TWN Briefing Paper 96
Third World Network
www.twn.my
June 2018

The trust limitations of cryptocurrencies

by Chakravarthi Raghavan

In less than 10 years since their inception, cryptocurrencies have emerged from obscurity to attract intense interest on the part of businesses and consumers, as well as central banks and other authorities, but their decentralized creation has inherent limitations in maintenance of trust in value and involves vast energy use presaging an environmental disaster and the potential to bring the Internet to a halt.

These are some of the conclusions of the Bank for International Settlements (BIS) in its in-depth study of cryptocurrencies and whether they could play any role as money. Titled "Cryptocurrencies: looking beyond the hype", the study is part of BIS' *Annual Economic Report 2018* and was pre-released on 17 June ahead of the 24 June publication of the full report.

The study notes that cryptocurrencies garner attention because they promise to replace trust in longstanding institutions, such as commercial and central banks, with trust in a new, fully decentralized system founded on the blockchain and related distributed ledger technology (DLT).

However, the BIS study warns, cryptocurrencies are a poor substitute for the solid institutional backing of money, cannot scale with transaction demand, are prone to congestion, and come with poor efficiency and vast energy use that could presage an environmental disaster and bring the Internet to a halt.

Nevertheless, says the BIS, the underlying technology could have promise in other applications, such as the simplification of administrative processes in the settlement of financial transactions, though this still remains to be tested.

The BIS notes that many past episodes of monetary instability and failed currencies illustrate that the institutional arrangements through which money is supplied matter a great deal. The essence of good money has always been trust in the stability of its value. And for money to live up to its property to act as a coordination device facilitating transactions, it needs to efficiently scale with the economy and be provided elastically to address fluctuating demand.

These considerations have led to specific institutional arrangements – the emergence of today's independent and accountable central banks, after episodes of individual private banks performing this role.

As for cryptocurrencies, they entail economic limitations inherent in the decentralized creation of trust. For the trust to be maintained, honest network participants need to control the vast majority of computing power, and each and every user needs

Address: 131 Jalan Macalister, 10400 Penang, MALAYSIA **Tel**: 60-4-2266728/2266159 **Fax**: 60-4-2264505
E-mail: twn@twnetwork.org **Website**: www.twn.my

to verify the history of transactions. And the supply of the cryptocurrency needs to be predetermined by its protocol. Trust can evaporate at any time because of the fragility of the decentralized consensus through which transactions are recorded. Not only does this call into question the finality of individual payments, but it also means that a cryptocurrency can simply stop functioning, resulting in a complete loss of value.

Money, the BIS notes, plays a crucial role in facilitating economic exchange. Before its advent millennia ago, goods were primarily exchanged for the promise to return the favour in the future (traded IOUs). However, as societies grew larger and economic activity expanded, it became harder to keep a record of ever more complex IOUs, and default and settlement risks became concerns. Money and the institutions issuing it came into existence to address this growing complexity and the associated difficulty in maintaining trust.

Money has three fundamental and complementary roles as: (i) a unit of account; (ii) a medium of exchange; and (iii) a store of value, enabling users to transfer purchasing power over time. To fulfil these functions, money needs to have the same value in different places and to keep a stable value over time. However, maintaining trust in the institutional arrangements through which money is supplied has been the biggest challenge.

Around the world, in different settings and at different times, money started to rely on issuance by centralized authorities. It evolved from the stamp of a sovereign certifying a coin's value in transactions, to bills of exchange intermediated by banks developed as a way for merchants to limit the costs and risks of travelling with large quantities of coinage.

However, historical experience also made clear an underlying trade-off: currencies that are supplied flexibly can also be debased easily. Sustained episodes of stable money are historically much more of an exception than the norm. "In fact, trust has failed so frequently that history is a graveyard of currencies."

History proves that money can be fragile, whether supplied through private means in a competitive manner, or by a sovereign as a monopolist supplier. Government-backed arrangements have not always worked well either. Avoiding abuse by the sovereign has thus been a key consideration in the design of monetary arrangements.

The quest for solid institutional underpinning for trust in money eventually culminated in the emergence of today's central banks. The tried, trusted and resilient way to provide confidence in money in modern times is the independent central bank with agreed goals: clear monetary policy and financial stability objectives; operational, instrument and administrative independence; and democratic accountability, so as to ensure broad-based political support and legitimacy.

Independent central banks have largely achieved the goal of safeguarding society's economic and political interest in a stable currency. In almost all modern-day economies, money is provided through a joint public-private venture between the central bank and private banks, with the central bank at the system's core. Electronic bank deposits are the main means of payment between ultimate users, while central bank reserves are the means of payment between banks.

In this two-tiered system, trust is generated through independent and accountable central banks, which back reserves through their asset holdings and operational rules. In turn, trust in bank deposits is generated through a variety of means, including regulation, supervision and deposit insurance schemes, many ultimately emanating from the state.

As part of fulfilling their mandate to maintain a stable unit of account and means of payment, central banks take an active role in supervising, overseeing and in some cases providing the payments infrastructure for their currency. The central bank's role includes ensuring that the payment system operates smoothly and seeing to it that the supply of reserves responds appropriately to shifting demand, i.e., ensuring an elastic money supply.

Thanks to the active involvement of central banks, today's diverse payment systems have achieved safety, cost-effectiveness, scalability and trust that a payment, once made, is final. Payment systems are safe and cost-effective, handling high volumes and accommodating rapid growth with hardly any abuse and at low costs. In today's sophisticated economies, the volume of payments is huge, equal to many multiples of GDP.

Despite these large volumes, expanding use of the instrument does not lead to a proportional increase in costs. This is important since an essential feature of any successful money and payment system is how widely used it is by both buyers and sellers: the more others connect to a particular payment system, the greater one's own incentive to use it.

Users not only need to have trust in money itself, they also need to trust that a payment will take place promptly and smoothly: "finality" in cer-

tainty of payment, and the related ability to contest transactions that may have been incorrectly executed. Finality requires that the system be largely free of fraud and operational risks, at the level of both individual transactions and the system as a whole. Strong oversight and central bank accountability both help to support finality and hence trust.

While most modern-day transactions occur through means ultimately supported by central banks, over time a wide range of public and private payment means has emerged. Money is typically based on one of two basic technologies: so-called "tokens" or accounts.

Token-based money – banknotes or physical coins – can be exchanged in peer-to-peer settings, but such exchange relies critically on the payee's ability to verify the validity of the payment object – with cash, the worry is counterfeiting. By contrast, systems based on account money depend fundamentally on the ability to verify the identity of the account holder.

Cryptocurrencies aspire to be a new form of currency and promise to maintain trust in the stability of their value through the use of technology. They consist of three elements: first, a set of rules (the "protocol"), computer code specifying how participants can transact; second, a ledger storing the history of transactions; and third, a decentralized network of participants that update, store and read the ledger of transactions following the rules of the protocol. With these elements, advocates claim, a cryptocurrency is not subject to the potentially misguided incentives of banks and sovereigns.

Cryptocurrencies are digital, aspiring to be a convenient means of payment and relying on cryptography to prevent counterfeiting and fraudulent transactions. Although created privately, they are no one's liability, i.e., they cannot be redeemed, and their value derives only from the expectation that they will continue to be accepted by others. And, last, they allow for digital peer-to-peer exchange.

Compared with other private digital moneys such as bank deposits, the distinguishing feature of cryptocurrencies is digital peer-to-peer exchange. Cryptocurrency transfers can in principle take place in a decentralized setting without the need for a central counterparty to execute the exchange.

The technological challenge in digital peer-to-peer exchange is the so-called "double-spending problem." Any digital form of money is easily replicable and can thus be fraudulently spent more than once. Digital information can be reproduced more easily than physical banknotes. For digital money, solving the double-spending problem requires, at a minimum, that someone keep a record of all transactions.

Prior to cryptocurrencies, the only solution was to have a centralized agent do this and verify all transactions. Cryptocurrencies overcome the double-spending problem via decentralized record-keeping through what is known as a "distributed ledger". The ledger starts with an initial distribution of cryptocurrency and records the history of all subsequent transactions. An up-to-date copy of the entire ledger is stored by each user, making it "distributed". With a distributed ledger, peer-to-peer exchange of digital money is feasible: each user can directly verify in their copy of the ledger whether a transfer took place and that there was no attempt to double-spend.

While all cryptocurrencies rely on a distributed ledger, they differ in terms of how the ledger is updated. One can distinguish two broad classes, with substantial differences in their operational setup.

One class, based on "permissioned" DLT, is similar to conventional payment mechanisms. In this class, to prevent abuse, the ledger can only be updated by trusted participants, or what is known as "trusted nodes", in the cryptocurrency. These nodes are chosen and subject to oversight by a central authority of the ledger, e.g., the firm that developed the cryptocurrency.

Thus, while cryptocurrencies based on permissioned systems differ from conventional money in terms of how transaction records are stored (decentralized versus centralized), they share with it the reliance on specific institutions as the ultimate source of trust.

In a much more radical departure from the prevailing institution-based setup, a second class of cryptocurrencies promises to generate trust in a fully decentralized setting using "permissionless" DLT. The ledger recording transactions can only be changed by a consensus of the participants in the currency: while anybody can participate, nobody has a special key to change the ledger.

The concept of permissionless cryptocurrencies, laid out for bitcoin, is based on a specific type of distributed ledger, the "blockchain", updated in groups of transactions called blocks. Blocks are then chained sequentially via the use of cryptography to form the blockchain. This concept has been adapted to countless other cryptocurrencies.

Blockchain-based permissionless cryptocurrencies have two groups of participants: "miners" who act

as bookkeepers, and "users" who want to transact in the cryptocurrency. At face value, the idea underlying these cryptocurrencies is simple: instead of a bank centrally recording transactions underlying this setup, the key feature of these cryptocurrencies is the implementation of a set of rules (the protocol) that aim to align the incentives of all participants so as to create a reliable payment technology without a central trusted agent.

The protocol determines the supply of the asset in order to counter debasement – for example, in the case of bitcoin, it states that no more than 21 million bitcoins can exist. In addition, the protocol is designed to ensure that all participants follow the rules out of self-interest, i.e., that they yield a self-sustaining equilibrium.

The rules entail a cost to updating the ledger, requiring in most cases a "proof-of-work", mathematical evidence that a certain amount of computational work has been done, in turn calling for costly equipment and electricity use. It is often referred to as "mining". In return for their efforts, miners receive fees from the users – and, if specified by the protocol, newly minted cryptocurrency.

Second, all miners and users of a cryptocurrency verify all ledger updates, which induces miners to include only valid transactions. If a ledger update includes an invalid transaction, it is rejected by the network and the miner's rewards are voided. The verification of all new ledger updates by the network of miners and users is thus essential to incentivize miners to add only valid transactions.

Third, the protocol specifies rules to achieve a consensus on the order of updates to the ledger.

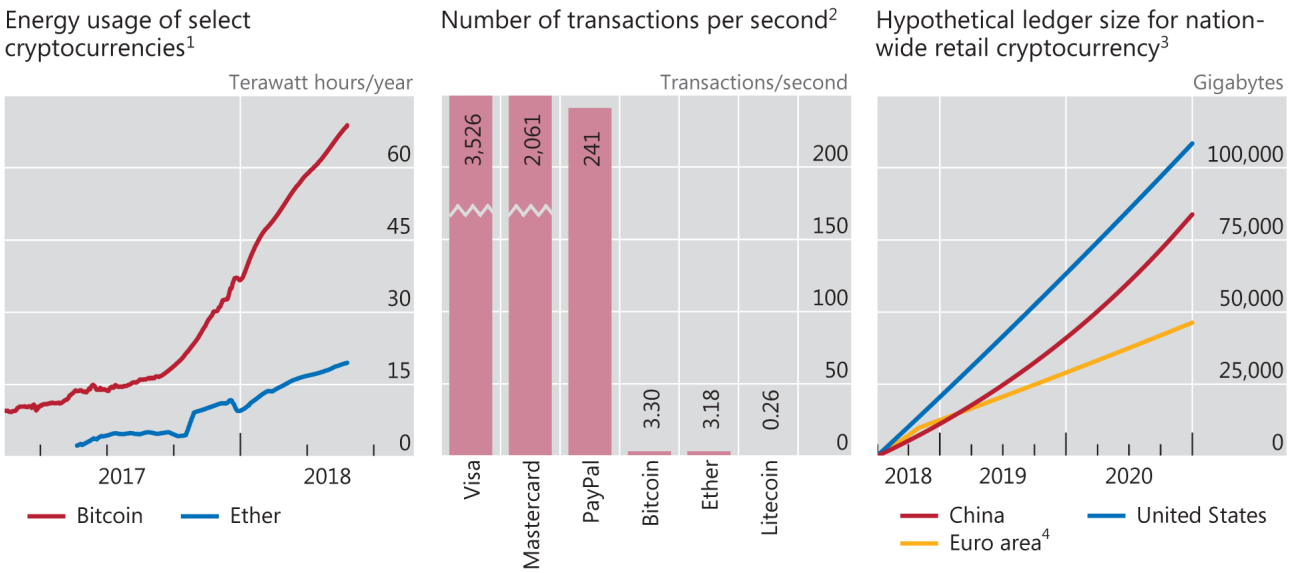
With these key ingredients, it is costly – though not impossible – for any individual to forge a cryptocurrency.

Cryptocurrencies such as bitcoin promise to deliver not only a convenient payment means based on digital technology, but also a novel model of trust. Yet delivering on this promise hinges on a set of assumptions: that honest miners control the vast majority of computing power, that users verify the history of all transactions and that the supply of the currency is predetermined by a protocol.

These assumptions give rise to two basic questions regarding the usefulness of cryptocurrencies. First, does this cumbersome way of trying to achieve trust come at the expense of efficiency? Second, can trust truly and always be achieved?

A key potential limitation in terms of efficiency is the enormous cost of generating decentralized

Energy consumption and scaling issues



[1] Estimated. [2] 2017 data. [3] The displayed hypothetical size of the blockchain/ledger is calculated assuming that, starting from 1 July 2018, all non-cash retail transactions of either China, the United States or the euro area are processed via a cryptocurrency. Calculations are based on information on non-cash transaction numbers from CPMI (2017) and assume that each transaction adds 250 bytes to the ledger. [4] BE, FR, DE, IT and NL.

Sources: Committee on Payments and Market Infrastructures, *Statistics on payment, clearing and settlement systems in the CPMI countries*, December 2017; www.bitinfocharts.com; Digiconomist; Mastercard; PayPal; Visa; BIS calculations.

This graph is reproduced from BIS, *Annual Economic Report 2018*, Chapter V.

trust. Individual facilities operated by miners can host computing power equivalent to that of millions of personal computers. At the time of writing (25 May), the BIS estimated that the total electricity use of bitcoin mining equalled that of mid-sized economies such as Switzerland; and other cryptocurrencies also use ample electricity (see graph, left-hand panel). Put in the simplest terms, the quest for decentralized trust has quickly become an environmental disaster.

But the underlying economic problems go well beyond the energy issue and relate to the signature property of money: to promote "network externalities" among users and thereby serve as a coordination device for economic activity. The shortcomings of cryptocurrencies in this respect lie in three areas: scalability, stability of value and trust in the finality of payments.

First, cryptocurrencies simply do not scale like sovereign moneys. At the most basic level of decentralized trust, cryptocurrencies require each and every user to download and verify the history of all transactions ever made, including amount paid, payer, payee and other details. With every transaction adding a few hundred bytes, the ledger grows substantially over time. For example, in mid-May, the bitcoin blockchain was growing at around 50 GB per year and stood at roughly 170 GB. Thus, to keep the ledger size and the time needed to verify all transactions (which increases with block size) manageable, cryptocurrencies have hard limits on the throughput of transactions (see graph, centre panel).

To process the number of digital retail transactions currently handled by selected national retail payment systems (see graph, right-hand panel), even under optimistic assumptions, the size of the ledger would swell well beyond the storage capacity of a typical smartphone in a matter of days, beyond that of a typical personal computer in a matter of weeks and beyond that of servers in a matter of months.

But the issue goes well beyond storage capacity and extends to processing capacity: only supercomputers could keep up with verification of the incoming transactions. The associated communication volumes could bring the Internet to a halt, as millions of users exchange files on the order of magnitude of a terabyte.

Another aspect of the scalability issue is that updating the ledger is subject to congestion. Transactions have at times remained in a queue for several hours, interrupting the payment process. This limits cryptocurrencies' usefulness for day-to-day transactions such as paying for a coffee or a conference fee, not to mention for wholesale payments.

Thus, the more people use a cryptocurrency, the more cumbersome payments become. This negates an essential property of present-day money: the more people use it, the stronger the incentive to use it.

The second key issue with cryptocurrencies is their unstable value, due to the absence of a central issuer with a mandate to guarantee the currency's stability, a role in which well-run central banks succeed in stabilizing the domestic value of their sovereign currency by adjusting the supply of the means of payment in line with transaction demand.

This contrasts with a cryptocurrency, where generating some confidence in its value requires that supply be predetermined by a protocol, preventing it from being supplied elastically. Therefore, any fluctuation in demand translates into changes in valuation.

This outcome is not coincidental. Keeping the supply of the means of payment in line with transaction demand requires a central authority, typically the central bank, which can expand or contract its balance sheet. The authority needs to be willing at times to trade against the market, even if this means taking risk onto its balance sheet and absorbing a loss.

In a decentralized network of cryptocurrency users, there is no central agent with the obligation or the incentives to stabilize the value of the currency: whenever demand for the cryptocurrency decreases, so does its price.

Further contributing to unstable valuations is the speed at which new cryptocurrencies – all tending to be very closely substitutable with one another – come into existence, with several thousand now estimated to be in existence. As in past private banking experiences, the outcome of such liberal issuance of new moneys is rarely stability.

The third issue concerns the fragile foundation of the trust in cryptocurrencies. This relates to uncertainty about the finality of individual payments, as well as trust in the value of individual cryptocurrencies.

In mainstream payment systems, once an individual payment makes its way through the national payment system and ultimately through the central bank books, it cannot be revoked. In contrast, permissionless cryptocurrencies cannot guarantee the

finality of individual payments. The lack of payment finality is exacerbated by the fact that cryptocurrencies can be manipulated by miners controlling substantial computing power, a real possibility given the concentration of mining for many cryptocurrencies. Finality will always remain uncertain.

Not only is the trust in individual payments uncertain, but the underpinning of trust in each cryptocurrency is also fragile. This is due to "forking", a process whereby a subset of cryptocurrency holders coordinate on using a new version of the ledger and protocol, while others stick to the original one. In this way, a cryptocurrency can split into two subnetworks of users.

An episode on 11 March 2013 is noteworthy because – counter to the idea of achieving trust by decentralized means – it was undone by centralized coordination of the miners. On that day, an erroneous software update led to incompatibilities between one part of the bitcoin network mining on the legacy protocol and another part mining using an updated one. For several hours, two separate blockchains grew; once news of this fork spread, the price of bitcoin tumbled by almost a third. The fork was ultimately rolled back by a coordinated effort whereby miners temporarily departed from protocol and ignored the longest chain. But many transactions were voided hours after users had believed them to be final.

An even more worrying aspect underlying such episodes is that forking may only be symptomatic of a fundamental shortcoming: the fragility of the decentralized consensus involved in updating the ledger and, with it, of the underlying trust in the cryptocurrency.

Overall, decentralized cryptocurrencies suffer from a range of shortcomings. The main inefficiencies arise from the extreme degree of decentralization: creating the required trust in such a setting wastes huge amounts of computing power, decentralized storage of a transaction ledger is inefficient and the decentralized consensus is vulnerable.

Some of these issues might be addressed by novel protocols and other advances. But others seem inherently linked to the fragility and limited scalability of such decentralized systems. Ultimately, this points to the lack of an adequate institutional arrangement at the national level as the fundamental shortcoming.

While cryptocurrencies do not work as money, the underlying technology may have promise in other fields. A notable example is in low-volume cross-border payment services. More generally, compared with mainstream centralized technological solutions, DLT can be efficient in niche settings where the benefits of decentralized access exceed the higher operating cost of maintaining multiple copies of the ledger.

Permissioned cryptopayment systems may also have promise with respect to small-value cross-border transfers, which are important for countries with a large share of their workforce living abroad. Global remittance flows total more than $540 billion annually. While cryptopayment systems are one option to address these needs, other technologies are also being considered, and it is not clear which will emerge as the most efficient one.

More important use cases are likely to combine cryptopayments with sophisticated self-executing codes and data permission systems.

Policy implications

The rise of cryptocurrencies and related technology brings to the fore a number of policy questions. Authorities are looking for ways to ensure the integrity of markets and payment systems, to protect consumers and investors, and to safeguard overall financial stability.

An important challenge is to combat illicit usage of funds. At the same time, authorities want to preserve long-run incentives for innovation and, in particular, maintain the principle of "same risk, same regulation."

These are largely recurrent objectives, but cryptocurrencies raise new challenges and potentially call for new tools and approaches. A related question is whether central banks should issue their own central bank digital currency (CBDC) (see below).

A first key regulatory challenge is anti-money laundering (AML) and combating the financing of terrorism (CFT). Because cryptocurrencies are anonymous, it is hard to quantify the extent to which they are being used to avoid capital controls or taxes, or to engage in illegal transactions more generally.

A second challenge encompasses securities rules and other regulations ensuring consumer and investor protection. Fraud issues also plague initial coin offerings (ICOs). An ICO involves the auctioning of an initial set of cryptocurrency coins to the public, with the proceeds sometimes granting participation rights in a startup business venture. Many of these projects have turned out to be fraudulent Ponzi schemes.

A third, longer-term challenge concerns the stability of the financial system. It remains to be seen whether widespread use of cryptocurrencies and related self-executing financial products will give rise to new financial vulnerabilities and systemic risks.

Close monitoring of developments will be required. And, given their novel risk profiles, these technologies call for enhanced capabilities of regulators and supervisory agencies. In some cases, such as the execution of large-value, high-volume payments, the regulatory perimeter may need to expand to include entities using new technologies, to avoid the build-up of systemic risks.

The need for strengthened or new regulations and monitoring of cryptocurrencies and related crypto-assets is widely recognized among regulators across the globe. In particular, a recent communique of the G20 Finance Ministers and Central Bank Governors highlights issues of consumer and investor protection, market integrity, tax evasion and AML/CFT, and calls for continuous monitoring by the international standard-setting bodies. It also calls for the Financial Action Task Force to advance global implementation of applicable standards.

However, the design and effective implementation of strengthened standards are challenging. Legal and regulatory definitions do not always align with the new realities. The technologies are used for multiple economic activities, which in many cases are regulated by different oversight bodies.

Operationally, the main complicating factor is that permissionless cryptocurrencies do not fit easily into existing frameworks. In particular, they lack a legal entity or person that can be brought into the regulatory perimeter. Their legal domicile – to the extent they have one – might be offshore or impossible to establish clearly. As a result, they can be regulated only indirectly.

To implement a regulatory approach, three considerations are relevant. First, the rise of cryptocurrencies and crypto-assets calls for a redrawing of regulatory boundaries. Second, the interoperability of cryptocurrencies with regulated financial entities could be addressed. Third, regulation can target institutions offering services specific to cryptocurrencies. To avoid leakages, the regulation would ideally be broadly similar and consistently implemented across jurisdictions.

Should central banks issue digital currencies?

A related medium-term policy question concerns the issuance of CBDCs, including who should have access to them. CBDCs would function much like cash: the central bank would issue a CBDC initially, but once issued it would circulate between banks, non-financial firms and consumers without further central bank involvement.

Such a CBDC might be exchanged between private sector participants bilaterally using distributed ledgers without requiring the central bank to keep track and adjust balances. It would be based on a permissioned distributed ledger, with the central bank determining who acts as a trusted node.

While the distinction between a general purpose CBDC and existing digital central bank liabilities – reserve balances of commercial banks – may appear technical, it is actually fundamental in terms of its repercussions for the financial system.

A general purpose CBDC – issued to consumers and firms – could profoundly affect three core central banking areas: payments, financial stability and monetary policy.

A recent joint report by the Committee on Payments and Market Infrastructures and the Markets Committee highlights the underlying considerations. It concludes that the strengths and weaknesses of a general purpose CBDC would depend on specific design features.

The report further notes that, while no leading contenders have yet emerged, such an instrument would come with substantial financial vulnerabilities, while the benefits are less clear. At the moment, central banks are closely monitoring the technologies while taking a cautious approach to implementation.

Some are evaluating the pros and cons of issuing narrowly targeted CBDCs, restricted to wholesale transactions among financial institutions. These would not challenge the current two-tier system but would instead be intended to enhance the operational efficiency of existing arrangements. So far, however, experiments with such wholesale CBDCs have not produced a strong case for immediate issuance.

Chakravarthi Raghavan is Editor Emeritus of the *South-North Development Monitor* (*SUNS*), which is published by the Third World Network. The above originally appeared in *SUNS* (No. 8704, 20 June 2018).