Bitcoin – The Promise and Limits of Private Innovation in Monetary and Payment Systems

Christian Beer, Beat Weber[1]

A private initiative that has created a virtual currency and a payment system based on cryptography and decentralized management, Bitcoin is considered not only an interesting, but also a disruptive technical innovation by many observers. A number of regulatory and supervisory bodies have issued assessments of the phenomenon, contributing to an emerging international discussion. Does Bitcoin's claim to provide useful monetary and payment services hold up when checked against principles of monetary theory and the economics of payment systems? We find that while Bitcoin does not rival the established money and payment systems in their traditional domains, a complementary function is conceivable in niches. Using the Bitcoin network poses several risks to customers, however. Since this network and financial services related to bitcoins are not regulated, costumers must take appropriate technical measures to protect their bitcoin holdings. In case of error and fraud, payments are difficult to reverse. Furthermore, the significant exchange rate fluctuations could pose a grave risk to bitcoin owners' wealth and discourage widespread use for monetary purposes. In a nutshell, at present, bitcoins can be regarded as speculative assets, and the Bitcoin network might inspire further innovation in payment systems and other applications.

JEL classification: E42, E52, E58
Keywords: Monetary reform, monetary policy, monetary systems, payment systems, innovation

The economic and financial crisis that had started in 2007 triggered a public discussion about the performance of the financial system. Contributions to this discussion have included innovative attempts of providing alternative solutions for a number of services offered by this system (Weber, 2015), with Bitcoin a prominent example, which has garnered a lot of media attention in the last two years. This privately initiated project, which is based on open participation, intends to provide a private digital currency – the bitcoin (BTC)[2] – and a system for transferring payments in this currency. In this article, we assess the claims of its supporters and the implications of its operation for central bank goals.

Section 1 describes the way Bitcoin works and its market development. In section 2 we assess Bitcoin's claims to work as a payment system, section 3 concentrates on Bitcoin as a currency, and section 4 reviews assessments from authorities. Finally, section 5 concludes.

1 Bitcoin – How Does It Work, and How Does It Perform?

In 2009, a white paper was published online under the name Satoshi Nakamoto (probably a pseudonym), proposing a new solution for something that some Internet enthusiasts had been looking forward to since the beginning of the Internet: A form of digital cash that functions based on principles dear to libertarian strands of the Internet community – non-state administered, decentralized ("peer to peer") and open source based. In this strand of thought, cryptography and anonymous transaction systems are seen as important instruments to defend privacy and freedom in the digital age (Hughes, 1993; Stephenson, 1999). With trust in the monetary and financial system shattered by the crisis, Nakamoto's proposal was

[1] *Oesterreichische Nationalbank, Economic Analysis Division, christian.beer@oenb.at, and European Affairs and International Financial Organizations Division, beat.weber@oenb.at.*

[2] *"Bitcoin" refers to the system, "bitcoin" and BTC to the unit of account in that system.*

Refereed by:
Adrian Blundell-Wignall and Gert Wehinger, OECD

taken up in 2009 and implemented by a significant number of supporters.

Bitcoin offers a purely digital currency consisting of strings of numbers. An open source software provides a platform where users can produce a private currency and make payments in this currency without recourse to banks and central banks, based on encryption technology. This setup is meant to make online payments comparable to cash payments offline.

The system is run by voluntary supporters that are attracted and governed by economic incentives provided by the system architecture. With each supporter contributing computing power, a network is formed. Network supporters are attracted by the prospect of engaging in competition over receiving newly issued bitcoins. This process is inspired by gold extraction: Like gold, bitcoins are "buried" in the system and may be unearthed and put into circulation by "miners." The mining process is designed in the following way: Every ten minutes, the system provides a new amount of bitcoin units. In order to obtain them, network supporters, i.e. miners, compete to solve mathematical problems with a random component. These problems are hard to solve, but the correctness of the solution is easy to verify. In each of these contests, the competitors coming up with the first correct solution receive the newly issued amount of bitcoin units. They broadcast their solutions to the whole network, where they are automatically verified by other members.

The software provides for a fixed amount of currency units (about BTC 21 million). A pre-established technical rule ensures the issuance of these units into circulation up to about 2140 according to a specified time path. However, as the reward to miners will be reduced[3] over time, more than 99% of all bitcoins will have been mined in about 2032. In mid-October 2014, more than 13 million bitcoins were in circulation.

Once new bitcoin units are in the possession of a member (apart from mining, bitcoins can be acquired on exchanges or by selling goods or services in exchange for bitcoins), they can be kept or spent if other members accept them as payment in a transaction, or exchanged for official currencies. So how are bitcoins transferred among members? Bitcoins are stored in anonymous addresses in the form of strings containing numbers and letters, equipped with two complementary keys, one public and one private. The public key can be compared to the account number of a bank account, and the private key to the PIN to access such account. If A wants to send a payment to B, A needs B's public key and encrypts a certain sum of bitcoins with B's public key and A's private key, so that only B can decrypt the payment and make use of the sum. To transmit the payment and, at the same time, to guarantee that A has not spent the same electronic string of numbers on another occasion (double spending), the transaction partners rely on the network. It performs the functions that payment intermediaries fulfill in conventional payment processes. Every ten minutes new payment transaction orders are collected by the system and are verified by the system supporters. To this end, new transactions are recorded in a public ledger called blockchain that comprises all transactions ever operated in the Bitcoin system. By comparing the new bitcoin payment orders with the history

[3] *Initially, the reward for solving a block (a record of recent transaction orders) was set to BTC 50. Every 210,000 blocks – i.e. about every four years (given an average rate of six blocks per hour) –, this subsidy is reduced by 50%.*

of all previous orders, the legitimacy and accuracy of the orders are verified. For various technical reasons, a bitcoin transaction can only be considered secure after a number of confirmations in the Bitcoin network. The incentive for network members to participate in the verification process is the above-mentioned mining process. The mathematical problem to be solved to gain newly created bitcoins or transaction fees depends also on information about the previous blockchain and transaction. Mining for bitcoins therefore also helps check that new transaction orders are legitimate and adds these new transactions to the blockchain.

Theoretically, the system offers an innovative method for solving the problem of producing agreements among mutually distrustful parties. Technically, this process consumes significant amounts of computing power and electricity. Competition among miners has led to continuous innovation and investment in computer processing power. Consequently, entry barriers have risen as well, given the cost of computer hardware and energy, which entails the risk of increasing concentration in mining (The Economist, 2013). Over time, it will be increasingly inconvenient to save the ever growing blockchain. Fewer supporters might therefore be willing to support public record keeping, which would weaken the network and make it more vulnerable to attack. Bitcoin mining continuously drives up energy consumption, and given low energy efficiency, energy consumption per transaction is high (Sorge and Krohn-Grimberghe, 2013).

The market price of one bitcoin unit, as derived from quotations on the most frequented private exchanges, was relatively flat until the beginning of 2013 (see chart 1). It then skyrocketed, reaching USD 1,151 in December 2013, which implied a price increase of 8,388% in 2013. This enormous price hike can be considered both cause and effect of growing media attention and further contributed to the popularity of Bitcoin (Salmon, 2013). Recently, we have observed a general downward trend, with BTC 1 worth USD 384.1 on October 22, 2014.

Chart 1

Market Price

USD market price of the bitcoin on the major exchanges

Source: http://blockchain.info.

In mid-2014, 41 million addresses were registered in the system (Ali et al., 2014, p. 4). As users are able, and even encouraged, to register multiple addresses to retain anonymity, the number of actual users is likely to be much smaller (Sorge and Krohn-Grimberghe, 2013). Only 1.6 million Bitcoin addresses existing in July 2014 accounted for holdings of more than BTC 0.001 (Ali et al., 2014, p. 4), which can be interpreted as being indicative of the upper limit of any estimate of the number of Bitcoin users. Given the anonymous and global nature of the system, no data are available on Bitcoin usage in Austria or other countries. The "Bitcoin Austria" association[4] hosts regular meetings for local Bitcoin users.

[4] *See http://bitcoin-austria.at.*

So far, user traffic has been significant, but still modest when compared with established payment systems. According to the Bitcoin information site blockchain.info,[5] the system had administered about 50 million bitcoin transactions by October 2014. In 2013, the daily average came to about 60,000 transactions (representing a total daily value of USD 237 million based on the bitcoin's peak valuation in December 2013). By contrast, the biggest credit card provider, Visa, registered 212 million transactions per day (representing a value of USD 16 billion).[6] Given the anonymous nature of bitcoin transactions, there is no reliable information on what they are used for.

2 Bitcoin as a Payment System

Bitcoin claims to operate a retail payment system with no need for trusted intermediaries. The latter are perceived to charge excessive fees for payment transmission[7], to lack adequate protection of personal financial data (e.g. with regard to credit card fraud or disclosure to public authorities) and to expose customers to financial risk by being prone to financial crises (Nakamoto cited in p2p foundation, n.d.). In this section, we discuss whether Bitcoin can legitimately claim to provide improvements on these charges.

Whereas users have over decades become accustomed to paying with cash at zero financial transaction costs within national economies thanks to public support for the underlying infrastructure, other forms of retail payments may involve (substantial) costs. However, the advent of globalization and digitalization has led to an increase of commercial innovation in the retail payment market, expanding on the initial innovation of the credit card (Maurer, 2011; Salmon, 2013). As a consequence, competition among payment service providers has been on the increase over the past few decades. The established business model of intermediating electronic payments can be characterized as a two-sided market, where a payment service provider links payer and payee. In facilitating and recording transactions, the payment service provider is faced with a choice concerning the allocation of the burden of fees among payer and payee. In most card payment systems, merchants bear most of the cost charged by the payment service provider. Consumers may likewise face significant costs, especially in cross-border consumer-to-consumer payment services (Bolt, 2013). In this context, Bitcoin has positioned itself as a low-cost alternative (Pflaum and Hateley, 2014).

With respect to cost, bitcoin payments can currently be made at minimal or no financial cost to the two parties engaged in a payment transfer. This is possible because the mining process described above is devised to substitute for the role of banks and other established payment operators in the Bitcoin system. Instead of a centralized intermediary, the payment transfer is operated by miners following the procedures of the Bitcoin protocol

[5] *See http://blockchain.info.*

[6] *See http://www.btcfeed.net/infographics/bitcoin-vs-other-payment-systems-daily-transaction-volume (retrieved on October 28, 2014).*

[7] *According to a survey by the European Commission published in 2012, the European payment card industry provides the means for consumer payments with an overall value of EUR 1,350 billion per year. Such payments generate an estimated EUR 25 billion in annual fees (European Competition Network, 2012, p. 17), which corresponds to an average fee of 1.9%. On the basis of this study, the European Commission started to launch proposals to regulate the market for card, Internet and mobile payments.*

(engaging in competition to solve problems, with the byproduct being the confirmation and recording of the payment transfer). As mentioned before, Bitcoin miners incur substantial costs for hardware and electricity. Stiffer competition and greater complexity of the problem to be solved[8] imply a continuous upgrade of computing power and increased electricity use. Miners incur that cost without charging substantial fees to customers because successful miners are rewarded with new units of the remaining bitcoin stock. So, the cost advantage for customers is based on systematic cross-subsidization of the payment system by the currency creation process. This advantage is dependent on collective value attributions to Bitcoin being sufficiently high in order for miners to cover their costs (which are due in official currency). Cross-subsidization may also be evident in traditional payment systems: Many banks, for instance, allow customers to make payments free of charge, recovering costs through profits in other areas. Most credit card operators charge merchants per-payment fees, while customers – apart from a lump-sum annual charge – do not pay extra for individual payments. In cash payments, important logistical costs are borne by central banks and by ATM operators (Schmiedel et al., 2012).

How sustainable is the cost recovery process in the Bitcoin system? While there is no fixed charge for bitcoin payments, users can and do offer small fees to miners. Because there is no obligation for miners to include all payments in their calculation, more resourceful miners can be incentivized to include a payment when a fee is offered, thereby increasing the speed of transaction for customers. Currently, transaction fees are of minor importance. Calculations with data from blockchain.info show that less than 1% of miners' revenues are from transaction fees. However, while successful miners are currently rewarded with 25 newly issued bitcoins, this amount will decrease to about 0.78 bitcoins in 2032 (when about 90% of all bitcoins will have been mined). Whether miners will be able to recover their costs with such a reward, will depend on the bitcoin's market value and the production costs. The reward will eventually drop to zero in 2140 when the whole bitcoin stock will have been put into circulation. Hence, eventually miners will have to fully recover their costs from customer fees. To give some estimates of transaction costs, calculations with the above-mentioned data reveal that, in 2014, miners' average revenue (new bitcoins plus fees) per transaction amounted to USD 37.05 (2013: USD 14.59), which is equivalent to 4.40% (2013: 2.42%) of the transaction volume. Based on an educated guess of capital and operating expenditure for competitive bitcoin mining, McCook (2014) calculated that, in mid-2014, the costs (capital expenditures and electricity, excluding labor costs) for bitcoin mining amounted to about USD 600 per bitcoin, which basically equaled the market price at the time.

Because all payment transfers are preceded by a race, where many competitors attempt to solve the same task, the marginal costs in the Bitcoin system for verifying transactions is higher than in centralized payment systems (Ali et al., 2014, p. 6).

All this implies that the price advantage of bitcoin payments is not based on a cost advantage and is a

[8] *The difficulty is adjusted in order to keep the average number of blocks solved at six per hour.*

transitory phenomenon only.[9] Moreover, if Bitcoin is merely used as a payment vehicle, the costs of exchanging legal tender currency for bitcoins and back must be added.[10]

Another important question is whether users of Bitcoin are exposed to risks. Bitcoin, which does not eliminate financial and operational risks to customers, rather implies a transfer of risks to the individual. The Bitcoin system's efforts to ensure the integrity of the payment system concentrate on counterfeit control and securing anonymity. Bitcoin attempts to digitally mimic cash in terms of anonymity, payment finality, transaction costs and decentralized operation of transfers. To prevent double spending, a public record of all transactions is kept against which every new transaction is checked. As long as users manage to prevent detection of address ownership by outside observers, transactions can remain anonymous. Anonymity in transactions could make the system suitable for money laundering, tax evasion and the purchase of illicit goods and services. While other payment systems (apart from cash) do not support such anonymity, they typically offer payment services as part of a bundle of services. For example, banks offer deposit taking, account keeping, proof of payment services and chargeback facilities together with payment services. In the Bitcoin system, these services are unbundled. The core infrastructure only offers one-way payment transfers and counterfeit checks. Related services must either be purchased from third-party providers or be provided by users themselves.

In light of the anonymous and decentralized nature of payment transfers in Bitcoin, there is no intermediary to reverse payments that were made erroneously or where counterparties did not fulfill their obligations in return. Consumers who want their money back have to pay for third-party escrow services or go to court in the case of complaints, provided anonymity does not prevent such measures. Merchants, on the other hand, might be inclined to perceive the lack of chargeback risks as an advantage. They may also benefit from the lower Bitcoin fees compared with card payment services, where they usually bear the brunt of fees. Also, accepting bitcoins might serve as a marketing move to attract additional customers and profit from the public attention the project receives (Fuchs, 2014; Wingfield, 2013). The "no chargeback" feature of Bitcoin and the elimination of merchant fees involved in credit card payments favor merchants. In contrast, consumers face a comparably higher risk of nondelivery, and may or may not be offered discounts by merchants to share in their fee advantage (Fleishman, 2014; Wingfield, 2013). In any case, these considerations apply mainly to online businesses. In offline retail commerce, undue waiting times result from the fact that a bitcoin transaction can only be considered secure after six confirmations in the Bitcoin network. This can be expected

[9] *The cost disadvantage vis-à-vis centralized systems can induce concentration pressure in the market of bitcoin miners in order to achieve economies of scale. Such an outcome would defeat the original intention of decentralization and increase fraud risks (Ali et al., 2014, p. 6).*

[10] *Within the scope of this article we cannot analyze whether there are circumstances where – despite these features – use of Bitcoin could promote financial inclusion either because of lack or excessive cost of alternatives, e.g. payments to and within underbanked areas (see Pflaum and Hateley, 2014, for a discussion of the legal dimension). Of course, Bitcoin is only one of many possible solutions in this regard, as indicated by the success of money transfers via mobile phones in some regions.*

to take up to one hour, which may in many cases be longer than customers are prepared to wait for payment to be completed (Velde, 2013).

In Bitcoin, users must store their holdings either on their own computer or in wallets provided by third-party service providers. Currently, the latter are private startups not (yet) subject to bank-like regulation and the associated safety nets. Bitcoin users are therefore subject to risks from loss, theft and fraud of their holdings to a greater degree than with established service providers. In February 2014, Mt.Gox, the biggest Bitcoin trading platform at that time, had to close after significant amounts of user holdings had been reported to be lost or stolen (McMillan, 2014).

Furthermore, there are significant risks and costs involved in exchanging bitcoins for official currency. As there is no market maker, being able to buy and sell bitcoins depends on finding a transaction partner on one of the private exchange platforms online. The exchange rate is very volatile, and the market is rather illiquid. Exchange charges can be in the order of a few percent (Fleishman, 2014). Many exchanges closed after a few months, with at least one involving severe losses for users (Moore and Christin, 2013). Although various exchanges coexist, there are rarely any arbitrage opportunities, as these are outweighed by the cost of moving funds between exchanges (Gandal and Halburda, 2014, p. 3).

3 Bitcoin as a Monetary System

In economic theory, money is defined by three functions: unit of account, means of payment and store of value.

In modern economies, there is a single unit of account in every currency area. This is considered to be an efficient solution: Having all prices in a currency area denominated in the same unit makes them comparable and enables the operation of markets. Usually, means of payment are issued as official currency by a central bank that is in charge of ensuring the quality and quantity of that money according to a public mandate. In most countries, such a mandate entails ensuring the functioning of these means of payment as stable and most liquid store of value over the short to medium term. The acceptance of official currency among the public is supported by the currency's exclusive acceptance by the state for the discharge of tax liabilities and its use by the state as (one of) the biggest single transaction parties in the economy. Apart from the central bank, private issuers can also offer means of payment as long as they are accepted by the public. Such private means of payment, denominated in the official unit of account, represent a claim on the issuer for official currency. Banks are the biggest providers of private means of payment, as the bulk of daily transactions among economic subjects is conducted by transferring bank deposits (which represent a claim on official currency). In their role as the biggest providers of private means of payment, banks are subject to regulation, supervision and monetary policy. The resulting monetary system is a hierarchical construction, where the state-provided unit of account and means of payment issued in that unit form the apex of the system, and private means of payment represent claims on the official means of payment denominated in the official unit of account. The need to maintain the ability to keep the promise underlying these claims serves as a major disciplining device for the issuers.

While Bitcoin represents one of many private means of payment, it entails three peculiarities: It introduces

a separate unit of account, it has no single and identified issuer and its quantity is ultimately fixed once and for all.

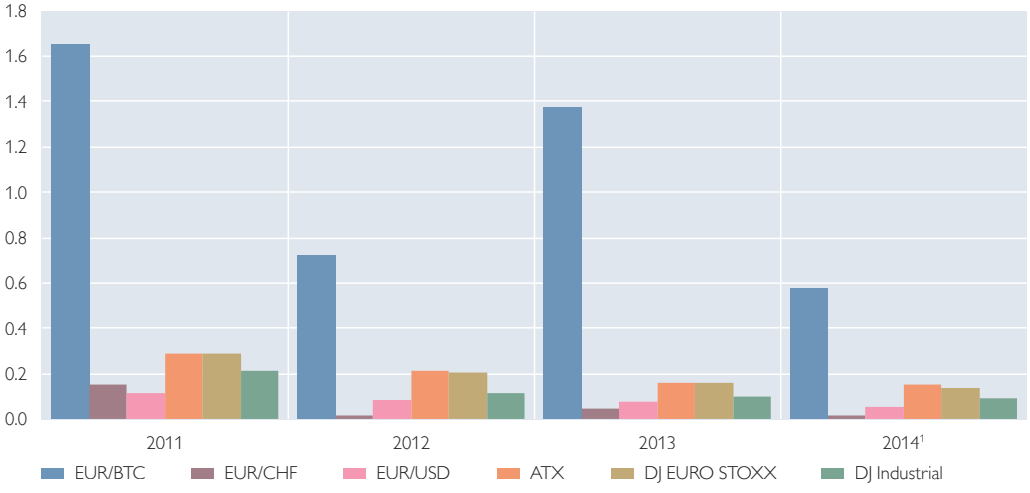
Built around the model of gold, the bitcoin is a pure asset not related to credit creation processes. It has no central issuer and does not represent anybody's liability. This implies that its quantity cannot be adjusted to variations in demand, and it does not come with anybody's promise to convert it into official currency at a certain rate. Given its operation based on cryptographic mechanisms described above, the term "cryptocurrency" has been introduced to characterize Bitcoin-type systems. Bitcoin governance is not completely decentralized: There is the Bitcoin Foundation, which describes its tasks as standardization (e.g. funding the Bitcoin infrastructure, including a core development team), protection (e.g. maintenance, improvement and legal protection of the integrity of the technical protocol underlying the operation of Bitcoin) and promotion of the Bitcoin system, but does not represent the issuer of the currency.[11] The latter is replaced by a decentralized process of mining as described above. The Foundation is based on voluntary membership, whose voting and other rights depend on the size of the fee (based on four membership classes with different rights). Whereas central banks' role in the monetary and payment system is based on a legal mandate of the polity of the currency area and its ability to issue currency, the Bitcoin Foundation lacks such ingredients and therefore cannot fulfill the role of a central bank. Indeed, deliberately designing a system without a central bank is one of the cornerstones of the Bitcoin concept.

Being nobody's liability is a feature the bitcoin shares with gold. But in contrast to gold, which is customarily used for various products (e.g. electronics, industry, dental fillings or jewelry) and has a commodity value, the bitcoin has no use value other than

Chart 2

Volatility

Annualized standard deviation of daily logarithmic changes



Source: OeNB, http://blockchain.info, authors' calculations.

[1] January 1 to October 20.

[11] *See https://bitcoinfoundation.org for more details.*

serving its role in the Bitcoin system. Therefore its value is determined only by the subjective valuation of users, exhibiting substantial volatility in terms of official currency (see chart 2). The fixed increase, up to a predefined final level, of supply makes demand effects dominant. This has led some observers to invoke the "greater fool theory" as basis for the bitcoin's valuation (Blundell-Wignall, 2014, p. 9). Can the bitcoin nevertheless serve monetary purposes?

Economists in the tradition of Friedrich A. Hayek have called for the abolition of the prevailing monetary system in favor of competing private units of account (see Weber, 2013, for a detailed account).[12] Such a conception entails a number of problems, however. A newly introduced rival private unit of account is at a huge disadvantage against an established unit, all the more if it has an unstable exchange rate against the official unit of account. A unit of account is subject to significant network effects, which entails switching costs for users (Dowd and Greenaway, 1993). If a merchant were to start to price goods and services in bitcoin, she would incur substantial exchange rate and conversion risks. With inputs and taxes being priced in official currency, bitcoin income from sales would have to be at least partially converted into official currency. But their value would fluctuate in terms of the official currency according to the daily exchange rate, and conversion costs would accrue. As a result, while there are a number of online merchants accepting bitcoins in payment, none of them is known to use the bitcoin as a unit of account. Instead, prices are fixed in official currency and bitcoin prices are adjusted according to the bitcoin's fluctuating exchange rate, possibly including additional costs for the conversion spread.

While several (mainly online) merchants accept payment in bitcoin[13] and the Bitcoin network has attracted a significant number of payment transactions, there are strong reasons to suspect that bitcoins are not widely used as a means of payment. Due to the anonymity of transactions, no direct observation on the motives underlying bitcoin payments is possible. But the fixed supply of bitcoins is designed to attract users with the promise of value appreciation in the face of growing demand. Whereas official currency is managed with a view to serving as a stable store of value over the short and medium term, Bitcoin builds on the promise of long-term value appreciation, not stability. In the short term, it even exhibits extraordinary volatility in comparison with most other financial assets (Yermack, 2013; see chart 2).[14] There is no market maker willing or able to ensure the stability usually expected from a currency by users. Rather than a store of value, the bitcoin can be better characterized as a speculative asset. In light of this, economic incentives for hoarding are far greater than incentives for spending bitcoins. Exceptions are transactions where using official currency is not applicable or disadvantageous (e.g. illicit transactions and small-denomination online payments). According to Segendorf (2014, p. 79), trade appears to be subdued as a mere 4% of all bitcoin holdings are traded within one week and 24% within three months. It takes six months for some 50% to be traded, and about 38% are held for more than one year.

[12] *According to a Bitcoin Foundation executive, "Choice in currency is the free speech of commerce." (Matonis, 2013).*

[13] *According to http://coinmap.org about 50 Austrian companies accept payment in bitcoin.*

[14] *Although the implications of this attribute for portfolio choice are subject to debate, see Briere et al. (2013).*

Gandal and Halburda's (2014) observations on market developments in competing cryptocurrencies confirm this assessment. A number of cryptocurrencies have emerged in the wake of Bitcoin, most of them modeled after the latter with small variations in design. If there were an emerging market for cryptocurrency as a substitute for money, network effects would entail a winner-takes-it-all dynamic. But although Bitcoin was the first and is by far the largest network in terms of market capitalization, several hundred competitors have since then been established by various entities and some have succeeded in gathering some support. This could be considered evidence that the financial asset function is a more prominent motive than currency adoption among users.

4 The Opinion of Governments and Regulators

Following the bitcoin's price hikes and increasing coverage by the media, governments, central banks and regulators have started to publish opinions on Bitcoin. These publications discuss the risks of Bitcoin (e.g. to costumers or financial stability), potential regulatory responses or the legal and fiscal classification of Bitcoin. In this section, we review some of these assessments, focusing on Austrian and European contributions.

The risks of Bitcoin and potential regulatory reactions are for example discussed by the European Central Bank (ECB, 2012) and the European Banking Authority (EBA, 2014). The ECB focuses on those aspects that are relevant for central banks, i.e. risk to price stability, financial stability, the payment system, and reputational risks for central banks. Overall, the ECB concludes that virtual currency schemes do not pose considerable risks, inter alia because of their relatively low volume and their limited interrelation with the real economy. However, this could change if virtual currency schemes became quantitatively more important and their use more widespread. The ECB further notes that, as payment systems, virtual currency schemes fall into the responsibility of central banks. Central banks therefore also need to take into account potential reputational risks as central banks may be held responsible by the public for incidents involving bitcoins. In any case, the development of virtual currency schemes and their interaction with the real economy should be closely monitored.

After the EBA had issued a warning to make consumers aware of risks that arise from the fact that virtual currencies are not regulated (EBA, 2013), the regulatory agency published an opinion on virtual currencies in July 2014 (EBA, 2014). It comprises a discussion of potential benefits and risks of virtual currency schemes as well as the EBA's opinion on their regulation. Even though the EBA (2014) concedes that there are potential benefits (e.g. lower transaction costs, increased financial inclusion), it considers these benefits less relevant in the EU. Some of the potential advantages may only exist because of the lack of regulation. Furthermore, it is not guaranteed that these advantages will still apply in the future. On the other hand, the EBA identifies about 70 risks and categorizes them (see figure 1 in EBA, 2014, p. 22), for instance, into risks to users (e.g. losses through hacking), risks to non-user market participants (e.g. merchants are eventually not reimbursed), risks to financial integrity (e.g. money laundering, other financial crime), risks to existing payment systems (e.g. conventional payment services compromised from virtual currency operations

of the payment system provider), and risks to regulatory authorities (e.g. reputational risks when chosen regulatory approach fails). Not all of these risks are specific to virtual currencies; some are also present in conventional payment services or financial products.

As to regulation, the EBA (2014) differentiates between an immediate response and a comprehensive response that can most likely only be implemented in the long term. The immediate regulatory response that the EBA advocates should mitigate risks that arise from the interaction of virtual currency schemes and the regulated financial sector. This should essentially be achieved by separating regulated financial services from virtual currency schemes as regulators should discourage regulated financial intermediaries from buying, holding or selling virtual currency schemes. Furthermore, the EBA recommends for "market participants at the direct interface between conventional and virtual currencies such as virtual currency exchanges, to become 'obliged entities' under the EU Anti Money Laundering Directive and thus subject to its anti-money laundering and counter terrorist financing requirements" (EBA, 2014, p. 6). The comprehensive long-term regime includes, among other elements, the creation of a governance authority for each virtual currency scheme that is accountable to the regulator, the collection of basic identity information when someone buys virtual currencies, standards for individuals performing certain functions with respect to a virtual currency scheme, mandatory incorporation as a legal person in an EU Member State, capital requirements for those market participants that hold virtual currency on behalf of others as well as measures that ensure the security of IT systems. Risks stemming from the fact that virtual currencies are not legal tender and that there is no authority that provides exchange rate stability remain deliberately unaddressed.

Another strand of official responses deals with the legal classification of both Bitcoin and economic activity related to bitcoins as well as tax-related issues. In this regard, the Austrian Ministry of Finance (BMF, 2014) argues that the bitcoin does not constitute a financial instrument. The Ministry of Finance basically shares the opinion of the Austrian Financial Market Authority (FMA, 2014), which states that – while Bitcoin is in principle neither regulated nor supervised by the FMA – certain business models involving Bitcoin may require compulsory licensing. Certain activities involving bitcoin transactions can be taxable, e.g. VAT for the exchange of bitcoins and income tax on income from mining and capital gains. The view of the Ministry of Finance that the bitcoin is not a financial instrument departs from the opinion of the Austrian Ministry of Economics (BMFWF, 2014). In the same vein, Germany's Federal Financial Supervisory Authority (BaFin, 2014) regards the bitcoin as a financial instrument, but not as e-money. Trading of bitcoins may require authorization.

Several institutions also warned consumers against using or investing in bitcoins, stressing the risks involved. The above-mentioned warning by the EBA (2013), for instance, stresses the fact that users of Bitcoin are not protected by regulation (e.g. in case "platforms that exchange or hold virtual currencies fail or go out of business") and that the value of bitcoins may not remain stable. The EBA (2013) discusses potential losses due to fraud (e.g. when digital wallets are hacked) and advises consumers to take care of potential tax liabilities resulting from

the use of virtual currencies. In Austria, the warnings of the EBA were reiterated by the FMA (2014). Similar warnings were issued, inter alia, by the Banca d'Italia (2014) and the Banque de France (2013).

5 Summary and Conclusions

From a technical point of view, Bitcoin offers an interesting proposal for a decentralized payment system. But doing away with regulated intermediaries in payment systems exposes users to a number of new risks and costs, which will make its use only attractive for purposes which are underserved by existing payment systems, such as illicit transactions due to its anonymity features as well as small-denomination online payments due to transitory low user costs. The risks involved have been the subject of a number of opinions recently issued by authorities worldwide.

The price hikes of bitcoins suggest that this virtual object is largely regarded as a speculative asset rather than as a currency. The high volatility of the exchange rate against official currencies makes the use of bitcoins in a world in which most payments eventually have to be made in official currencies quite risky.

While exposing the lack of competition in certain payment markets and potentially contributing to competition-inducing innovation in payment systems, the bitcoin in its present form cannot therefore be expected to offer noteworthy competition for official currencies in their established domain. Its design points to instability over time, disfavoring adoption as a unit of account, means of payment and store of value.

Nevertheless, technological innovations that are associated with bitcoins and other cryptocurrencies may inspire innovation in payment systems and other applications.

References

Ali, R., J. Barrdear, R. Clews and J. Southgate. 2014. The economics of digital currencies. In: Bank of England Quarterly Bulletin Q3. 1–11.

BaFin. 2014. Annual Report 2013.

Banca d'Italia. 2014. Financial Stability Report 1/2014. May.

Banque de France. 2013. Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin. Focus n°10 – 5 décembre 2013.

Bitcoin Foundation. 2014 https://bitcoinfoundation.org/about (retrieved on October 22, 2014).

Blundell-Wignall, A. 2014. The Bitcoin Question. Currency versus Trust-less Transfer Technology. OECD Working Papers on Finance, Insurance and Private Pensions 37. http://dx.doi.org/10.1787/5jz2pwjd9t20-en.

BMF (Bundesministerium für Finanzen). 2014. Anfragebeantwortung zur schriftlichen Anfrage betreffend rechtliche Klarstellung zu Bitcoin und weiteren virtuellen Währungen. http://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_01485/imfname_359813.pdf (retrieved on December 18, 2014).

BMWFW (Bundesministerium für Wissenschaft, Forschung und Wirtschaft). 2014. Anfragebeantwortung zur schriftlichen Anfrage betreffend rechtliche Klarstellung zu Bitcoin und weiteren virtuellen Währungen. http://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_01446/imfname_359616.pdf (retrieved on December 18, 2014).

Bolt, W. 2013. Pricing, Competition and Innovation in Retail Payment Systems: a brief Overview. In: Journal of Financial Market Infrastructures 1(3). 73–90.

Briere, M., Oosterlinck, K. and Szafarz, A. 2013. Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins. http://ssrn.com/abstract=2324780 (retrieved on December 18, 2014).

Dowd, K. and D. Greenaway. 1993. Currency Competition, Network Externalities and Switching Costs: Towards an Alternative View of Optimum Currency Areas. In: The Economic Journal 103(420). 1180–1189.

EBA. 2013. Warning to Consumers on Virtual Currencies. December. https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf (retrieved on October 30, 2014).

EBA. 2014. EBA Opinion on 'virtual currencies.' http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (retrieved on October 30, 2014).

ECB. 2012. Virtual Currency Schemes, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (retrieved on November 27, 2014).

European Competition Network Subgroup Banking and Payments. 2012. Information paper on competition enforcement in the payments sector. http://ec.europa.eu/competition/sectors/financial_services/information_paper_payments_en.pdf (retrieved on October 30, 2014).

Fleishman, G. 2014. On the Matter of why Bitcoin Matters. https://medium.com/the-magazine/23e551c67a6 (retrieved on March 17, 2014).

FMA. 2014. Bitcoin. http://www.fma.gv.at/en/special-topics/bitcoin.html (retrieved on October 30, 2014).

Fuchs, J. G. 2014: Bitcoin, jetzt oder nie: Warum sich die Kryptowährung für deinen Onlineshop lohnt. http://t3n.de/news/bitcoin-yolo-kryptowaehrung-558694 (retrieved on October 30, 2014).

Gandal, N. and H. Halburda. 2014. Competition in the Cryptocurrency Market. Bank of Canada Working Paper 2014–33.

Hughes, E. 1993. A Cypherpunk Manifesto. http://www.activism.net/cypherpunk/manifesto.html (retrieved on October 30, 2014).

Matonis, J. 2013. Why I Accepted Executive Director Position for Bitcoin Foundation. July 9. http://themonetaryfuture.blogspot.co.at/2013/07/why-i-accepted-executive-director.html (retrieved on October 20, 2014).

Maurer, B. 2011. Money Nutters. In: Economic Sociology 12(3). July 2011.

McCook, H. 2014. Under the Microscope: Economic and Environmental Costs of Bitcoin Mining. June 21. http://www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining (retrieved on October 28, 2014).

McMillan, R. 2014. The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster. In: Wired. March 3. http://www.wired.com/2014/03/bitcoin-exchange (retrieved on October 28, 2014).

Moore, T. and N. Christin. 2013. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. http://fc13.ifca.ai/proc/1-2.pdf (retrieved on October 20, 2014).

Nakamoto, S. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf (retrieved on October 30, 2014).

p2p Foundation, n.d. Bitcoin. http://p2pfoundation.net/bitcoin (retrieved on October 30, 2014).

Pflaum, I. and E. Hateley. 2014. A Bit of a Problem: National and Extraterritorial Regulation of Virtual Currency in the Age of Financial Disintermediation. In: Georgetown Journal of International Law 45(4). 1169–1214.

Salmon, F. 2013. The Bitcoin Bubble and the Future of Currency.

https://medium.com/@felixsalmon/the-bitcoin-bubble-and-the-future-of-currency-2b5ef79482cb (retrieved on October 30, 2014).

Schmiedel, H., G. Kostova and W. Ruttenberg. 2012. The Social and Private Costs of Retail Payment Instruments. A European Perspective. ECB Occasional Paper Series 137.

Segendorf, B. 2014. What is Bitcoin? In: Sveriges Riksbank Economic Review 2. 71–87.

Sorge, C. and A. Krohn-Grimberghe. 2013. Bitcoin – das Zahlungsmittel der Zukunft? In: Wirtschaftsdienst 93(10). 720–722.

Stephenson, N. 1999. Cryptonomicon. Avon Books: New York.

The Economist. 2013. Bitcoin under Pressure. In: Economist Technology Quarterly no. 4. 30 November 2013. http://www.economist.com/news/technology-quarterly/21590766-virtual-currency-it-mathematically-elegant-increasingly-popular-and-highly (retrieved on October 30, 2014).

Velde, F. R. 2013. Bitcoin: A Primer. In: Chicago Fed Letter December No. 317.

Weber, B. 2013. Ordoliberale Geldreform als Antwort auf die Krise? Bitcoin und Vollgeld im Vergleich. In: DIW Vierteljahreshefte für Wirtschaftsforschung 82(4). 73–88.

Weber B. 2015. Bitcoin and the Legitimacy Crisis of Money. In: Cambridge Journal of Economics. Forthcoming. DOI 10.1093/cje/beu067.

Wingfield, N. 2013. Bitcoin Pursues the Mainstream. In: International New York Times. November 11.

Yermack, D. 2013. Is Bitcoin a Real Currency? NBER Working Paper 19747.