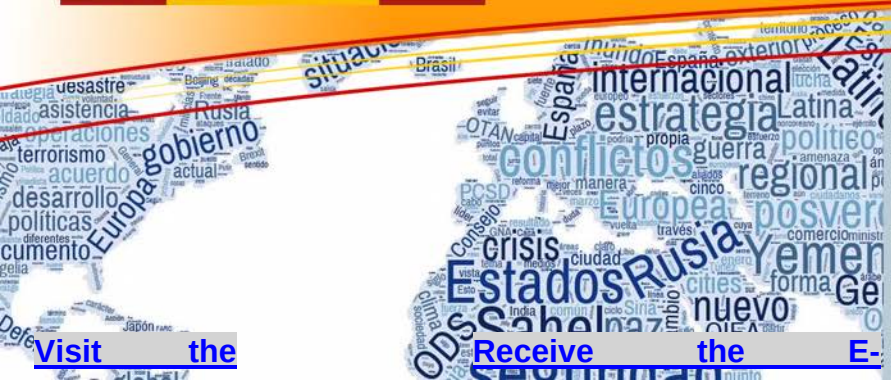
Analysis
Paper

34/2021 29/09/2021

David Ramírez Morán

Digital money



[Visit the](#) [Receive the E-](#)

Digital money

Abstract:

Digital money is a requirement for the world in which we live in currently, where most transactions are carried out by trust links between stakeholder and/or a maybe third actor that provides trustfulness to the transaction. Several models have appeared under this approach, and it is in cryptocurrencies based on ledger technologies where alerts have emerged given the illicit uses available thanks to the anonymity the transactions may have. Anonymity might foster the use of these tools to fundraise and support criminal activities although, according to different studies, while crime is making use of these tools, this is not the case for terrorist groups.

Keywords:

Digital currency, cryptocurrency, terrorism, criminality, digital coin.

How to cite this document:

RAMÍREZ MORÁN, David. *Digital money*. IEEE Analysis Paper 34/2021. https://www.ieee.es/Galerias/fichero/docs_analisis/2021/DIEEEA34_2021_DAVRAM_Dinero_ENG.pdf y/o enlace bie[3]

Dinero digital

Resumen:

El dinero digital es una herramienta imprescindible para el mundo actual en el que la mayor parte de las transacciones se llevan a cabo mediante vínculos de confianza entre las partes involucradas y/o un posible tercero que de fiabilidad a la transacción. Son varios los modelos que han ido surgiendo bajo esta aproximación y en las criptomonedas basadas en tecnologías de confianza distribuida existe preocupación por los usos ilícitos que se pueden hacer gracias a las características de anonimato que pueden tener las transacciones. Este anonimato podría fomentar la utilización de estos medios para financiar y respaldar actividades criminales, aunque, de acuerdo con varios estudios, mientras la delincuencia si está haciendo uso de estas herramientas, no ocurre lo mismo en los grupos terroristas.

Palabras clave:

Divisa digital, criptodivisa, terrorismo, delincuencia, moneda digital.

INTRODUCTION

For quite some years, digital money has been receiving more and more attention both from the specialist sectors and, increasingly, from the general public. Several models have led to this evolution, which is why the term digital money has been used in this paper.

Under the term 'digital money', and understanding this as the possibility of making monetary transactions without using a tangible currency, it is necessary to include a technology that initially had nothing to do with the digital world but nowadays depends almost entirely on it. These are credit and debit cards, which to all intents and purposes now implement a digitisation of tangible currency because payments made with them are based on a relationship of trust between the three parties involved: the buyer, the seller and the issuing bank. Transactions carried out with these means are recorded in transaction processing systems enabling forensic analysis and identification of the transactions and individuals involved.

Before the arrival of the first publicly available cryptocurrency, bitcoin, the alternative use of virtual currencies or credits implemented in multiplayer online video games had been detected for the acquisition of in-game goods and services that allowed a faster evolution or the achievement of certain objectives. Certain users hoarded these coins or credits and traded through the games' own communication tools or through external platforms the sale of packs of these credits or items purchased with them. The virtual currencies in the gaming environment thus became digital assets with a tangible currency quotation.

The arrival of bitcoin[1] in 2009 opened the way for cryptocurrencies and aroused interest in issues that are still highly topical today, such as the anonymity of transactions, the lack of backing for the currency, etc. Over the following years, new currencies based on blockchain technology to collect transactions emerged. The new options provided features such as increased anonymisation measures for transactions, other algorithms to avoid concentration of block capacity on the blockchain, and the democratisation of mining. New blockchain usage models also emerged with platforms and currencies such

[1] Satoshi Nakamoto. "Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer" https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

as ethereum and ether allowing for smart contracts, which are applications that are loaded onto the blockchain itself and run in a fully automated way.

2017 saw the simultaneous launch of a multitude of ICOs. An Initial Coin Offer (ICO) is the equivalent of a company's IPO where the shares are materialised in the form of a cryptocurrency or token whose value will be governed by the law of supply and demand between those who want to dispose of the tokens and those who want to acquire them to become part of the company's investors. In regulated markets, before a public offering, traditionally known as a flotation, the company has to comply with a series of requirements to ensure transparency and investor protection, which are imposed by bodies and authorities that subject the operation to current legislation. In an ICO, all liability is placed on the issuer of the cryptocurrency. There is no authority to analyse the operation and its compliance with the law. In fact, it is not clear which legislation applies. In practice, there have been cases where an individual has launched an ICO that has subsequently turned out to be a fraud and national legislation has been applied to bring them to justice.

Initially, it was relatively easy to gain access to the world of cryptocurrencies by installing software on a private computer that incorporates blocks into the blockchain in exchange for a reward in the form of a certain amount of the cryptocurrency itself. This operation is called mining because of its similarity to the work of extracting raw materials. The growing interest in mining cryptocurrencies drove these users out as their computing power lagged far behind that of the new players, who used more specific hardware such as graphics cards or integrated circuits designed specifically for mining. They provide a higher return because they perform operations faster, are more likely to find the right results, and do so in a more energy-efficient manner. With the rapid price increases of some cryptocurrencies due to new miners, the option of mining was completely out of reach for the normal user.

Exchange houses emerged, allowing cryptocurrencies to be bought or sold as tradable assets, decoupling the customer from the technologies that support them. Exchange houses are the interface between the tangible financial world and the virtual financial world, allowing the purchase of digital assets in exchange for tangible money and the sale of digital assets in exchange for their countervalue in tangible money. However, the

cryptocurrency holder's relationship with the decentralised and distributed infrastructure again required placing trust, especially in terms of anonymity, in the exchange's platform. Nowadays there are even ATMs where cryptocurrencies can be acquired by paying with a bank card, although, at least in the case of Spain, they are not anonymous and require identification data to be provided.

Once again, in an open world where the anonymity of cryptocurrencies and the advantages they provide are valued, various alternatives are being developed, known as DeFi, decentralised finance[2], which aim to give the normal cryptocurrency user back the possibility of being able to operate without having to place their trust in a third party. These are applications based on the use of smart contracts that are automatically executed by the digital currency infrastructure, the distributed network of nodes that manages transactions. This has led to the creation of tools for automated loan management, decentralised exchange houses, derivative tools that allow speculation on currency exchange rate changes or assets in the form of digital tokens, NFTs, which allow the sale of digital assets such as art or other intangibles.

States are no strangers to the evolution of digital currencies and are identifying the advantages they provide over traditional currencies. They are evaluating the creation of digital currencies backed by their own currency or with their own resources, with which to establish a reliable and regulated environment for citizens to trade safely and securely. CBDCs, Central Bank Digital Currencies, are on the agendas of numerous central banks including the European Central Bank[3], the PBoC, and the People's Bank of China. They are also being used for other purposes such as leveraging the decentralised nature to establish trading channels to avoid internationally imposed sanctions.

In 2019 it was announced that Facebook, as the main promoter, and in partnership with other large companies in the financial sector, intended to create a new cryptocurrency, Libra[4], aimed at facilitating financial transactions for users of its application. As designed, it proposes a parallel economic system to the traditional one, for which implementing

2 The Complete Beginner's Guide to Decentralized Finance (DeFi) https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi

3 "A digital euro" https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html

4 Eduardo Ricou. Libra (LIBRA) Coin: Facebook's Cryptocurrency. https://stormgain.com/blog/libra-coin-facebooks-cryptocurrency

legislation and mechanisms to fit into the current economic system have not yet been put in place.

Finally, we should not forget platforms such as Apple pay or Paypal, where these platforms act as an intermediary between the user and the bank of which they are a customer through the user's payment card or current account. The use of these tools aims to protect user information by providing a mechanism that allows the specific information of the account or card with which a transaction is made not to be known by the counterparty. This reduces traditional risks such as number theft or card cloning and protects the payer's privacy by hiding the company that manages their finances.

CHARACTERISTICS OF CRYPTOCURRENCIES

Cryptocurrencies have a number of characteristics that differentiate them from traditional tangible currencies and that constitute advantages over the latter depending on the use cases or applications for which they are intended to be used

Anonymity

The anonymity of cryptocurrencies is based on the difficulty of identifying the owner of a cybercurrency, or a balance of them, only through a number or sequence of values that identifies the individual user. The anonymity of cryptocurrency transactions is only anonymous as long as it is not possible to establish a link between the user's wallet identifier and the user's real identity.

Cryptocurrencies such as *monero* provide an additional degree of anonymity because, unlike others such as bitcoin, new disposable identifiers are generated at the destination of each transaction and only the destination can determine the origin. To disguise the origin of the transaction, it includes a so-called ring mechanism that makes it difficult to identify the true originator of a transaction by having the signature made by one individual among several individuals with the same balance. Also the amount is hidden through the use of the Ring Confidential Transaction so that only the ends of the transaction will know the amount even if the transaction appears in the chain.

Mining

Mining is the name applied to the computer operations used in various cryptocurrencies for the incorporation of transactions into the blockchain. The security of the blockchain relies on the existence of a proof that validates the information that an actor tries to add to the blockchain.

Proof of work is the mechanism used in cryptocurrencies to ensure the reliability of transactions and eliminate the possibility of earlier blocks in the chain being modified at a later date.

One of the main factors affecting the profitability of mining is the price of energy. Running the algorithms to find the number that results in a validated block requires increasing amounts of electrical power. This is why in 2019 an estimated 65% of cryptocurrency mining capacity was located in China[5]. This concentration of mining capacity also poses a problem for the reliability of the coins, as the trust mechanism requires that no single party involved in mining has more than 51% of the capacity[6], otherwise it could block the network by monopolising the mining.

Recently there was an article in a generalist newspaper about the installation of mining devices on Turkish farms[7] as a tool to fight inflation.

The algorithm governing Bitcoin mining has led to what was previously explained as the *de facto* expulsion of small miners. Mining capacity measured in hashes per second currently reaches exahash (10 raised to 15) per second to keep up with the bitcoin block addition rate of 10 minutes per block. Only by using specific mining devices is it possible to achieve cost-effective mining to cover the costs of the device and especially of the energy required. Against this backdrop, other currencies have resorted to different algorithms that do not allow for such efficiency to be achieved through the use of dedicated devices. This encourages small miners to qualify for the rewards associated

[5] Roger Huang. "The 'Chinese Mining Centralization' Of Bitcoin And Ethereum https://www.forbes.com/sites/rogerhuang/2021/12/29/the-chinese-mining-centralization-of-bitcoin-and-ethereum/

[6] https://academy.binance.com/en/articles/what-is-a-51-percent-attack

[7] "Los turcos apuestan por las criptomonedas como valor refugio ante la inflación" https://www.expansion.com/mercados/2021/06/19/60cdd409e5fdea226d8b4599.html

with inserting a block, and makes it once again viable to use a normal computer for mining. *Monero* is again an example of a cryptocurrency whose algorithm is adapted to these characteristics.

However, this virtue also becomes a risk because any internet user's computer or any server can carry it out. This has been exploited by both legal actors and criminals to use the computers of users and companies for mining. Lawfully by informing the user that, for example, while browsing a website their computer is mining cryptocurrency for the benefit of its owner, and unlawfully by fraudulently introducing cryptomining algorithms into third-party websites by exploiting a vulnerability or gaining access to the processing power of a vulnerable internet server and using its computing power for mining. In the case of Spain, the National Cryptologic Centre's "Report on cyber threats and trends 13/20" also identified this threat[8].

Volatility of digital currencies and stable coins

The volatility of digital currencies is one of the main issues that raises questions about their day-to-day use beyond speculative trading. There have been episodes of high volatility in cryptocurrencies due to events of little relevance, such as the publication of a Twitter post by Elon Musk or the incorrect publication of a web page in which it appeared that a large company was going to start accepting a digital currency as a means of payment. High volatility refers to price changes of more than 20% in less than one week. 2019 was an example of this volatility, with bitcoin starting the year at around $1,000 and ending it at around $20,000.

Stable currencies, on the other hand, are digital currencies whose price is backed by a physical asset or pool of assets, such as a currency, a foreign exchange or commodities. They arise from the problem of the volatility of other currencies whose value fluctuates solely on the basis of supply and demand. This price stability allows a more secure use in financial terms and avoids behaviour such as hodling[9], a term used to describe, in the context of cryptocurrencies, the attitude of a cryptocurrency holder who, faced with a rapid

[8] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html

[9] This name comes from the typo of a forum member who wrote hodl instead of hold when stating that he would not dispose of his cryptocurrencies in order to take advantage of the growth in their price.

increase in their price, decides to keep them to benefit from their appreciation instead of spending them to acquire assets.

In the case of ICOs, the backing of the cryptocurrency is the company's own real value. Its share price is therefore the result of factors that are common in the financial world of listed companies. Variables such as expectations, the evolution of the company and all those factors external to the company that may affect its business model come into play.

Fungibility

Fungibility is a property whereby the units that make up a currency can be identified individually or if all of its units are indiscernible from each other. Coins of a non-fungible nature allow for the individual identification of a specific currency and could declare certain coins invalid, allow the identification of coins that have been used in certain transactions and therefore identify perpetrators who may have been involved or related to criminals on the basis of the funds they have received and to whom they have been sent. This is a feature that differentiates, for example, bitcoin, a non-fungible currency, from monero. In fact, the monero website highlights this feature when demonstrating the greater privacy and security of this currency compared to bitcoin.

Forensic analysis

The blockchain associated with a cryptocurrency contains all transactions made to date with the cryptocurrency. The identity of users is protected by the numerical identifiers of their wallet but, if it is possible to establish the relationship between a wallet and a person, the transactions made by this person could be identified. From these transactions it would be possible to trace forward or backward transactions in order to identify who sent funds to this person or to whom this person has sent funds.

In order to make this analysis more difficult, so-called mixed transactions are carried out, whereby the amount of a transaction is subjected to a large number of additional intermediate transactions in order to make it more difficult to identify the originator and the recipient of a transaction. Today, with the computing and storage power available and with the application of artificial intelligence, it is possible to investigate these mixed transactions and extract source and destination information.

But for forensic investigations to be able to take action, it is essential that a link exists or is found between a physical identity and the wallet code or identifier under which that person trades cryptocurrencies.

STATES AND DIGITAL MONEY

Currency or asset?

For the purposes of States, this differentiation is important because it differs in the legislation applicable to users of cryptocurrencies.

In the case of being considered as an asset, users would operate with them by acquiringor selling them, paying the taxes corresponding to the profit obtained from them.

In the European Union, work is underway to regulate exchange houses to allow for the supervision of cryptocurrency transactions. As an asset whose price varies over time, the user of the cryptocurrency will have a capital gain or loss due to the difference in price from the time of acquisition to the time of disposal of the cryptocurrency.

All players who do not use exchanges to acquire or dispose of cryptocurrencies would therefore be excluded from this supervisory power.

Venezuela

In 2018, Venezuelan President Nicolás Maduro announced the creation of Petro[10], a cryptocurrency that would allow the country to continue importing and exporting goods while avoiding the sanctions imposed by which numerous foreign accounts were blocked, making it difficult to export its main sources of income, oil and gas. The president said that each element of the currency would be backed by a barrel of oil.

Shortly afterwards, US President Donald Trump issued an executive order banning "All transactions related to, provision or financing or otherwise in [...] any digital currency,

[10] https://petro.gob.ve/es/

digital currency or digital object issued by or for the benefit of the Government of Venezuela".[11]

This cryptocurrency has been criticised for its limited impact in the world of cryptocurrencies as it is not available on exchanges and has a practically unidirectional usage model in which only foreign citizens can acquire it to spend it on goods and services provided in the country.

El Salvador

On 6 September 2021 Bitcoin became legal tender in El Salvador in a highly controversial move that has sparked significant social backlash. With this measure, both citizens and businesses are obliged to accept payments and receipts in this currency.

The rejection has been mainly motivated by the perception that cryptocurrencies, because of their anonymity, are conducive to crime and corruption.

This measure requires the population to incorporate digital technologies in their daily lives because only those who have the application installed on their mobile phones will be able to access the cryptocurrency without fees,

This is highly controversial because it places the economic future of a country on the evolution of a fiat currency without any backing beyond the trust of its users.

It is interesting to assess the effects of introducing Bitcoin in a dollarised economy such as El Salvador. It is a dollarised economy and therefore has very little ability to control the domestic economy with measures such as exchange controls on its own currency. It can only take macroeconomic action by controlling interest rates. The introduction of bitcoin does not change this situation either, as the price of the digital currency is also denominated in dollars and is determined by external factors. Therefore, the interest in introducing Bitcoin in the country responds to the other advantages it brings, such as the reduction of fees for remittance transfers compared to traditional financial systems and the reduction of the time required to complete these transactions, both very relevant

[11] https://www.cnbc.com/2018/03/19/trump-issues-action-blocking-us-citizens-from-trading-or-financing-venezuela-cryptocurrency.html

aspects if we take into account that "remittances represent more than 24% of the Gross Domestic Product"[12] according to data from the World Bank.

The day-to-day use of bitcoin through e-wallets would not be a problem if the country were self-sufficient because, regardless of its value outside the borders, transactions inside the country would not be affected by exchange rates. This would reduce the country's need for foreign exchange, in particular for the dollars that are currently necessary for the functioning of the country's economy. However, this is not the reality and the country has to make both imports and exports, which are generally paid for in dollars. Therefore, the prices of imported products will affect the purchasing power of a citizen who uses the cryptocurrency to buy a product whose price has been adjusted to the dollar costs of its raw materials.

Through the application developed to manage users' virtual wallets, called Chivo, it is possible to buy and sell and exchange currency between the cryptocurrency and the dollar without fees. This operation is only subject to exchange rate fluctuations between the two currencies and therefore the exchange rate risk is borne by all citizens.

To encourage the introduction of the digital currency, the government will provide each citizen who installs the Chivo e-wallet with $30 worth of bitcoin. These are wallets associated with individuals, which would allow for a quick analysis of transactions between citizens in the country. This analysis could facilitate the identification of tax fraud in cryptocurrency transactions. Therefore, the widespread use of electronic currency as opposed to US currency in the form of cash could lead to a reduction in economic crime, tax evasion and corruption. Forensic analysis of the blockchain would make it possible to identify each citizen's income and expenditure and to identify fraud.

Nayib Bukele, the country's president, also advanced plans to dedicate geothermal energy to cryptocurrency mining. This is in an attempt to locate on Salvadoran territory the mining capacity that has left China following the ban on mining in that territory and provides a rebuttal to claims about the enormous amount of energy required for mining.

[12] https://www.criptonoticias.com/comunidad/adopcion/dice-gente-asi-estan-cajeros-bitcoin-chivo-salvador/

China

One of the countries in which cryptocurrency issues have been most widely discussed is China. There are several factors that have motivated this, starting with the possibility of having access to money that is not controlled by the authorities.

In 2017, in view of the obvious risks posed by ICOs, it declared them to be illicit sources of funding and banned ICO trading on its territory.[13] This decision was swiftly followed by a significant fall in the prices of the main cryptocurrencies.

The price of energy in certain areas of China led to an explosion in the deployment of cryptocurrency mining capacity, especially Bitcoin. Mining directly reports cryptocurrencies to the owner of the equipment that manages to find the algorithmic solution to include a new block in the chain.

One of the latest measures taken by the country is a ban on cryptocurrency mining on its territory. The energy footprint of mining is significant and many mining infrastructures had been located in the country to take advantage of low energy costs, mainly hydroelectric, in some regions of the country.

On 24 September 2021, the PBoC has declared illegal all activity related to digital currencies «not issued by monetary authorities, using cryptography, distributed accounts or similar technologies, and existing in digital form», both in its territory or that developed overseas providing services to residents in China[14].

Digital Yuan

Since 2014, China has been working on the creation of the digital Yuan, a digital currency whose exchange rate corresponds directly to the traditional yuan. For each digital yuan

[13] China bans initial coin offerings calling them 'illegal fundraising' https://www.bbc.com/news/business-41157249

[14] "Notice on further prevention and disposal of the risk of speculation in virtual currency trading". Available in: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4348521/index.html (in Chinese)

distributed by banks, banks must deposit the same amount as a reserve at the PBOC[15]. In this way there is no volatility in the price of the digital currency. The duality of currencies, however, allows for economic practices such as monetary policy interventions on certain regions, classes or other groups, and could even impose negative interest rates on electronic cash to encourage consumption.

Citizens use QR codes generated by the digital wallet to make payments and these transactions are validated directly by the bank, as the digital currency is not based on a distributed trust technology such as blockchain. This allows transactions to be streamlined as the time required to validate the transaction can be drastically reduced.

FINANCING OF ILLEGAL ACTIVITIES

Cryptocurrencies are often associated with illegal activities because they provide anonymity in electronic transactions that is not possible with traditional banking systems. It is possible to exchange cryptocurrency between two unidentified individuals without relying on third parties. However, this anonymity disappears when virtual currency has to be converted into tangible currency or goods. This is when a cryptocurrency holder must match the anonymous identifier with a real-world ID.

The G20 meeting held in Argentina in 2018 reported that "[f]inance ministers and central bankers from the world's 20 largest economies meeting in Buenos Aires will be told on Tuesday that such "crypto assets" do not threaten financial stability but can serve to launder money or finance terrorism and hurt consumers who buy them"[16] where it was reflected that the capitalisation of the digital currency market did not pose a risk to global financial stability and, therefore, to its security, although there were scenarios where these tools could contribute to insecurity by facilitating money laundering, terrorist financing and financially harming those consumers who acquire them.

15 Alun John. “Explainer: How does China's digital yuan work?” https://www.reuters.com/article/us-china-currency-digital-explainer-idUSKBN27411T 20210923

16 Francesco Canepa. “G20 leaders to hold fire on cryptocurrencies amid discord: sources”. https://uk.reuters.com/article/us-g20-argentina-bitcoin/g20-leaders-to-hold-fire-on-cryptocurrencies-amid-discord-sources-idUKKBN1GV2QR

Recently, a retired former CIA employee with ties to a cryptocurrency intelligence company published a paper in which he also concluded that cryptocurrencies do not currently provide the anonymity required for criminal activity and that mechanisms already exist to apply intelligence to blockchains and identify suspicious behaviour. The ability to analyse the most complex mixed transactions using artificial intelligence techniques is available.[17] The graph in Figure 1 shows how the percentage of illegal activity dropped sharply with the closure of the illegal drugs and weapons shop, Silk Road, and how since then, by the standards of the company conducting the study, it has been below one percent of recorded cryptocurrency activity.

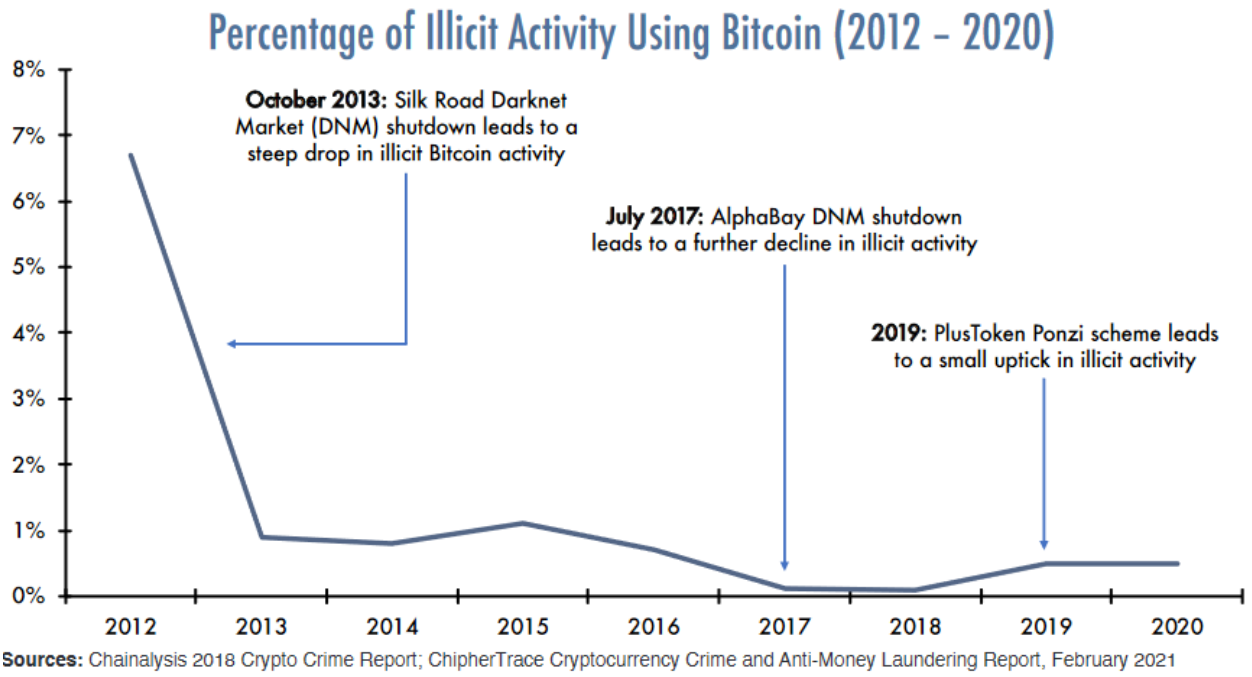


Figure 1 Evolution of illicit activity using Bitcoin (Source: Morell)

In turn, Figure 2 shows that the total capitalisation of all cryptocurrencies does not reach two trillion dollars, which, although it represents an amount greater than Spain's GDP, for global purposes does not constitute a sufficient amount to affect global financial stability.

[17] Michael Morell et al. "An Analysis of Bitcoin's Use in Illicit Finance" https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf

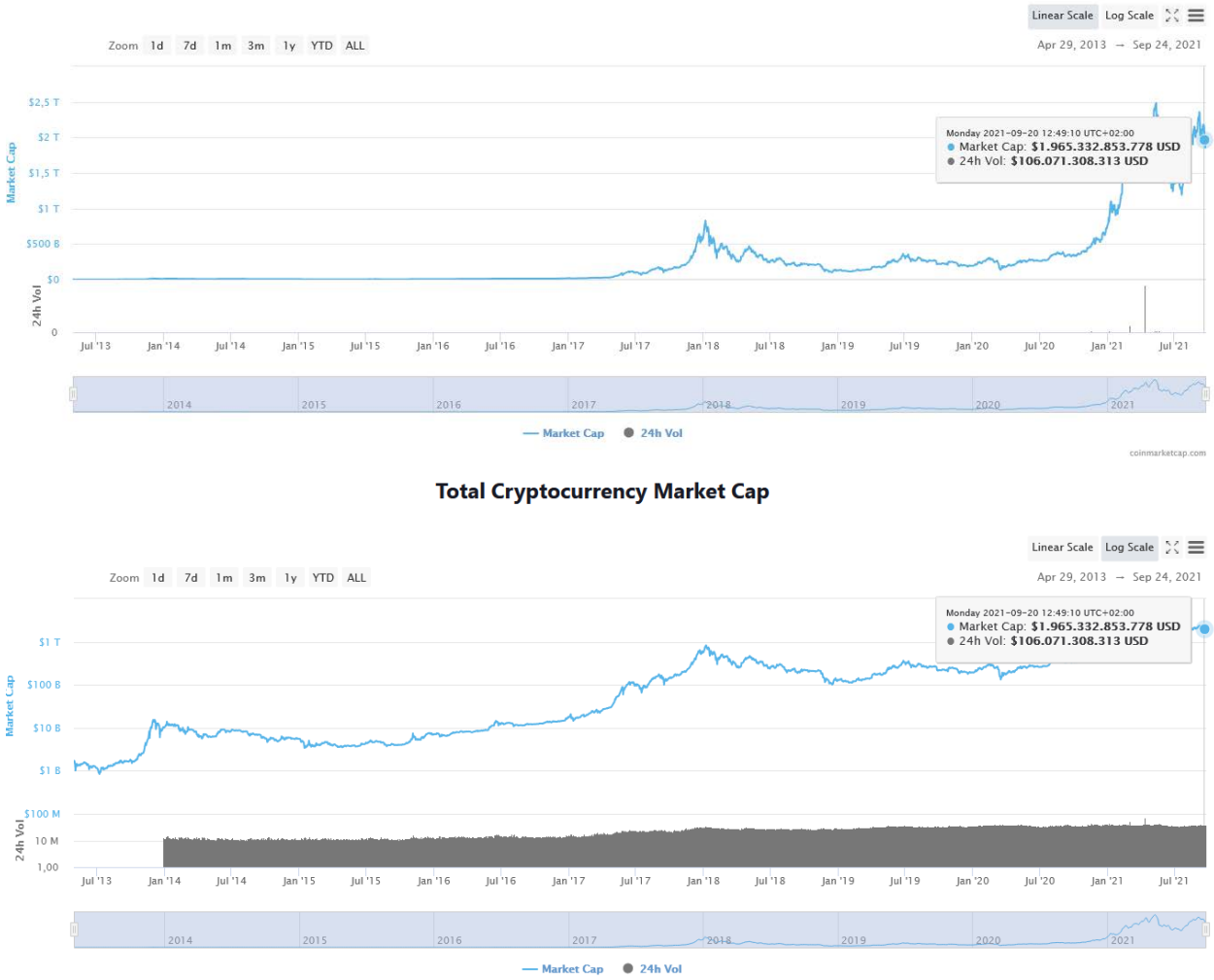


Figure 2 Evolution of cryptocurrency capitalisation (Source: https://coinmarketcap.com/charts/)

Sanctions

Distributed currencies offer states an alternative to international financial systems. Sanctioned states may see their foreign accounts blocked so that they cannot carry out transactions such as importing or exporting goods or accessing funds deposited in those accounts. In distributed currencies, there is no authority that can carry out this blocking, so sanctioned states could continue to conduct transactions with those actors willing to use this mode of payment.

Terrorism

As noted above, there is international concern about how cryptocurrencies can be used by terrorists.

The European Union addressed this issue in a study conducted in May 2018[18]. It also concluded that the use by terrorist groups of cryptocurrencies to carry out their activities was testimonial and did not constitute a significant risk to date.

Rand Corporation published an extensive study[19] along these lines that addressed this problem with an analysis for various terrorist groups in order to be able to expose the different situations in which they could make use of cryptocurrencies according to their particular structure and functioning.

The paper analyses the five activities identified as of greatest interest to terrorist organisations: financing, illegal trafficking of arms and drugs, sending and receiving funds, financing attacks, and operational financing.

In order to do so, they identified the characteristics necessary for cryptocurrencies to be of use to terrorist groups: anonymity, usability, security, acceptance, reliability and volume; and concluded that currently none of the main existing cryptocurrencies meet all of these criteria simultaneously. However, they warned that the continuing advance in cryptocurrency technology requires continued market monitoring to identify when these features might occur simultaneously.

They concluded, in line with the results obtained, that the alarm on this line does not currently constitute a major risk.

Crime

Crime is the area that is currently making most use of cryptocurrencies to benefit from the anonymity they provide. The scenario in which they carry out their activities is very different from that of terrorism and therefore does not require the same characteristics as terrorist groups. Existing solutions are already sufficient to meet the needs of their operations and, in fact, are continuously being developed.

Online scams such as the CEO scam, where the offender poses as the head of the organisation and instructs financial bodies to make urgent transfers, accessing bank

[18] Tom KEATINGE, David CARLISLE, Florence KEEN. "Virtual currencies and terrorist financing: assessing the risks and evaluating responses". https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

[19] Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston. "Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats". https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

users' current accounts or stealing credentials are the order of the day. The ransomware phenomenon whereby the attacker exploits a vulnerability in the systems, encrypts the information and then demands a ransom to provide the decryption key also occurs very frequently. All of these attacks involve the need to get the swindled money into the criminal's coffers, and this is where cryptocurrencies are being used.

For illustrative purposes, the following are two significant cases in this line, such as the already famous case of Colonial, and how measures are beginning to be taken to reduce the impunity with which it is possible to use cryptocurrencies for crime.

Attack on Colonial

The attack on the IT infrastructure of the American fuel distribution company Colonial had spill-over effects that even affected the price of oil. In fact, the incident was considered a national emergency because the attack led to oil supply problems in much of the east coast of the United States.

It was a system hijacking attack, a ransomware attack, for which a reward was demanded to recover the information and control of the company's IT assets. This was the most visible effect of the attack, although it cannot be ruled out that, in addition to the kidnapping, the criminals had previously obtained confidential information or altered the functioning of the company's systems.

The payment of this reward was made via bitcoin to the address indicated by the hijackers. Within days, a significant portion of the reward was recovered because the secret key protecting the e-wallet of the group that had launched the attack was available to the US authorities and they were able to recover part of the ransom funds[20]. The rest of the funds could not be recovered because they had been remitted to another party involved in the operation, an organisation that provides services, lends its infrastructure, to carry out operations such as the one that occurred.

Sanctions on exchange houses

In a recent development, the United States has sanctioned a Russian exchange for its contribution to cryptocurrency laundering "by providing material support to the threat

[20] Paul Ducklin. “How could the FBI recover BTC from Colonial’s ransomware payment?” https://nakedsecurity.sophos.com/2021/06/09/how-could-the-fbi-recover-btc-from-colonials-ransomware-payment/

posed by criminal ransomware authors". According to the investigation, a significant part of the volume of cryptocurrencies coming into the company came from illegal activities such as ransomware attacks, scams, illegal marketplaces, etc.[21]

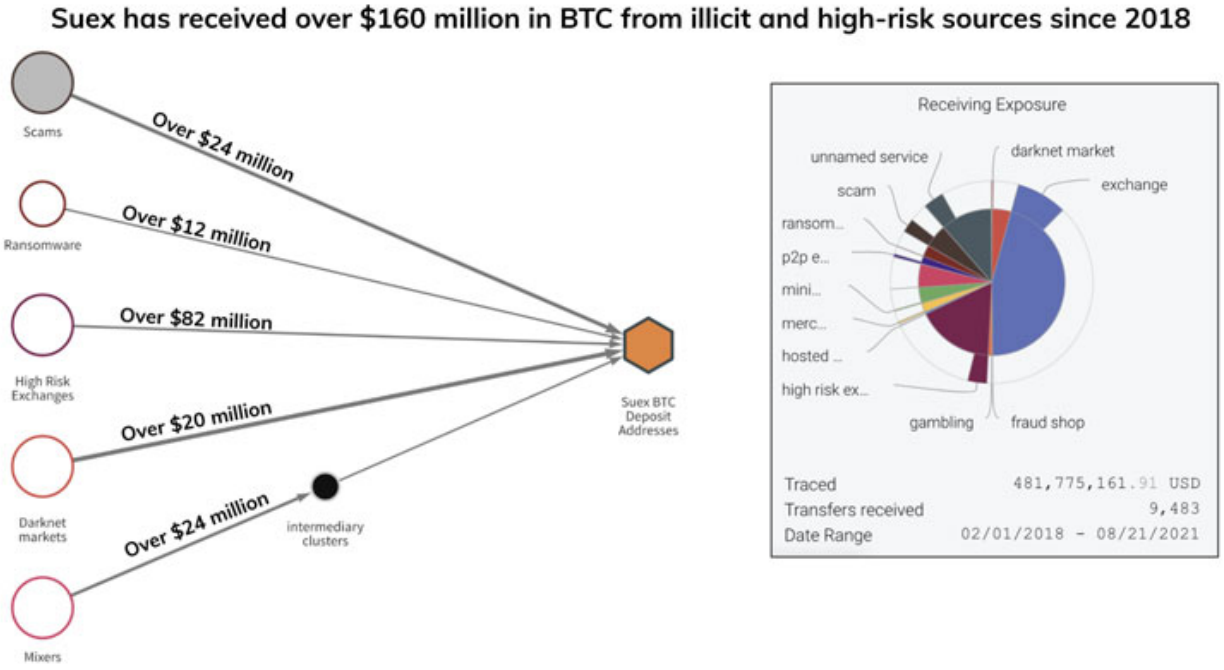


Figure 3 Breakdown of SUEX revenues (Source: www.thehackernews.com)

CONCLUSIONS

Digital currencies are a reality today and, given the increasing digitisation of societies globally, it is foreseeable that they will only grow. Central banks are working to enable citizens to take advantage of the benefits that these technologies bring in a secure and trusted environment.

Despite the general perception that cryptocurrencies are used for illicit purposes, which is fuelled by the continuing emergence of cases where they have appeared as necessary tools for crime, there is also a growing private sector interest in these new financial tools.

The main source of security risks posed by cryptocurrencies today is of an eminently economic nature and stems mainly from the lack of regulation. This regulation is either

[21] Ravie Lakshmanan "US Sanctions Cryptocurrency Exchange SUEX for Aiding Ransomware Gangs" https://thehackernews.com/2021/09/us-sanctions-cryptocurrency-exchange.html

incomplete or not easily enforceable in the face of distributed technologies that lack nationality and accountability.

In the case of the more developed countries, where the use of electronic means of payment is more widespread, the implementation of a digital currency as opposed to the tangible alternative makes little difference to the vast majority of users. In the case of eliminating tangible currency, the impact on activity would be negligible, although illicit activities that used to make use of cash payments will be forced to change their practices.

In less developed societies, the implementation of digital currencies is a double challenge, given the need to generate the necessary trust among the population and to provide the technological means, infrastructures and devices, as well as the necessary training, so that no segment of the population is excluded from the digital payment revolution.

The digitisation of payments is a tool that can contribute to the reduction of corruption and fraud as every transaction leaves a trace. However, this crime-fighting advantage comes at the expense of the loss of anonymity that is achieved with the use of cash and, moreover, can be a violation of citizens' privacy. In repressive environments, it can be an important tool to control the population and provide rulers or companies with information.

While in the area of crime many activities have been identified that benefit from the characteristics of digital currencies, it is also true that the capabilities that states are developing to analyse information are shifting the fight to the side of law enforcement.

In contrast, two reports conclude that the use of cryptocurrencies for terrorist financing is currently testimonial because they do not provide the necessary features for these groups to use them securely to carry out their activities. Therefore, the alarm generated around cryptocurrencies in this respect can be considered unjustified as long as cryptocurrency technology does not develop the functionalities it currently lacks.

*David Ramírez Morán**

Main Analyst at the Spanish Institute for Strategic Studies