What is Bitcoin?

Björn Segendorf*

Björn Segendorf holds a Ph.D. in economics and works at the Riksbank's Financial Stability Department.

Bitcoin is a so-called virtual currency that has been devised for anonymous payments made entirely independently of governments and banks. In recent years, Bitcoin has generated a great deal of attention on several fronts. Bitcoin payments are based on a new interesting technical solution and function differently to traditional payments. In certain payment situations, Bitcoin can bring advantages in the form of lower costs, rapidity, anonymity, etc. over traditional payment methods. However, usage can also be more risky because Bitcoin is not directly covered by the laws that govern other payment mediation. Weak consumer protection is also a reason for why it may be difficult for Bitcoin to become generally accepted and viable as a means of payment. Use of Bitcoin for payments is low today, and although Bitcoin's future is uncertain, it is an interesting innovation worthy of description. This article explains what a virtual currency is, and how Bitcoin works. Bitcoin use in Sweden – which is very limited – is also described. Finally, the future of Bitcoin and other virtual currencies is discussed.

Responding to new needs?

Many areas have undergone rapid technological progress in recent years. Our needs in terms of making payments are also undergoing transformation. For instance, households are shopping online to a growing extent, and the amount of cross-border payments is on the rise. Payment solutions, especially for person-to-person payments, have however not evolved as quickly. Bitcoin can be seen as a response to the lack of such payment solutions and has often been a topic of discussion in the media, at workplaces and among friends in recent years. Various factors have evoked curiosity about how the currency works, such as the supposed anonymity for users, the fact that banks are not involved in the payments and the ability to make payments worldwide. At the same time, it is difficult to understand what Bitcoin really is, and how it works. I attempt to elucidate this in this article.

I start by explaining what a virtual currency is, the different types of virtual currency that exist, and where Bitcoin fits into that categorisation. I then go on to describe how Bitcoin works and what we know about its use in Sweden. Finally, I discuss Bitcoin's benefits and risks, and the difficulties it may face in future.

* I would like to thank those who have contributed their valuable input. While they are too many to mention, I would like to extend particular thanks to Malin Alpen, Susanna Grufman, Marianne Sterner, Claes Berg and Kristian Jönsson.

Virtual currency

Bitcoin is what is known as a virtual currency.[1] A virtual currency is a means of payment; that is, units of the virtual currency represent a value. It is intended for use in payments within a specific virtual community, such as a particular website, or in a network of users with special software for managing the virtual currency and making payments. This type of virtual community can thus be said to resemble a voluntary agreement to use a specific item as a means of payment. This is an important difference to national currencies, such as the Swedish krona. For the latter, it has been established in law that the monetary unit in Sweden shall be called the Swedish krona. The virtual currency thus has a different unit of account than national currencies. For Bitcoin, the unit of account is the Bitcoin itself.

The issuer of the virtual currency can be a non-financial company or even a private individual, but such an issuer is not under the supervision of a government authority. The issuance of virtual currency is thus not a government-regulated activity.[2] However, each virtual currency has some type of rules of its own governing where and how it may be used, and some form of technical infrastructure in which the payments are carried out. The virtual currency, the own set of rules and the technical infrastructure combined form a small payment system, hereinafter referred to as a virtual currency scheme.

There are a large number of virtual currency schemes that have been built up, and function, in different ways. They can be broken down into different categories depending on the extent to which it is possible to buy and sell the virtual currency. Here, we divide them into virtual currency schemes that are closed, with unidirectional flow and bidirectional flows. In closed virtual currency schemes, the virtual currency can be neither bought nor sold, but only earned and used on certain websites (such as World-of-Warcraft Gold). If the virtual currency can be bought for national currency but not exchanged back, the scheme has a unidirectional flow (such as Amazon coins). When the virtual currency can both be bought and sold and used outside of a certain website, the scheme has bidirectional flows. As explained below, Bitcoin is an example of a scheme with bidirectional flows. However, these categories can overlap.[3]

A further distinction that can be made is whether the virtual currency is centralised or decentralised. As with banknotes and coins, payments with virtual currency units are made by means of them changing ownership. The ownership structure must therefore be registered somewhere, otherwise it might be tempting for a virtual currency unit holder to duplicate it and use it multiple times. A centralised virtual currency scheme has a centralised

[1] The term “virtual currency” is used by the ECB (2012) and we use their terminology. Other terms are sometimes used in other articles, such as digital currency. However, it is doubtful as to whether Bitcoin is a currency in the proper sense, see Yermack (2014).

[2] The issuance of virtual currency must be distinguished from offering different forms of payment service in virtual currency. The providers of financial services, such as exchanges, in virtual currency are subject to anti-money laundering regulation. Regarding payment services, the main regulation in Sweden is the Payment Services Act (2010:751) which sets out the rights and obligations of both mediators of payments and users of payment services. It applies to payment services in Euro or other EES-currencies but could in principle be extended to other currencies, including virtual currencies.

[3] See Segendorf (2014) for a more detailed description of the various categories.

system for verifying and executing transactions, often with the issuer. In practice, the latter administrates all of the accounts through which the payments are made. In a decentralised virtual currency scheme, like Bitcoin, the transactions are instead verified and executed via the network of users that carry out some form of activity to this end. The right to register events is thus delegated to the network's participants.[4] The decentralised virtual currency schemes are not uncommonly based on an exchange of encrypted messages and are therefore usually called cryptocurrencies. The anonymity and security that this provides are the fundamental concepts on which Bitcoin rests.

How Bitcoin works

Bitcoin is a decentralised virtual currency scheme with bidirectional flow, and a cryptocurrency.[5] It was devised to be independent of governments, banks and other institutions. At an overarching level, Bitcoin works rather like a type of electronic cash. Bitcoins can be purchased on special websites, both abroad and in Sweden, where they are exchanged for national currency.[6] [7] The exchange rate for Bitcoin is determined by the market as a function of supply and demand.

Bitcoin payments can be made between anybody with the requisite software on their computer, smartphone or tablet. This software is called a *wallet.* Yet, Bitcoin should not be considered to be a type of digital cash. The reason is that Bitcoins are not digital units of value stored on e.g. a computer. A Bitcoin is thus not a digital note or coin and should not be compared to regular notes and coins. Rather, Bitcoin should be viewed as funds in an account. When a payment is made, the payer thus does not send digital notes and coins to the recipient; rather, the payment occurs by means of debiting the sender's account and crediting the recipient's account. Payments are made by means of exchanging encrypted messages and are verified within the user network. I describe this process below.

[4] Also, traditional retail payments can be divided up into centralised and decentralised systems. Cash is a decentralised system. It suffices for the paying and receiving parties to agree on the validity of the payment for its acceptance. Other retail payments such as credit transfers, direct debits, cards and cheques are centralised in that they are centrally cleared and the payments are settled at a settlement institution, commonly the central bank. See Sveriges Riksbank (2013) for an account of clearing and settlement of retail payments.

[5] Bitcoin was launched in 2009 by Satoshi Nakamoto, which is possibly a pseudonym. Until 6 March 2014, when Newsweek claimed that it had found the real Satoshi Nakamoto, there was a general conviction that the true founder, or group of founders, was unknown. The identified man has denied that he is the true Satoshi Nakamoto. It is currently uncertain whether or not it was the true Satoshi Nakamoto who was found. Source: http://mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html and http://www.coindesk.com/one-simply-find-satoshi-nakamoto/

[6] Different exchange sites offer slightly different services. Some only exchange, while others can offer accounts. There are also websites that match buyers and sellers geographically. In Sweden and most other countries, companies that offer exchange services are regulated and come under supervision.

[7] The largest international exchange site by far has long been Mt.Gox. At the end of February 2014, a major theft/fraud was uncovered, whereupon Mt.Gox became insolvent and was declared bankrupt.

ASYMMETRICAL ENCRYPTION GIVES SAFE PAYMENTS

I start by explaining the concept "asymmetrical encryption" and how the sender (person A) and the recipient (person B) of encrypted messages can be securely identified. Asymmetrical encryption is based on A and B having two encryption keys each. The encryption keys are unique and nobody can have the same keys as anybody else. One of the keys is public; in other words it is or could be made publicly known. The other is private, or secret in other words. When A wishes to send an encrypted message to B, he uses B's public key to encrypt the message which can then only be de-encrypted using B's private key. So, B is the only person who can read the message.

Asymmetrical encryption can also be used for signing. If A uses his private key to encrypt a message, this can only be de-encrypted using A's public key. The person de-encrypting the message can then be sure that it was sent by A – nobody else has access to A's private key. This is comparable with A having signed the message.

Assume that A is to pay 1 Bitcoin (BTC) to B. A and B both have their wallets on their computers, and each such wallet has a private and a public encryption key. A wallet is associated with its public encryption key, which serves as an address or an account number. A and B communicate through their wallets.

THE TRANSACTION IS VERIFIED BY THE NETWORK

The transaction commences by B sending his public encryption key (account number) to A. A, or more precisely A's wallet, now writes a payment order for 1 BTC to B and signs it with A's private key. The payment order is issued to the network of Bitcoin users. One could say that the transaction between A's and B's wallets is proposed to the network, which now has to confirm/verify the transaction for it to become valid. The method used to send the message to the network is based on technology similar to file sharing (BitTorrent), which is common for spreading/sharing films, music, etc. online.

The verification process is as follows: Every tenth minute, a certain type of participant in the Bitcoin network gathers the transactions proposed in the last ten-minute period. This occurs automatically, and the round of gathered transactions is called a "block" and the special participants are called "miners".[8] They have the task of verifying the transaction by adding the new block (the transactions) to what is known as the blockchain, which is the official list or register of verified Bitcoin transactions. Because the blockchain contains information about sending wallets, receiving wallets and amounts, it can be used to verify how many BTC belong to a specific wallet. It is the same as being able to calculate the balance of a normal bank account if one has access to all the incoming and outgoing transactions of that account. A wallet can therefore be viewed as an account, for which the public key serves as an account number for the wallet. A Bitcoin transaction is not

[8] Anybody can become a miner; it's the choice of the individual. They are called miners because their activity has been likened to gold digging, because they are rewarded with new Bitcoins. It is an ill-fitting comparison, however, because Bitcoin, unlike gold, has no intrinsic value. For gold, this value comes from the ability to use it for jewellery, in industrial processes, etc.

completely anonymous. Because it is added to the blockchain, it is registered and readily available online. It is thus fairly simple to identify the wallets between which a transaction has been made. However, it is very difficult to link wallets to individual users, which means that the transaction is in practice anonymous.

The payments are verified by means of miners solving a mathematical problem for which the solution is difficult to calculate, but easy to verify once calculated. In order to better understand the verification, the concept "hash function" must be explained. A hash function is a function that converts an arbitrary-length number or text into a given-length number.[9] For example, the individual figures in a number can be added together and if the sum exceeds a one-digit number, the components of the sum are added together, and so on. The number 678910 is thus 6+7+8+9+1+0=31, and 31 is 3+1=4. Hence, the multi-digit number has been converted into a single-digit number. Let x denote the original blockchain, y the transactions to be verified and z a different number. The mathematical problem to be resolved can be formulated as $f(x,y,z)\leq v$ where f is a hash function and it is a case of finding a number z so that the hash function assumes a lower value than v where v can in this case be interpreted as the degree of difficulty of the hash function.

Miners compete with each other over who can find a solution fastest. When a miner has found a solution, the proposed solution is sent out in the network, in which other miners can simply verify whether or not the solution is correct. A decision to accept a solution is taken by majority decision, in which the voting strength of a miner depends on the extent of calculation capacity, or computing power, he brings to the network. When a solution is supported by miners who represent a majority of the network's computing power, the solution is considered to be accepted. The proposed transactions are now added to the blockchain, which becomes one block longer. Now that the transaction between A and B has been accepted, B is the owner of the transferred 1 BTC with which his wallet was credited. At the same time, 1 BTC has been debited from A's wallet.

MINERS GET NEW BITCOINS FOR THEIR EFFORTS

The incentive for miners to invest computing power in the verification process is that, as compensation, they may create new Bitcoins. The process is as follows: the miner that resolved the hash function quickest, in other words who first computed z, as a reward also adds an extra "transaction" to the block to be verified (y). This transaction credits the miner's wallet with N amount of BTC without anybody else's wallet being debited. In order words, N amount of new Bitcoins is created with the winning miner as the owner. Every other week, the set of rules (the protocol)[10] governing Bitcoin adjusts the degree of difficulty v of the hash function and the amount of Bitcoins (N) created in each verification. The adjustment is to ensure that the network can verify transactions once every ten

[9] The specific hash function used in the Bitcoin protocol is SHA-256. For more information about this function, see http://en.wikipedia.org/wiki/Sha-256.

[10] A protocol is a set of rules that helps the computers concerned to communicate online. Nobody owns a protocol; rather, it is created to be a usable standard.

minutes. If computing power in the network increases, so will the degree of difficulty, and vice versa. The amount of Bitcoins created decreases over time through N being halved after 210,000 blocks, which equates to around 4 years. The initial amount was $N=50$ and now it is $N=25$. Because N decreases over time, there is an upper limit of 21 million on the number of Bitcoins that can exist. This limit can be seen as a mathematical threshold that is never reached, even if the amount of BTC can get arbitrarily close. At 30 June 2014, there were around 13 million BTC.

Because of this way of creating new Bitcoins, there is, unlike for national currencies issued by central banks, no central Bitcoin issuer – the creation of new Bitcoins being governed by its protocol. Hence, neither is Bitcoin a monetary claim on another party. Swedish notes and coins are formally a claim on the Riksbank and bank balances are a claim on the bank, backed by its balance sheet. The value of a Bitcoin is thus not based on any type of claim or underlying asset. Rather, its market value depends entirely on an expectation that it can be used in future transactions.

PAYMENTS ARE NOT IN REAL TIME

A Bitcoin payment is not a real-time payment. It can take up to ten minutes for a payment to be verified, and the general rule is that one should wait six verification rounds to be sure that the payment was actually added to the blockchain.[11] Obtaining verification for a Bitcoin payment can thus take up to around an hour. Depending on the situation, this can be perceived as a long or short space of time. It is also worth noting that, due to the file sharing technology and the verification process, there is no central storage location for the blockchain. Each network participant has information about all or parts of the blockchain.

[11] The recommendation comes from Bitcoin.se. The underlying reason for why waiting a couple of verification rounds is recommended is a consequence of the decentralised verification process. Expressed simply, different versions of the blockchain can occur. In such cases, the longest blockchain is considered to be the proper one. The transaction that was just verified is registered in the final block of the blockchain. Should duplicate versions occur, there is hence a risk of the other version of the blockchain being selected as the proper one by the network, and hence of the final block being different. If the transaction is no longer included in the blockchain, it is not verified either. It is therefore wise to wait a couple of verification rounds to eliminate the risk of the blockchain changing.

Box 1. Electronic money is not virtual currency

The concept "electronic money" should not be confused with virtual currency. Electronic money is an electronically stored money value that represents a claim on the issuer, has a value that equals no more than the amount for which it was purchased, and which is accepted by parties other than the issuer.[12] By the latter, it is meant that the e-money must be accepted by a sufficiently broad circle of companies. Bitcoins are thus not electronic money, one reason being because they do not represent a claim on the issuer.

In general, a virtual currency can fulfil a couple of the above criteria, but not all. For example, most virtual currencies do not fulfil the requirement of a sufficiently broad circle of recipients. Neither is it always possible to exchange the virtual currency for national currency. Virtual currencies are also specified in other units of account than national ones. This is an important difference to electronic money. Redemption need not take place on a one-to-one basis because the units of value differ. In a potential redemption or exchange for national currency, the value cannot usually be predicted because the exchange rate fluctuates. Control of the regulations governing the virtual currency rests with the issuer. There is no supervision of the currency and the issuer is usually a non-financial company. Payments via virtual currency schemes are hence not covered by the Electronic Money Act (2011:755) or the Payment Services Act (2010:751). In addition, the issuer is not usually located in Sweden.

THE EXTENT OF BITCOIN USAGE

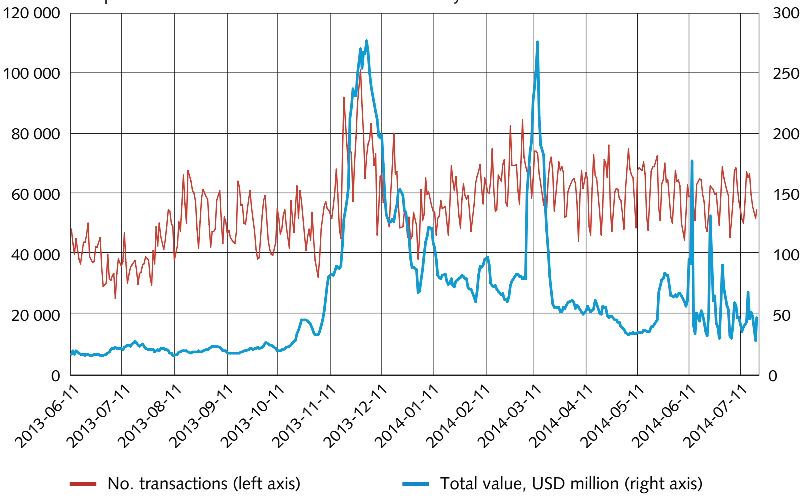
There are statistics about all transactions made using Bitcoin from 2009 onwards. These statistics come from the blockchain and are basically available to everybody. Some analyses are available online and provide an overview of global Bitcoin usage. However, it is not possible to see the extent of usage in a certain country because the wallet holders between which transactions were made can typically not be identified.

Bitcoin usage is low globally

In the past year, almost 60,000 Bitcoin transactions per day have been made. At the lowest, there were 28,000 per day, and just over 100,000 at most. This equates to around 0.1 per thousand of the number of card payments. The total value, measured in USD million, has also varied sharply – partly due to major fluctuations in the exchange rate. On average, the total value was no more than around USD 64 million per day. Diagram 1 shows the number of transactions per day and the total mediated value.

[12] See Sveriges Riksbank (2013) for a description of the law.

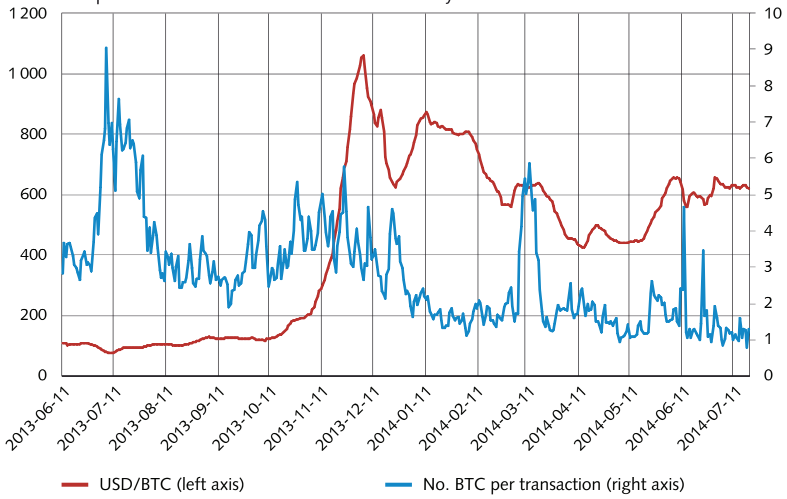
Diagram 1. Number of Bitcoin transactions and mediated value (USD million) per day
The period extends from 11 June 2013 to 21 July 2014



Source: blockchain.info. Revision by the Riksbank.

The average transaction value, measured in BTC, has dropped somewhat over time, probably because the exchange rate appreciated sharply in the autumn of 2013. Diagram 2 shows the exchange rate and the number of Bitcoins per transaction. The increase in the mediated value in the autumn of 2013 is often explained by increased demand for Bitcoin from China.

Diagram 2. Exchange rate USD/BTC and the average number of BTC per transaction
The period extends from 11 June 2013 to 21 July 2014



Source: Blockchain.info. Revision by the Riksbank.

Only 4 per cent of all Bitcoins are traded within a week by their holders. If the time interval is extended to three months, a further 24 per cent is traded. Only after six months have more than half been traded. Around 38 per cent are kept for over a year.[13] Bitcoin holders thus do not apparently trade them particularly often. It should also be mentioned in this context that many miners, especially major participants or those that cooperate in pools, often exchange their earned Bitcoins into national currency immediately to cover their overheads. The fact that only a small proportion of all Bitcoins seems to be used for transactions suggests that most of them are held for more long-term purposes, such as currency exchange speculation or saving.

BITCOIN USAGE IN SWEDEN IS EVEN LOWER

A rough estimate indicates that, in mid-August 2014, there were around thirty companies/websites accepting Bitcoin in Sweden.[14] It is mainly a matter of small companies and Bitcoin does not seem to have any broad acceptance as a commercial means of payment. It is therefore probable that a large proportion of the Bitcoin transactions in which the sender or recipient is located in Sweden takes place between private individuals or to payees abroad.

Bitcoin transactions are anonymous and it is not possible to obtain statistics for payments in which one of the parties is in Sweden. However, there is some data on the amount and value of exchange transactions between BTC and SEK.[15] The table below shows aggregate information regarding exchange traffic for the period 15 December 2012 to 31 May 2014. An average of SEK 266,000 was exchanged daily. The high volatility in the exchange transactions is illustrated in Diagram 3. The total value of the exchange transactions between BTC and SEK appears to amount to a couple of per cent of the corresponding value for exchange between BTC and EUR and less than 1 per cent of the exchange value between BTC and USD. The SEK is thus a minor currency in a Bitcoin context. It is also apparent that exchanging between BTC and SEK is a minor market when comparing it with the SEK 25 billion exchanged on average on the spot market to and from USD.[16]

Table 1. Daily values for exchanging between Bitcoin and SEK

	VOLUME (BC)	EX. RATE (SEK)	TURNOVER (SEK)
Mean	212	1 995	265 501
Min	7	89	2 536
Max	1 065	7 720	2 574 066
Std. dev	184	1 916	312 520

Sources: http://bitcoincharts.com, Safello and BTCX. Revision: The Riksbank.

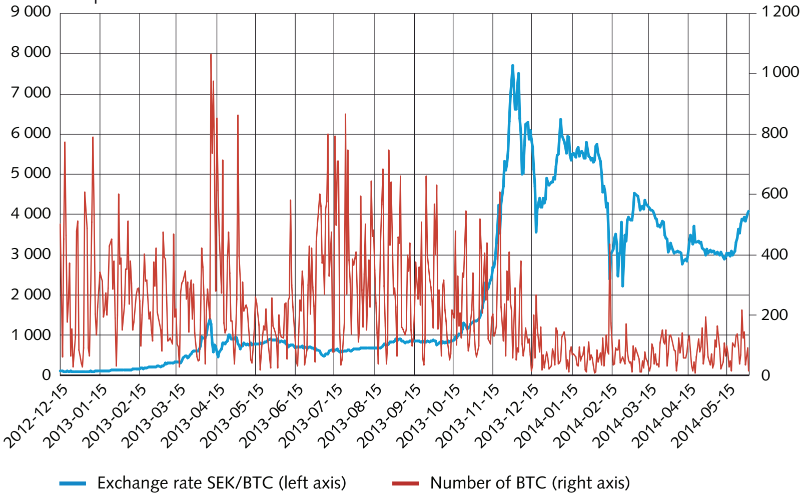
[13] Source: Swanson (2014).

[14] Source: bitcoin.se

[15] These statistics do not capture exchange by private individuals and companies in Sweden to e.g. USD. The extent of exchange by Swedish participants into other currencies is unknown. For example, according to Dagens Industri (2014), KNC Miner earns SEK 3 million per day by mining Bitcoin. But, they always exchange it to USD.

[16] Refers to the average for June 2014. Source: http://www.riksbank.se/Documents/Statistik/Turnover/2014/stat_omsFX_1406_sve.xls

Diagram 3. Daily values for exchange between BTC and SEK
The period extends from 15/12/2012 to 31/05/2014



Sources: http://bitcoincharts.com, Safello and BTCX. Revision: The Riksbank.

It is uncertain how well the exchange transactions reflect Bitcoin payment traffic. If Bitcoin is reused for payment without it being converted into SEK in the process, Bitcoin use for payment purposes is underestimated. However, if Bitcoin is bought and held for the purpose of speculation, it is overestimated. If the usage of Swedish holders resembles global use, the lion's share of the holding should be for saving or speculation, and the exchange transactions ought then to overestimate the volume of pure Bitcoin payments. Whichever the case, values are low in relation to the Swedish payment system. In total, household payments amount to around half of GDP for one year. This amounts on average to over SEK 4.5 billion daily. With cards and cash alone, households make more than 8 million payments to a value of over SEK 3 billion per day. Even if use of Bitcoin in Sweden were much greater than the exchanged value, the values are comparatively low.

DOES BITCOIN WORK AS A CURRENCY?

A currency has three functions. First, it serves as a means of payment, in the form of notes and coins. Second, it serves as a unit of account used to express prices, saving, mortgages, etc. in terms of e.g. kronor and öre. Third, it serves to preserve value in savings; in other words, I can refrain from consumption today, stuff my money in my mattress and use it for consumption tomorrow.

In theory, it can be said that Bitcoin fulfils the three roles of a currency, but in practice it doesn't. The role of a means of payment presumes that there is broad acceptance for the currency in society, otherwise it is hard to use it to make payments. In Sweden, there is no such broad acceptance and the possibilities of using Bitcoin as a means of payment are therefore very limited in practice. Similarly, it is uncommon for prices to be expressed in Bitcoin, although this does occur. It therefore cannot be said that Bitcoin serves as a generally accepted unit of account. Finally, the high volatility in Bitcoin's exchange rate makes it unsuitable for preserving value, because its purchasing power can very quickly diminish and a large part of the value is then lost.

A further difference between Bitcoin and traditional national currencies, such as the SEK, is that the latter enjoy special legal status in their country of issue. In Sweden, the Sveriges Riksbank Act establishes that the monetary unit in Sweden is called the krona, that it is divided into one hundred öre, that only the Riksbank may issue notes and coins and that these are legal tender, i.e. that the recipient of a payment has an obligation to accept cash.[17]

The benefits and risks of Bitcoin for users

For individual users, there are both benefits and drawbacks in Bitcoin, depending on the payment situation. The benefits mainly relate to anonymity/integrity, convenience, rapidity and costs. The drawbacks mainly relate to the lack of any kind of protection for users. In certain situations the benefits can outweigh the drawbacks, and vice versa in other situations. Normally, the benefits should weigh heavier in situations in which there are no simple, cost-efficient traditional payment services.

BITCOIN PROTECTS USER IDENTITY

The stated purpose of Bitcoin is to enable anonymous payments online and make them independent of governments, banks and other institutions. So, for users, the benefit of Bitcoin is that the network in which payments are mediated is global, and that certain payments that were not previously made for integrity reasons can now be made, both locally and globally. If a payment on a website is reduced to the push of a button instead of requiring entering a volume of payment information such as card numbers, etc. the time(cost) of the paying party for a payment is reduced. The risk of fraud can also be perceived as lower unless card numbers or account numbers need to be disclosed to the recipient. Personal integrity can then also be perceived as higher. A virtual currency can also allow users to make payments to new groups of recipients that are otherwise hard to reach, especially for payments for which the sender and recipient are in different countries. For some cross-border payments of this kind, Bitcoin can also prove a much cheaper and/or convenient alternative to more traditional payment services.

BITCOIN IS NOT REGULATED BY ANY NATIONAL LEGISLATION

There is no central Bitcoin issuer because the value units are created automatically in the network. Bitcoin thus does not come under any national legislation, neither is there a body to which any claims can be directed. The payments are also anonymous and as a rule it is not possible to show that a payment was made to a certain recipient. The exception is if the

[17] The Sveriges Riksbank Act (1988:1385).

parties involved know each other's identities and it is possible to demonstrate who owns a certain wallet. Individual users thus only have a narrow possibility of asserting their rights in the event of a payment going wrong.

A Bitcoin payment differs from a payment in Swedish kronor from a consumer protection perspective due to this very factor – i.e. that the Bitcoin payment is mediated via a global, decentralised network outside of the financial sector. The regulations governing normal payment mediation, such as the Payment Services Act, are not applicable, so neither do consumers have the same protection as in e.g. credit transfers or card payments. In other words, it might be more risky for the paying party to make payments using Bitcoin than using traditional payment services.

SHARP FLUCTUATIONS IN THE BITCOIN EXCHANGE RATE

Bitcoin does not represent a claim on another party; rather, its value consists entirely of an expectation that it can be used in future transactions. The value is thus highly sensitive to changes in such expectations. Diagrams 2 and 3 clearly show the major volatility in the Bitcoin exchange rate. Depending on the point in time at which somebody buys or receives Bitcoin, major exchange rate gains or losses can be made. Whether this is bad or not depends on the purpose of holding Bitcoins. If it is purely for transaction purposes, the exchange rate risk is considered to be negative because it makes the payment more risky; that is, the sender and recipient of the payment find it more difficult to set prices in BTC. This is perceived as an increased transaction cost.

For the Bitcoin holder, there is also a risk of losing value, either by fraud or accident. This is because the wallet and encryption keys are stored in some type of medium, such as on a hard drive. Should the hard drive be destroyed for some reason, the information would also be lost and hence so too access to the Bitcoin registered in the wallet. Through hacking, an external party can also access the value by initiating a payment to another wallet he controls. Fraud has occurred, the primary example being that which happened to exchange company Mt Gox, in which several hundred thousand Bitcoins were lost.[18] In this way, Bitcoins are more like cash than funds in bank accounts. If one loses or inadvertently destroys cash, its monetary value is lost. It can also be stolen. Funds in banks accounts are more protected. If the bank acts negligibly, it is liable to pay compensation. If the customer acts negligibly there is a statutory limit to his liability to pay compensation, and if the bank

[18] Mt Gox was the world's largest exchange company for virtual currency. It was located in Japan and offered its services globally. Mt Gox itself has not been very forthcoming about what happened, but it is thought the following occurred: one/several hacker(s) is/are thought to have manipulated the blockchain so that it appeared as though the outgoing Bitcoin payment did not go through to the buyer. Mt Gox then automatically made a new outgoing payment and in so doing was slowly drained of Bitcoin over a long period of time. Mt Gox started to experience difficulties in making outgoing payments at the end of 2013 and suspended them at the beginning of February 2014. It is thought that a total of around 850,000 Bitcoins disappeared. If so, the market value ought to amount to SEK 2-3 billion. In Canada, Bitcoins equalling USD 600,000 were stolen from Flexcoin, a Bitcoin bank/exchange site. Source: http://www.businessweek.com/articles/2014-02-26/where-did-the-bitcoins-go-the-mt-dot-gox-shutdown-explained#r=read

goes bankrupt there is a state deposit guarantee scheme that protects funds in accounts up to a value equalling EUR 100,000.

Benefits and risks for society

There are three main types of benefit that a virtual currency like Bitcoin brings to society. First, payments in Bitcoin can be more cost-efficient than traditional payments in certain situations. Bitcoin can thus, in some cases, involve savings and hence a more efficient payment system.

Second, a virtual currency like Bitcoin can contribute over time to a more robust payment system by not all payments passing through the traditional financial infrastructure that constitutes hubs around which the payment flow is concentrated.[19] If the functioning of such a hub were disrupted for some reason, the related payment traffic also comes to a halt. The mere fact of there being alternative routes for certain types of payment is positive from a contingency point of view.[20]

Third, there is a potential benefit in the form of innovation of new payment services and financial services that can be built around Bitcoin. Another important aspect is that the Bitcoin protocol is publicly available online, and that it can be modified if a majority of the network's computing power supports such a modification.

There are essentially two types of risk that Bitcoin could pose to the payment system. First, there is a risk that potential distrust of Bitcoin could spread and lead to more extensive distrust of other participants in the retail payment market too. This could lead to consumers and companies also rejecting safe payment services and participants in favour of perhaps more costly and slower payment services. The market would then not function as well.

Second, if key participants in the retail payment market, such as banks and financial infrastructure, were to have major Bitcoin holdings, this could expose them to substantial financial risks. It is they who provide payment services to households and companies, and if a few such participants were to fail at the same time, this could lead to a deterioration in the functioning of the market, at least temporarily. At the same time, risks to financial stability could theoretically arise if important financial institutions are directly exposed to the virtual currency, or if credit losses are sustained because the institution's customers are heavily exposed.

[19] See Sveriges Riksbank (2013). Chapter 1 explains how the Swedish payment system works, and Chapter 6 discusses future risks.

[20] The Riksbank and the infrastructure concerned are therefore working actively to prevent risks in the core financial infrastructure, see Sveriges Riksbank (2012). In the Riksbank's opinion, the Swedish financial infrastructure is secure and of a high international standard, see Sveriges Riksbank (2014).

LOW USAGE INVOLVES LITTLE BENEFIT AND LOW RISKS

Very small amounts are currently traded in Bitcoin on the Swedish market, and there is nothing to suggest that key participants have Bitcoin holdings. This renders both the potential welfare gain and systemic risks very low, and the conclusion is therefore that, to date, Bitcoin has not had any measurable impact on the Swedish retail payment market or financial stability.

Another type of problem in terms of society is however that certain virtual currency schemes, such as Bitcoin, which enable anonymous payments can be used for money laundering and other criminal ends.[21] While nobody knows the extent of criminal usage of Bitcoin, anecdotal examples (see footnote 21) suggest potentially substantial sums.

Future outlook for Bitcoin and other virtual currencies

It is believed that Bitcoin is only used to a minor extent for payments. Instead, the currency is held for speculation or saving purposes. If Bitcoin is to take market share from traditional payment services, it must thus be used for payments to a much greater extent than currently. What could prevent such a course of events? What could be the role of other virtual currencies in future?

NO CONSUMER PROTECTION OR SUPERVISION

The main factor that will probably make it difficult for Bitcoin to grow as a means of payment is the absence of consumer protection and supervision by public authorities. The reason for this is simple. Broad usage of Bitcoin for payments would also require a high proportion of consumers to be prepared to have Bitcoin holdings. If Bitcoin is perceived as risky, it is not very probable that the general public would be prepared to do this. I have called attention above to this lack of consumer protection in Bitcoin payments. Bitcoin holdings are also more risky than funds held in accounts. It is thus probable that Bitcoin must, in some way, be placed under the same or equivalent regulations that apply for other payment services or funds in accounts in order to gain broad acceptance – for anything other than very small payments.

At the same time, however, rendering the use of Bitcoin more reminiscent of traditional payments would overturn the fundamental concept underlying Bitcoin; that is, of it being independent of governments and the financial sector. Creating the requisite regulations could also prove difficult for the government. For example, how could something that is decentralised and does not have an issuer be regulated?

[21] The website Silk Road, on which drugs and criminal services were offered in exchange for Bitcoin, is the most notorious example. It was closed down by the FBI in October 2013. A new website, Silk Road 2.0 was however soon opened under different management to the original website. However, the new website was shut down in mid-February 2014 because Bitcoins worth around USD 2.5 million were missing – probably through embezzlement. Money laundering is another concern. The website Liberty Reserve, which was used for extensive money laundering, was closed down in May 2013. Fraudsters had appropriated regular currency for themselves, exchanged it to Bitcoin then sent it off untraceably.

DOESN'T WORK FOR ALL TYPES OF PAYMENT

Another obstacle is that Bitcoin is not suitable for all payment types, Bitcoin payments not occurring in real time. While payments are verified every ten minutes, it is also recommended that users wait for a couple of more verification rounds to be completed to be sure that the transaction has actually been added to the blockchain. Hence, it can take up to an hour for a user to be sure that the payment really has gone through. This makes Bitcoin unsuitable for many types of common payments, such as at the checkout of a convenience store. In card payments, which do not occur in real time either because the account of the recipient is credited with the funds one or several days later, this problem is resolved by reserving funds in the account of the payer and guaranteeing the payment to the payee. Bitcoin, which does not have a central issuer or verification process, cannot do this. However, individual payment service providers can guarantee Bitcoin payments to their customers. But, finding a guarantee that supports the decentralised usage of Bitcoin, without central participants, is difficult.

CREDIBILITY ISSUES OF A TECHNICAL NATURE ARE ALSO A BARRIER

Bitcoin's functioning is based on miners verifying transactions. Incentives for them to do so mainly consist of new Bitcoins being allotted to miners. However, this incentive could be undermined, which could erode confidence in the virtual currency.

One reason is that the creation of new Bitcoins declines over time.[22] This risks reducing the incentive for miners to continue with their activity. Another is the upper limit to how many Bitcoins there can be (21 million). The fundamental problem is that virtual currency can easily be newly created. If 21 million Bitcoins can suddenly turn into 42 million, each individual Bitcoin would also be worth less. Keeping an upper limit of 21 million Bitcoins is therefore important to preserving credibility in Bitcoin's future value. That credibility is affected by the perceived stability of the protocol governing Bitcoin. In connection with problems or a crisis, the protocol might quickly need modifying. Yet, if it is considered far too easy to modify the protocol, there is also a risk of confidence in the cap on the number of Bitcoins being undermined.

Another reason for why incentives for miners could be undermined is that the exchange rate could decline, which would reduce the value of the reward. On top of that, computing power and electricity might become too expensive. As the hash function becomes more complex, increasing computing power and bespoke computers are needed.

Another potential problem is that the length of the blockchain is constantly increasing. It is currently at over 14 gigabytes. The Bitcoin network presupposes that there is a great number of nodes with the entire blockchain stored on their machines. This makes the network robust. The incentive for managing such a "full" node has diminished, and such

[22] As described above in the section on how Bitcoin transactions work, the reward (N) for miners is halved around once every four years.

nodes are apparently decreasing in number.[23] It appears, in other words, as though Bitcoin is becoming increasingly centralised and thus less robust.

If incentives for miners disappear, the decentralised verification of transactions will cease and it will not be possible to use Bitcoin.

OTHER VIRTUAL CURRENCIES COULD REPLACE BITCOIN

There are thus several potential obstacles to Bitcoin's ability to grow as a means of payment. However, it is also important to bear in mind that Bitcoin was the first virtual currency. Although the Bitcoin protocol can be modified and is publicly available, which stimulates further innovation surrounding Bitcoin, it is not certain that Bitcoin will mark the end of the evolution of virtual currencies – better solutions could emerge, putting it out of business. There are currently over 450 other cryptocurrencies and they are constantly on the rise.[24] Some of them have taken Bitcoin's structure as their basis, but enhanced or modified it. Others have seemingly emerged as part of a business model to capitalise on the attention generated by Bitcoin.

The success and future of Bitcoin are thus not clear cut. All we know is that the future will not be as it is today, and how we make payments in 25 or 50 years' time is an open-ended question.

[23] See Cawrey, D. (2014a) and (2014b).

[24] According to http://coinmarketcap.com/ there were around 460 different cryptocurrencies in mid-August 2014. At the beginning of 2014 there were fewer than half that amount. The five largest in terms of issued value are Bitcoin, Ripples, Litecoin, Peercoin and Mastercoin. More about other virtual currencies can be found in Segendorf (2014).

References

Cawrey, Daniel (2014a), “What Are Bitcoin Nodes and Why Do We Need Them?”, www.coindesk.com, 9 May 2014.

Cawrey, Daniel (2014b), “The Five Biggest Threats Facing Bitcoin”, www.coindesk.com, 26 May, 2014.

Dagens Industri (2014), Drar in en halv miljard på bitcoin, article, March 24, 2014.

ECB (2012), *Virtual Currency Schemes*, October 2012.

Velde, François R. (2013), “Bitcoin – a primer”, *Chicago Fed Letter*, no. 317, December 2013.

Segendorf, Björn (2014), "Have virtual currencies affected the retail payments market?", *Economic Commentaries*, no. 2, Sveriges Riksbank, 2014.

Sveriges Riksbank (2012), *The Riksbank's oversight of the financial infrastructure.*

Sveriges Riksbank (2013), "The Swedish retail payment market", *Riksbank Studies*, Sveriges Riksbank.

Sveriges Riksbank (2014), *Financial Infrastructure Report*.

Swanson, Tim (2014), "What Block Chain Analysis Tells Us About Bitcoin", www.coindesk.com, 17 May 2014.

The Economist (2013), “Bitcoin under pressure”, 30 November.

Yermack, David (2014), “Is bitcoin a real currency – An economic appraisal", Working paper, New York University Stern School of Business and National Bureau of Economic Research.