EPRS
European Parliamentary Research Service

Briefing
11/04/2014

Bitcoin

Market, economics and regulation

SUMMARY

Bitcoin is a digital currency which started circulating in 2009. It was the first form of virtual money to become relatively popular. Bitcoin is public in nature as it maintains a log of all transactions. These are verified by its users in a process called mining. The extent of computing power and energy needed to mine bitcoins is set to increase over time. The main advantages of Bitcoin in comparison to traditional currencies are low transaction fees, and anonymity of use. It also has numerous drawbacks, in particular high price volatility, being prone to security breaches, inelastic supply coded by mathematical formula, lack of legal security as well as numerous risks stemming from its immaturity as a currency.

Due to the anonymity embedded in the system Bitcoin has the potential to be used for money laundering and tax evasion. However, research so far shows this potential has not yet been taken up on a significant scale. Regulation of Bitcoin is at a nascent stage with those systems so far instituted characterised by strict capital controls banning its use, and a few governments aiming to ensure it is covered for tax purposes. Many central bank authorities have issued warnings about Bitcoin, mentioning in particular its high price volatility and lack of consumer protection as the main risks to its users.

Despite demonstrating the breakthrough in technology, Bitcoin's future as a currency remains far from certain. The inevitable increase in regulation will increase transaction fees and reduce the anonymity of its use, two of its main strengths. Bitcoin might not become an established currency due to its volatility and ensuing lack of wide acceptance, but it holds promise for its technology.

In this briefing:

Author: Marcin Szczepański, Members' Research Service
European Parliamentary Research Service
140793REV1
http://www.eprs.ep.parl.union.eu — http://epthinktank.eu
eprs@ep.europa.eu

EUROPEAN PARLIAMENT

Glossary

Bitcoin: Term used when describing the entire Bitcoin concept or network.

bitcoin: Term used to describe a unit of Bitcoin currency.

Cryptocurrency: A digital, virtual or electronic currency that uses cryptography for security.

Fiat currency: Money declared by a government to be legal tender. It is not based on or convertible to gold, silver or other commodities. All central bank emitted currencies are currently fiat.

What is Bitcoin?

Bitcoin is an electronic peer-to-peer (i.e. with no third party being involved) payment network and a digital currency. It started in 2009. Its main feature is decentralisation – not being backed by or tied to any government or central bank. Bitcoins can be used to buy and sell items and services. They can also be exchanged for fiat money. The price of bitcoins is set purely by market demand and supply.

Short history of Bitcoin

Attempts to create a virtual currency have been linked to the creation of online communities. The Internet appears to have many advantages for the creation of a new means of payment specific to it, and aimed at making transactions easier, safer and cheaper than traditional money. The double-spending problem (spending the same money twice) prevented earlier attempts from being successful. A way of overcoming this weakness was first mentioned in the 2008 paper by Satoshi Nakamoto. There is on-going speculation about whether this is a real person or the pseudonym of the group of people who designed Bitcoin. The domain bitcoin.org was registered in 2008 but the identity of the person(s) behind it is protected from being made public. In January 2009 the first batch of bitcoins was generated (the so-called "genesis block" or "block 0"). The first exchange rate for bitcoin was published in October 2009 by New Liberty Standard (US$1 corresponded to 1 309 bitcoins). Public trading began in 2010, and the recent market capitalisation of Bitcoin amounts to over US$5.29 billion. On average, the Bitcoin market encompasses less than 100 million US dollars in worldwide trading activity on a daily basis (for comparison, daily trading is US$16.5 billion for Visa and US$9.8 billion for MasterCard). Nonetheless, Bitcoin's success has resulted in other cryptocurrencies being created.

How does it work?

The Bitcoin system relies on complicated mathematical-based cryptography (encoding) to secure its data and money creation, and prevent communication among members from being accessible to third parties. All bitcoins and users have their own unique identity and each transaction is recorded in a public ledger (which acts as a digital financial record book with a record of all Bitcoin transactions in chronological order). This ledger, called the "blockchain" in Bitcoin terminology, is visible to all computers on the network, but does not disclose personal information about the parties involved in transactions. The public nature of the ledger helps to prevent double-spending of the same bitcoins, and also eliminates the need for a third party to verify transactions between buyers and sellers.

To become part of the Bitcoin network, users need to download the free and open-source software (which has a publicly available control code). Users may obtain bitcoins by buying them with conventional money on one of the exchange platforms. Otherwise,

a user can obtain bitcoins in exchange for the sale of goods or services or through a process called "mining". Once users obtain bitcoins they can check their balance and spend them via their digital wallet. This activity all takes place online, but works like paying cash for goods; i.e. it does not involve any intermediaries. The wallet contains the private key of the user which is a secret piece of data proving their right to spend bitcoins from this specific wallet.

Transactions

When a user sends bitcoins to someone, a transaction is created. In this process, the new owner's public key (their digital identity) is attached to the bitcoins sent, and confirmed by the signature of the sending party (using their private key). All transactions are transmitted via the network. The complete history of transactions is accessible to everyone who has access to the Bitcoin network, therefore any user can see the digitally encrypted identity of the owner of a given bitcoin. Bitcoins are divisible, so amounts less than one bitcoin can be used, and checked. The smallest amount in the system is 1 Satoshi – equal to one hundred-millionth of one bitcoin.

Confirmation

All new transactions are grouped in a "block", with each of these recorded in the "blockchain" containing all blocks. A transaction is only confirmed to have occurred when it is included in a block of current transactions. Confirmation means that the network has processed the transaction and that it is highly unlikely to be reversed. About every ten minutes, on average, a new block of transactions is added to the blockchain. Each subsequent block added to the blockchain also reconfirms the validity of previous blocks (prior groups of transactions), going all the way back to the first ever block from 2009. The main website for Bitcoin's core developers and communities says that a single confirmation can be considered secure for low-level transactions, but recommends waiting for at least six confirmations for amounts larger than US$1 000, as the risk of a reversed transaction decreases significantly with each confirmation. This somewhat complicated process means the system works without any independent party to verify transactions.

Mining

Blocks are connected to the blockchain through a process called mining. In order to maintain the integrity of the blockchain, each block in the chain confirms the integrity of previous ones. Each block must satisfy certain requirements (complicated mathematical algorithms need to be solved) to become attached. This computationally expensive operation demands substantial computer power and has significant costs in terms of electricity and cost of equipment. If a miner's computers solve the complex mathematical puzzle before anyone else, they get a payment of 25 bitcoins. Consequently, the blockchain is updated, and everyone in the network is notified of this. To encourage mining, users are also allocated fees based on the value of transactions verified.

Over time, fewer bitcoins will be provided as a reward for mining, while the complexity of verifying a block will increase. The mining process is becoming progressively more and more complicated and resource-demanding, because the data chunks to be processed become larger. It used to be quite simple to mine, while the reward was 50 bitcoins. Today, the reward for attaching a block to a blockchain has been reduced to 25 bitcoins. Since the supply of bitcoins is fixed, the block reward is programmed to halve every four years, and eventually only the fees will be paid to successful miners.

Some rough estimates indicate that users spend significantly more money on electricity and equipment than the bitcoins they are trying to obtain are worth (figures from 11 December 2013 showed US$17 million were spent for rewards of just $4.4 million). In order to control the number of bitcoins emitted, the design of the system means it becomes progressively more difficult to mine new bitcoins. It is economically not very profitable to mine taking into account the costs of electricity and hardware (which can cost thousands of dollars). For this reason, users often pool their computers together to increase the computational power and share the rewards. Nobody has yet pooled enough computers to control more than 50% of the entire network. If this happens however, there is a risk that the integrity of the whole system will be compromised as this would allow transactions to be reversed and false confirmations to be sent. The environmental footprint is criticised by many, but Bitcoin's community suggests that redeployment of the energy spent on mining is possible.

Emission of bitcoins

Bitcoins are created each time a user confirms a new block. The rate of block creation is approximately six per hour. The number of bitcoins generated per block is programmed to decrease geometrically, with a 50% reduction every four years. This algorithm was applied because it resembles the rate at which real commodities like gold are mined. A predefined schedule limits the total number of bitcoins to be emitted to 21 million (without taking into account those lost through deleted or misplaced wallets). This limit is encoded in the protocol and cannot be exceeded. The total number of bitcoins in circulation as of 24 March 2014 is 12 590 575. It has risen from 8 695 500 over the past two years. Some estimate that the last bitcoins will be emitted as soon as 2030, but the mainstream view is that 21 million is programmed to be reached only in 2140.

Why is Bitcoin successful? Advantages of using Bitcoin

Lower transaction fees

Bitcoin offers three main advantages to its users. The first is lower transaction costs, as there is no third-party intermediary charging users. To date there is no comprehensive research on the actual size of Bitcoin's transaction cost advantage. Some however state that the average transaction fees are between 0 and 1 percent. Taking into account that traditional online payment systems charge fees of 2 to 3 per cent per transaction, it is likely that Bitcoin is cheaper to use even when swapping it for conventional fiat money, which has a fee of about 1 per cent. These benefits may however be offset by Bitcoin's high volatility (see below).

Anonymity

The second advantage is greater anonymity for users. Their identity is encrypted but a full record of every user and every bitcoin is preserved on the publicly available ledger. Therefore, some consider the Bitcoin system to be "pseudonymous" rather than fully anonymous, and suggest that there are possibilities to trace users' real identities.

Controlled inflation

Thirdly, inflation does not seem to be affecting the purchasing power of bitcoins as the release schedule is pre-programmed and predictable. Again, this could however be offset by the price volatility of this cryptocurrency.

Apart from this, Bitcoin is characterised by simplicity in use: users do not need a bank account or credit card to use it – an internet connection is sufficient for its use worldwide.

Main disadvantages of Bitcoin

Volatility

Bitcoin's price has been subject to high volatility since its creation, with 2013 bringing record high appreciations and precipitous depreciations in value (see Annex A). For example, it rose more than 20 times in value between September and December 2013, but then lost about 60% of its value over the next three months. Almost half of bitcoins are owned by less than 1 000 people (47 own almost one-third). Some say that this may create a cartel-like effect on pricing, especially when there is a shortage of bitcoins on the market. Media coverage and regulatory stances, speculation on exchanges, hacking and shutting down of exchange platforms, one-off events such as closure of banks in Cyprus (and apparent loss of trust in traditional fiat currency) have all had significant effects on the price of bitcoins. The volatility of Bitcoin is likely to discourage many potential buyers. Falling prices may deter selling by hoarders of bitcoins who expect higher returns in the future, or it may cause them to panic and sell. In fact, there seems to be consensus among observers that the recent instability in prices is one of the main hurdles to the wider use of Bitcoin as a medium of exchange. Its adoption for day-to-day use is directly related to price stability, needed by consumers and businesses for planning their consumption and savings decisions.

Security threats

Even though counterfeiting bitcoins is supposedly not feasible as they all have a unique identity, many problems have been reported concerning other aspects of the currency, such as security of the exchange platforms and wallets. Cybercrime is on the rise with bitcoins also attracting more attention, while there have also been problems signalled with Bitcoin-based Ponzi schemes. Bitcoin's main security focus is on preventing the same unit being spent twice, whereas it cannot validate whether the true owner of a key signed the transaction. Empirical research on Bitcoin exchanges showed that the less popular ones are more likely to suffer a security breach and be closed due to theft of bitcoins. Fundamentally, since Bitcoin is outside the banking system and not backed by any central body, in most cases users cannot recover any of their losses since they are not covered by deposit insurance.

Mt. Gox exchange platform

Mt. Gox started as an exchange platform for a fantasy game and became a main Bitcoin-to-money exchange system in 2010. In 2011 Mt. Gox was hacked, and over 60 000 usernames and passwords were stolen. Mt. Gox was forced to go offline and trading was halted for seven days. That resulted in a crash from $17.51 down to $0.01 per bitcoin on the Mt. Gox exchange (bitcoins have different values on different exchanges). In February 2014 Mt. Gox was hacked again, resulting in $500 million losses. The company filed for bankruptcy in Japan in February 2014 and the CEO has been called to appear in a US Court on 17 April 2014.

Immaturity and risks

Bitcoin is a currency in a nascent stage which has various risks involved. Firstly, it is not yet widely accepted as a payment method by merchants. In fact, current uses of Bitcoin are mostly speculative in nature (keeping bitcoins in the hope of price increases), as in the retail and commercial sectors it remains a niche phenomenon. And as speculation fuels volatility, the commercial world is ever more reluctant to accept Bitcoin widely. Furthermore, Bitcoin's security and operational robustness may be exposed to unforeseen challenges in the future as Bitcoin matures and handles larger transaction volumes. An unforeseen flaw might have a detrimental effect on the whole system.

Finally, Bitcoin may become less popular than another cryptocurrency which may come onto the market, even though some claim that Bitcoin has first-mover advantage. Being first on the market creates some barriers to entry for others, as consumers have less incentive to experiment with alternative digital currencies if Bitcoin works well. From traders' point of view, mainly due to its immaturity, a significant sell-off of bitcoins (possibly after a "pump and dump" scheme) may cause panic selling by holders and a "domino effect" which could erode its value.

Lack of supply elasticity

Bitcoin emission is capped, which means it has an inherent deflationary bias. On average, the supply of Bitcoins will increase by 0.6 per cent a year. If the Bitcoin economy expands faster than this, the currency will become scarce and the price of bitcoins will rise. At the same time, the price of goods expressed in bitcoins will fall, causing a deflationary effect. Furthermore, the pace of issue of bitcoins will most likely be slower than that of physical currencies, which is likely to lead to its exchange rate increasing significantly (this theory can be tempered by looking at the reality of volumes in current use). This lack of supply elasticity makes Bitcoin's issuance independent of general economic activity and its possible wider acceptance as a means of payment (and therefore of increased demand). This may encourage its use as a speculative instrument – in view of its expected future rise in value – rather than as a means of payment.

Money laundering & tax fraud issues

Research on money laundering and tax fraud via Bitcoin is limited due to difficulties in obtaining data. One landmark paper suggests that Bitcoin (and other cryptocurrencies) is reasonably likely to replace tax havens as a choice for tax evaders. As earnings are not subject to taxation, the identity of traders remains anonymous, no bank account is needed and there are no third parties with reporting obligations involved, Bitcoin has high potential for tax evasion. For the same reasons some researchers believe that Bitcoin use will be maintained by hackers, online gamblers, drug dealers, smugglers, and anarchists, since the features of the system make it a very practical tool to purchase illegal items or support illegitimate activities. However, the scale of tax evasion at present is not likely to be very high, as the number of bitcoins available is simply not large enough and its volatility in value too high.

Silk Road

This online market started operating in January 2011. It was a website through which people could buy weapons and drugs such as cocaine and heroin using bitcoins for payment. It had 60 000 visitors per day. The website was shut down in October 2013 by the FBI who confiscated bitcoins worth $28.5 million at the going rate. The alleged creator of the website pleaded not guilty to the charges.

The European Banking Authority, European Central Bank and the FBI have all recognised that Bitcoin may be used for money-laundering purposes. The potential comes mainly from the anonymity and lack of regulation. Money laundering may for example take place by converting illegal gains to bitcoins, spreading them through several wallets and then using several services to receive other legitimate bitcoins for a commission. Technically proficient criminals may take additional steps to cover their traces and some security experts argue that international drug cartels have indeed migrated online to launder their illegal profits. The US introduced anti-money-laundering guidelines applicable to Bitcoin in 2013, and the first arrest of a prominent Bitcoin figure on money laundering charges occurred there in January 2014. On the other hand, some analysts state that laundering money through Bitcoin is more of a

theoretical possibility than an actual one. They argue that the small number of Bitcoin exchanges (which allegedly started offering aid to relevant investigating agencies in 2011) and the public nature of the Bitcoin ledger make the currency currently unattractive for high-volume money laundering activities.

Regulating Bitcoin

The EU has not adopted any specific regulation on Bitcoin. A 2012 report of the European Central Bank states that Bitcoin falls outside the scope of both the Electronic Money Directive and the Payment Services Directive. The report notes that cryptocurrencies may pose challenges to authorities "given their legal uncertainty ... as they can be used by criminals, fraudsters and money launderers". Observers noted in March 2014 the first attempt to put Bitcoin on the European agenda. Risk experts suggest that rather than specific legislation, adapting the existing payment and electronic money framework and anti-money laundering laws will be sufficient. Others argue that the multitude of approaches at Member State level may mean that harmonization at EU level will be needed.

A January 2014 survey of 40 jurisdictions pointed out that very few countries have Bitcoin-specific regulations and that the debate on how to deal with it is still in its infancy. It also reported widespread concern about the potential impact of Bitcoin on national currencies, taxation, and its potential for criminal misuse. The main issue with regulating Bitcoin seems to be that it is considered neither to be legal tender nor a security or similar financial instrument but a "hybrid product". Financial analysts argue that Bitcoin has both currency and commodity features. Ambiguity about its status is reflected in recent developments: Japan decided to treat Bitcoin as a commodity, guidelines from US authorities describe Bitcoin as property, but in Germany it is recognised as private money. There is a consensus among commentators that as Bitcoin gains in prominence it will become more regulated. Currently, the most restrictive approach is in countries with strong capital controls (such as China). Authorities in the few other countries pioneering regulation have focused mostly on taxing Bitcoin trade and preventing its use for money laundering or involvement in illicit activities (see Annex B), giving a nascent industry time to grow and possibly create public benefits. Recently Japan called for international regulation of Bitcoin to avoid exploitation of loopholes. The least developed field of regulation seems to be that of consumer protection. One of the rare instances, the US guidelines, makes losses on Bitcoin trading tax deductible.

Institutional views

In December 2013, the European Banking Authority warned consumers about the lack of regulatory protection when using cryptocurrencies and the risk of losing their money. It also added that there is no guarantee of stability in such currencies' value. Recently the ECB confirmed that cryptocurrencies are not yet economically important but pose risks to users, in particular in the areas of speculative investment and consumer protection. Similar warning messages have been voiced by a number of other central banks (e.g. Germany, France, Netherlands, India).

Some Members of the European Parliament have asked the Commission to investigate Bitcoin further. In a motion for resolution on Bitcoin, Sergio Silvestris (EPP, Italy) asked the Commission to assess Bitcoin's positive and negative sides.

The US Senate hearing on Bitcoin held in November 2013 recognised that it has legitimate uses. The House Small Business Committee stated that Bitcoin could help small businesses cut costs and reduce their prices, but it also presents a number of risks.

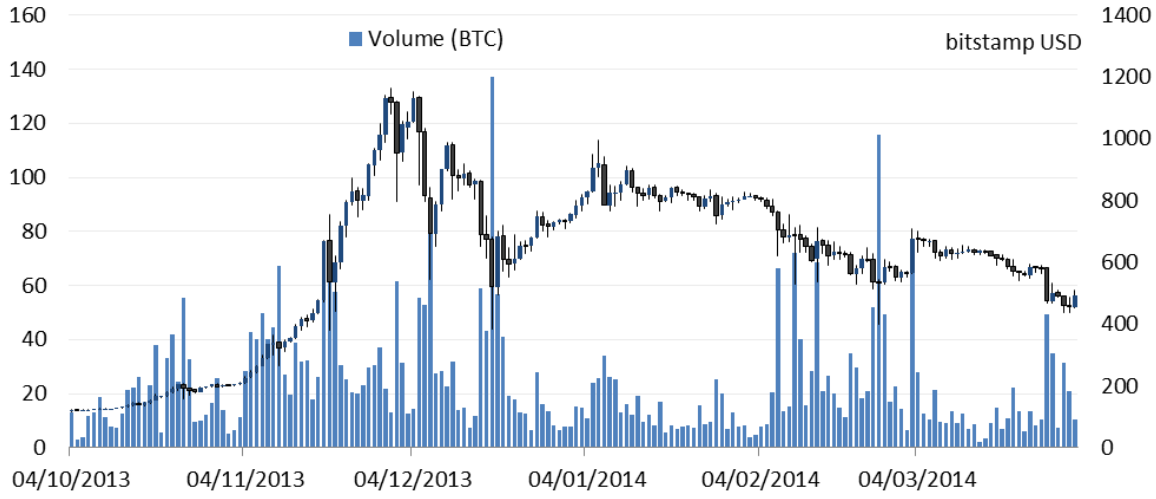
Future prospects

Despite being a technological novelty, Bitcoin's future as a currency remains far from certain. The inevitable increase in regulation and increased compliance requirements will raise Bitcoin's transaction costs and reduce the anonymity of its users, which are two of its strengths. Some from the industry criticise the increased regulation as impossible to enforce and likely to hamper innovation, while entrepreneurs welcome regulation as it should increase consumer protection and possibly bring participation of the banks. The lack of acceptance by the financial system and lack of protection are indeed quoted by some analysts as major obstacles to gaining trust and wider acceptance in society. It remains to be seen whether global financial institutions acting in their own interest will try to impact on future policies on Bitcoin as well as create competitive virtual currencies. Many see the volatility of Bitcoin as an obstacle for it to becoming a corporate investment. However, Bank of America Merrill Lynch considers this volatility temporary due to the highly speculative nature of the market and believes Bitcoin can become a serious competitor to traditional money-transfer providers. They also argue that the current system may not be able to handle the possible increase of transactions – higher value ones may be subject to fraud if they need to be verified six times as at present. This is an issue when the two parties to a transaction are anonymous, and will inevitably increase with the network's growth.

One of the main arguments against Bitcoin's future as a currency is that the deflationary character of Bitcoin may create strong incentive to hoard bitcoins rather than to circulate them, further limiting the amount available for trade rather than investment. The Bitcoin community confirms that bitcoins deflate in value when the Bitcoin economy is growing. It is also most likely that the vast majority of users are already keeping bitcoins for price speculation. Some economists argue that slow, predictable deflation will not be destructive to Bitcoin, but even Bitcoin proponents revert to the possibility of changing the system's code to allow for higher supply. Some analysts believe that Bitcoin's real impact is the innovation in payments technology it has brought about, which will eventually force the existing players to adapt to it or co-opt it. Established investors underline the fact that Bitcoin has no intrinsic value.

EPRS European Parliamentary Research Service
http://www.eprs.ep.parl.union.eu
http://epthinktank.eu
eprs@ep.europa.eu

Annex A: Bitcoin prices (in US$ - left-hand scale) and trading volumes (in thousands - right-hand scale)



Source: bitcoincharts.com, 2014

Annex B: Bitcoin regulation or plans therefor in selected countries

Scope / content	Country	Additional information
Prohibition	China	Banks and payment systems prohibited from dealing in bitcoins. Individuals free to trade.
	Russia	Bitcoins cannot be used by citizens and legal entities.
	Iceland	Foreign exchange activities with Bitcoin illegal.
Prohibition of ATMs	Taiwan	Approval for Bitcoin ATMs refused.
Protection from money laundering & illicit activities financing	Singapore	Financial intermediaries to verify the identities of their customers and report suspicious transactions.
	USA	Bitcoin exchanges and most miners obliged to collect information on potentially suspicious transactions and report these to the federal government
Taxing Bitcoin		The sale, exchange or use of Bitcoin for payment in a real-world economy transaction may result in tax liability.
	Japan	The tax will cover gains from trading bitcoins, purchases made with bitcoins and revenues from transactions. Banks and securities firms will be prohibited from Bitcoin trades.
	Finland	Rules on taxation of capital gains apply when profits are made from transfer to another currency. Increase in value in Bitcoin after it was obtained as payment is also taxable.
	Germany	Profits from mining or trading subject to capital gains tax unless hoarded for at least one year