to see cryptocurrencies also as a payment system.

Cryptocurrencies can be used as a payment mechanism. An individual can make a payment to another individual in a cryptocurrency which is recorded on blockchain. Consequently, the key question is not whether they can be used as a payment mechanism, but whether cryptocurrencies are, or could be, a viable challenger to the existing fiat currency payment systems for anything more than a few ad hoc barter transfers.

Current situation

In the fiat currency world there is an array of payment mechanisms, many doing something slightly different. Frequently, multiple mechanisms are used sequentially to complete each payment. Some are domestic/ single currency (e.g. BACS[1], Faster Payments, CHIPS[2], CHAPS[3]), some regional (e.g. SEPA[4]) and some international/multi-currency (e.g. Visa, Mastercard, Letters of Credit). Some of these mechanisms relate to high volume retail transactions (e.g. retail card payments and electronic payments), whereas others are lower volume business-to-business transactions (e.g. international bank-to-bank payments and Letters of Credit). Overlaid on the actual payments systems lie messaging systems, principally Swift[5], which is the conduit for payment instructions and therefore forms an integral part of the whole solution for inter-bank payments. The processes have evolved organically over time and, as a result, are fairly archaic. International payments for example, often involve a series of intermediary (correspondent) banks connected via thousands of bilateral agreements. For international trade payments, networks of banks are involved to process payments and/or check documents and/or guarantee payments.

The complexity of the current solution, particularly for international payments, means that payments are expensive and take a relatively long time to process. For retail card payments, an infrastructure exists both domestically and internationally which is broadly fit for purpose, if rather expensive; however, in its recent report[6], the UK Payment Systems Regulator (PSR) stated that, *"the supply of card-acquiring services does not work well for small and medium-sized merchants."* The PSR goes on to say, *"We will work…to develop remedies that … ensures that the market works better for them."* There is clearly room for improvement.

1. **BACS -** Bankers' Automated Clearing System (GBP)
2. **CHIPS -** Clearing House Interbank Payments System (USD)
3. **CHAPS -** Clearing House Automated Payments System (GBP)
4. **SEPA -** Single Euro Payments Area (EUR)
5. **Swift -** Society for Worldwide Interbank Financial Telecommunications.
6. **Source -** https://www.psr.org.uk/publications/market reviews/mr18-1-8-card-acquiring-report-final/

Cryptocurrencies as a potential game changer

The recent launch of The Bank of London (only the second clearing bank launched in the UK in the last 250 years) as a self-proclaimed disrupter of the fundamentals of banking, specifically regarding end-to-end international banking services, also indicates that change is in the air.

An innovation that revolutionises the industry and delivers far simpler, quicker, and cheaper solutions may be overdue. Some argue that cryptocurrencies, or rather the underlying blockchain, may form the basis of these solutions.

Let's look at a few of the pertinent factors which have been aired in the press over recent months: value volatility, transaction rate, transaction time, transaction cost, energy consumption and blockchain size.

I. Value volatility

The first key challenge that cryptocurrencies face versus fiat currencies is value volatility. Few of us have encountered the chaos caused by hyperinflation, but cryptocurrency-based transactions face similar challenges. Typically, businesses want to make profits on the products they sell. To reduce risk, they usually price in the same currency as their costs. If they are pricing (or buying) in a different currency, they hedge, at a cost, against adverse foreign exchange movements. If payments were made in cryptocurrencies, there would be a crypto/fiat exchange, and therefore hedging required, on every transaction. Given the high volatility, the use of hedging instruments is not a viable option. There are two possible solutions that address this in some way:

Ia. Stablecoins

Stablecoins are cryptocurrencies which are purportedly more stable and secure than unbacked cryptocurrencies, on the basis that they are typically tied to the value of a fiat currency and therefore address this issue head on. Products or services could be priced in fiat and/or a stablecoin in the confidence that their values would not diverge drastically. However, recurring questions over the reality of the collateral behind these does raise some concerns; are some merely the latest iteration of a Madoff or Wirecard style fraud where the reported underlying collateral does not actually exist? Without adequate regulatory oversight, we cannot be confident.

Ib. Rapid transactions

The "claimed" speed of cryptocurrency transactions means that if one prices in home fiat currency, a payment service provider could convert the payment to a cryptocurrency at the spot rate at the time of transaction, send the payment and convert back to fiat. If this can be achieved in a few seconds, the exchange rate risk is minimised.

II. Transaction rate

The credit card payments network, Visa, can process 32,000 transactions per second ("tps")[7], whilst Bitcoin, as a first-generation cryptocurrency, processes at only 3 tps[8]. The way a block is added to the blockchain (its consensus protocol, proof-of-work), the number of transactions it processes at a time (block size, 1 MB) and the target time to add a block (10 minutes), are the parameters that limit its transaction rate. As blockchain technology evolves, new solutions are emerging that address the restrictions inherent with Bitcoin.

Changes are also being made to Ethereum, the second largest blockchain, in a series of steps to transition to Ethereum 2.0 by June 2022. The target for Ethereum 2.0 is to increase transaction rates from the current 15-45 tps to 100,000 tps.

Already, third-generation blockchains are emerging with claims of significantly increased transaction rates: Nano at 1,000 tps and Solana[9] at 50,000 tps. These use a blockchain and are distributed but use very different mechanisms to Bitcoin. In short, although the original protocols were unsuited for high volume transactions, the emerging protocols address this issue and could, it appears, deliver transaction rates which would support a viable payments system.

7. **Source -** Visa fact sheet, two Visa transactions per payment
8. **Source -** https://www.blockchain.com/charts/transactions-per-second
9. **Source -** https://break.solana.com/

III. Transaction time

For a cryptocurrency transaction, there are two relevant transaction time measures: The time to process the transaction (record the transaction in the blockchain) and the time to be confident that the transaction will not be annulled (confirmation). For Bitcoin this is seen as an average of 10 minutes to process the transaction and an hour for confirmation. However, 10 minutes is a target average; if the fee is low and/or volume high it may take longer (and may never happen). Third-generation blockchains are emerging with claims of far faster transaction times, some purporting to be near-instant anywhere in the world (e.g. Nano and Solana claiming sub-second settlement times).

Alternative approaches, such as net payments where multiple individual payments are aggregated and netted off between parties and only the net movement written to the blockchain, are also emerging. The Lightning network does this for Bitcoin to address the transaction rate and time issues mentioned above. These services offer faster transaction times but add another layer of infrastructure and start to move away from the blockchain concept, becoming closer to the existing fiat currency payment models. It is worth comparing this to a fiat currency transaction. In the UK, a transfer between UK banks can be close to instantaneous.

Faster payments are normally a few seconds (but can take up to two hours), 24 hours a day, seven days a week. For larger sums or direct debit/standing order payments, CHAPS is same day and BACS takes three days. On the other hand, international payments can take significantly longer, up to five days (especially if between smaller banks in smaller countries which are routed via several intermediaries) and may require arrangements to be put in place prior to the transaction (such as nominating advising or confirming banks for Letters of Credit) to provide the level of confidence required for trade. In that time, there remains an exposure to exchange rate risk which may need to be hedged. These payments are also affected by weekends and bank holidays.

In conclusion, although the first-generation cryptocurrencies could not support high volume "retail" transactions, the emerging solutions could; and for international payments, even the oldest and slowest cryptocurrency payment is significantly faster than the best a fiat currency payment system can currently achieve.

IV. Transaction cost

The fee structures vary significantly, with variable percentages (some decreasing with the value of transaction), fixed elements and a discretionary element (tips) to increase the probability of rapid processing. Some of the newer cryptocurrencies have zero transaction fees (e.g. Nano); the older ones rather higher fees. In general, given the variation, there is no reason why newer cryptocurrencies can't be very competitive with fiat payments systems in terms of fees.

V. Energy consumption

In May 2021, China banned the processing of transactions, also known as mining, of Bitcoin on the premise that it was too energy intensive. In November 2021, India announced a similar ban and in January 2022, Kosovo also banned mining. Was this a ruse or do these countries have a point? Let us look at some facts. Currently, global Bitcoin mining consumes 300 GWh per day[10]. In terms that we can assimilate, that is one third of the UK's entire electricity consumption. If Bitcoin were to process the same number of transactions as Visa, it would consume 30 times the electricity consumption of the entire globe. So, in a world ever more conscious of the effects of climate change, Bitcoin as a volume payment method has some significant issues to resolve. But there is a recurring theme: Third-generation cryptocurrencies can process transactions without consuming vast amount of energy by utilising different ways of adding blocks to the blockchain (different consensus protocols) which avoid multiple parallel processing.

VI. Blockchain size

In first-generation distributed networks, each node has a copy of the entire blockchain. If we again take Bitcoin as an example, the current Bitcoin blockchain is about 360 GB. Every new block adds 1 MB, and a new block is created every 10 minutes. That's 144 MB per day, 53 GB per year. This data must be transmitted between nodes and stored across the distributed network. Scaling this to handle the volume of transactions needed to make it a realistic competitor to the existing fiat payment systems is impracticable.

Third-generation cryptocurrencies are trying to tackle this head on. Pruning, subscriptions, partitioning and/or compression can reduce the amount of data each node has to store significantly. Viability at scale is a key objective of the new entrants.

10. Source - https://ccaf.io/cbeci/index

Predictions

As Nostradamus purportedly once said, "prediction is difficult, especially about the future," but let us nail our colours to the mast.

The concept is new, progress is being made very rapidly and there appears to be no shortage of investment in its development. It is also worth noting that current payments processing, especially internationally, is not a straightforward, fast and cheap process with zero risk.

As the first cryptocurrency, Bitcoin gets most of the press. But we should consider it as the Motorola brick phone of the cryptocurrency world: a significant innovation, of great academic interest and a catalyst of change, but of limited real-world use. The concept as defined in 2008 for Bitcoin does not work for volume transactions for many reasons, but there is real promise in the emerging solutions which its creation has spawned. Here are some key questions we leave you to consider alongside our predictions:

What forms of payments could cryptocurrency be beneficial for?

For international payments, the opportunities are immense. The current processes are protracted and expensive. We can see a wholesale adoption of cryptocurrency-based international payments for legitimate purposes emerge; however, the volume is relatively low, which may hamper progress. Whether this change is driven by the emerging technology players or whether any of the current players can move rapidly enough to remain in the game has yet to become clear.

For volume transactions there are many more barriers to overcome, but the market is huge.

The technology undoubtably has huge potential. There are many players vying to be the first to develop blockchains which are truly scalable, secure, interoperable, robust and energy efficient. Our guess is that they will be successful.

The focus will move away from the cryptocurrency element and towards the utility of the mechanism. The actual cryptocurrency used may become invisible to the sender and recipient, a transaction being initiated and completed in fiat currency and the cryptocurrency merely becoming part of the technology solution.

What about unbacked coins?

Given the speculative nature of unbacked coins, we believe the future of payments will be based on stablecoins or coins invisible to the user. Nevertheless, some regulation will be required before the established banks are likely to adopt them in order to avoid another Madoff or Wirecard. Unbacked cryptocurrencies may continue as a speculative asset class or die as the latest manifestation of Tulipmania[11].

Who will the future players be?

Will the entities currently processing payments be able to develop and/or adopt the new technologies rapidly enough to avoid going the way of Kodak? Will their value-added services and ubiquity in the market mean that they will continue, albeit in a very different form? Cryptocurrencies/blockchain may provide the infrastructure, but there is more to the end-to-end payment solution than the wires. The applications and relationships that surround it will be key, and the existing players have the edge on these aspects.

The threat to the existing players doesn't stop with the infrastructure providers themselves (e.g. Swift, Mastercard, CHIPS). If international payments can be made rapidly, cheaply and at low risk, what will happen to the trade banks advising and confirming payments? The regulatory challenges are significant, but let us for now assume that a suitable international regulatory regime will emerge in time. The regulators will undoubtably play an important role in the wholesale adoption of such a payments infrastructure. In parallel, many governments are investigating the issuance of Central Bank Digital Currencies (CBDCs). Although not cryptocurrencies, we may see a merging of technologies and concepts and central banks reasserting their dominance of control in the payments space.

11. **Tulipmania -** https://www.investopedia.com/terms/d/dutch_tulip_bulb_market_bubble.asp

Conclusions

It is impossible to conclude with any certainty on the future of payments systems and the role cryptocurrencies will play in their development. However, we believe there is about to be a fundamental change to payments, the like of which we have not seen before. Many of the incumbent large players will be replaced by new entrants. A few incumbents may be agile enough to adapt and survive. As a result, payments will look strikingly different.

Key Contacts

If any of these issues resonate with you, please contact Teneo's Financial Services team below:

David Taylor

Author & Managing Director
Phone: 07712 776 691
Email: david.taylor@teneo.com

David Soden

Senior Managing Director
Phone: 07780 954 883
Email: david.soden@teneo.com

Stephen Browne

Senior Managing Director
Phone: 07710 378 740
Email: stephen.browne@teneo.com

Appendix – Definitions

Bitcoin	Bitcoin was the first cryptocurrency and is an example of an unbacked cryptocurrency using blockchain across a public network. Its design was set out in a paper written in 2008 by an unidentified person or group calling itself Satoshi Nakamoto12. It is the largest cryptocurrency by market capitalisation.
Block	A group of transactions which are processed and added to a blockchain simultaneously. The data in the block comprises the transaction data, data about the transaction (meta data), a timestamp and a code which links it to the blockchain as it was when the block was added.
Blockchain	A system, originally defined by Satoshi Nakamoto in 2008, in which records of transactions are recorded in multiple locations across a distributed peer-to-peer network. Cryptography is used to protect against fraud. It is simply a chain of sequential blocks, each one derived from the previous blocks and the block being added.
Consensus protocol	The integrity of the transactions added to the blockchain is maintained through the consensus protocol. As there is no central control, consensus must be agreed by the nodes in the network to prevent malicious parties taking over the validation and process fraudulent transactions. There are multiple consensus protocols.
Consensus protocol - Proof of Stake	An increasingly popular mechanism, as it is seen as the “green” approach. Blocks are “forged.” Forgers are selected by a pseudo-random election process broadly in proportion to their quantity of holdings in the associated cryptocurrency (i.e. the size of their stake). A common factor is Coin Age (number of days coins held X number of coins staked); the days held is reset to zero once the node has added a block, thus preventing very large forgers to dominate. If the network identifies a fraudulent transaction, the forger node will lose part of its stake and its right to participate as a forger in the future. If the stake is higher than the reward, the validator would lose more coins that it would gain in case of attempted fraud.
Consensus protocol - Proof of Work	The first consensus mechanism and used by Bitcoin. The nodes on the network try, simultaneously, to be the fastest to add a block, a process called “mining.” As only the first node (miner) reaps a reward, speed is of the essence, which is leading to a processing power race. This method is under pressure due to the enormous and increasing amounts of power used and heat generated across the globe. As the amount of effort required to obtain a reward is significant, and that would be sacrificed if an invalid/ fraudulent block was mined, fraud is discouraged.
Cryptocurrency	Digital currency in which transactions are verified and records maintained on a decentralised system using cryptography and which is not controlled or issued by a centralised authority.
Fiat currency	A currency backed by a government or other central body, but not linked to any underlying asset/ commodity (e.g. USD, GBP, EUR).
FX Hedge	A transaction processed into order to reduce the risk of adverse foreign exchange movements. A hedge costs money to process but provides some protection if the exchange rate moves against you.
Proof of Stake	See Consensus protocol - Proof of Stake.
Proof of Work	See Consensus protocol - Proof of Work.
Smart Contract	Contracts written in lines of code and recorded in a decentralised blockchain. The code controls the execution of the contract. As they are written to a blockchain they are immutable. They can include health and voting records, not solely traditional contracts.
Stablecoin	Cryptocurrency where the price is designed to be pegged to real world assets, e.g. fiat money (e.g. Tether) or exchanged traded commodity (e.g. Digix Gold Tokens (DGX). Where the collateral is volatile (e.g. another cryptocurrency), price stability is achieved through introduction of supplementary instruments and incentives, not just collateral. How and whether this is achieved is frequently rather opaque.
Unbacked cryptocurrency	A privately created cryptocurrency, the value of which is determined solely by the market. For example, Bitcoin.

https://www.teneo.com/service/financial-advisory/

12. Source - https://nakamotoinstitute.org/bitcoin/

Teneo®

The Global CEO Advisory Firm

London

5th Floor,
6 More London Place
SE1 2DA

https://www.teneo.com/service/financial-advisory/