WSBI

The Global Voice of Savings and Retail Banking

Virtual currencies: passion, prospects and challenges

RETAIL

REGIONAL

RESPONSIBLE

World Savings and Retail Banking Institute - aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Bruxelles ▪ Tel: + 32 2 211 11 11 ▪ Fax: + 32 2 211 11 99
E-mail: first name.surname@wsbi-esbg.org ▪ Website: www.wsbi.org

Doc 0085/14
Vers.1.0

11 October 2014
NBI

Virtual currencies: passion, prospects and challenges

1- Executive summary

The purpose of this Working Paper is to provide a snapshot[1] on virtual currencies. It focuses on convertible, decentralised virtual currencies. Taking Bitcoin as proxy, it reviews its short history and early use cases as means of payment and speculative asset, finding these customer requirements supported by an ever increasing range of service providers, many of which attract venture capital with great ease. Whilst the actual economic footprint of virtual currencies remains very limited, there is a flurry of debates as to the impact a wider adoption could have notably on the economy and on monetary policy, as well as to whether the underlying technology – in essence a distributed, global ledger not requiring the intervention of a trusted third party - couldn't be leveraged more significantly to record transfers of assets other than money. As with any new development though, risks need to be assessed, whether inherent to a virtual currency's concept, architecture or technology, or inherent to understanding any given virtual currency. More generic risks must be acknowledged too which in the absence of consumer understanding and protection may have multiplication effects. In the face of these developments this Working Paper finds that regulatory responses across the world for the time being differ widely. There is little consensus so far with respect to the classification of virtual currency (money, currency, foreign currency, commodity?) and as to whether new legislation is required, and if so, for which part of the value chain. Some convergence however can be noted: the tax avoidance, fraud, money-laundering and terrorist financing potential of virtual currencies is a concern, and many regulators already cautioned consumers against perceived virtual currency-related risks.
From this snapshot several strategic findings should, for now, be highlighted. First the question as to whether to legislate or not, and what, and whom, deserves a coordinated, well-balanced approach on a global basis, yet an approach wary of unintended consequences on innovation and the ongoing digitalization of economies. Second there are at this point in time use cases that, notably because of uncertainty in consumer protection and the volatility of virtual currencies, should not be promoted; e.g. worker remittances, financial inclusion, store of value. Third the potential to apply the distributed, global ledger technology to the exchange and holding of assets other than money is still to be explored. Finally, a virtual currency-like technology platform could enable central banks to migrate cash from a physical to a digital form factor – thus significantly reducing the cost of cash to society.

2- Introduction

Maybe the Net has run out of good topics to debate, or maybe crypto-currency has become the door to today's every essential question on payment systems and monetary policy. At the same time whilst venture capital is being mobilized by virtual currency market participants, crypto-criminals are said to develop their own solutions and many Parliaments and central banks ponder the subject.

[1] An update of this Working Paper will be released in April 2015 to take into account any significant development.

Even week-end magazines with a large circulation[2] cover the story. Any discussion quickly pits two camps against each other: the tenants of "this is unstoppable", vs the "never ever" crowd.
Time has come to take stock. This Working Paper begins with the assumption that noise and investment may have a cause. Therefore it proposes a scope for the discussion, then looks into why virtual currency is there, prior to reviewing the technology and value chain of the more prominent virtual currency today. The Working Paper then assesses the risks triggered by virtual currencies, and provides an overview of how regulators across the world have begun to address the challenge. It concludes with a number of strategic take-aways.

3- Virtual currencies: definitions

To understand virtual currency, the current debate, the challenges and upcoming opportunities, it is useful to refresh what money means. It is widely accepted that there are 3 different functions of money[3]:

- Medium of exchange (in today's words: a means of payment): money is used as an intermediary in trade to avoid the inconveniences of a barter system, i.e. the need for a coincidence of wants between the 2 parties involved in the transaction;
- Unit of account: money acts as a standard numerical unit for the measurement of value and costs of goods, services, assets and liabilities;
- Store of value: money can be saved and retrieved in the future.

Money has been initially described as a "commodity few people would be likely to refuse in exchange for the produce of their industry[4]". The value of money as a medium of exchange then depends on individuals' expectations that it will be accepted by other people. Earlier monies – because of the metals they were made of - had a monetary as well as a non-monetary use and value, which facilitated broad acceptance. Generally, such acceptance was facilitated further when states made a money legal tender, i.e. legally valid for the payment of debts and to be accepted for that purpose when offered. Eventually most states suspended the redeemability of money in favour of "fiat" money, which has no non-monetary value (it is just paper, or - for coins - low value metal).

Fiat money thus is the opposite of commodity money. One academic[5] expands on this comparison and stresses that commodity money not only has a use other than medium of exchange but is naturally scarce, whilst fiat money is only an exchange medium which scarcity is contrived, meaning: contingent, i.e. a matter of policy (at times thus with a severe risk of mismanagement). Commodity money is vulnerable to supply shocks, e.g. changes in non-monetary demand, shocks that shift the base-money supply schedule. Selgin divides money into 4 categories, depending as to whether their scarcity is absolute or contingent, and whether they have, or have not a non-monetary use. Fiat money is characterised by contingent scarcity and no non-monetary use, whilst monies characterised by no non-monetary use and absolute scarcity are called "synthetic commodity". These distinctions could be usefully leveraged when virtual currencies expand.

A convergence of definitions of virtual currency can be noted. We will retain that virtual currency is "a digital representation of value[6] that can be digitally traded and functions as (1) a medium of

[2] The Sunday Times run a piece on Bitcoin on 2 March 2014: "Desperately seeking Satoshi"
[3] first defined by Aristotle, Nichomachean Ethics, Book V, and Politics, Book 1
[4] Adam Smith
[5] George Selgin – see References and acknowledgements at the end of this Working Paper
[6] Stressing that the very terminology of "currency" is misleading the European Banking Authority further defines Virtual Currencies as digital representation of value issued neither by a central bank nor a public authority, nor necessarily attached to a fiat currency, yet accepted by natural or legal persons as a means of payment.

exchange; and/or (2) a unit of account[7]; and/or (3) a store of value, but does not have legal tender status, and is neither issued nor guaranteed by any jurisdiction, functioning only by agreement within its community of users[8]". At this point in time, for virtual currencies, the focus would be mostly on the medium of exchange and store of value functions. Virtual currency differs from fiat currency (or: real currency, real money, national currency) in that a country's coin and paper money are designated as legal tender and circulate and are accepted as medium of exchange in the country of issuance. Virtual currency is distinct from e-money which is the digital representation of fiat currency – electronically transferring value that has legal tender. Unlike gold or silver virtual currencies have no non-monetary use or value – they're just bits of data. Over 200 different virtual currency schemes were reportedly in operation in mid-2014[9]. Bitcoin alternatives[10] ("altcoins") include Bitcloud, Coloured Coin, Dogecoin, Ethereum, JPMorgan, Klickex[11], Litecoin, Mastercoin, Mintchip, Realcoin, Ripple, Stellar, Zerocoin.

It becomes generally accepted as well that virtual currency can be divided into 2 "basic" types: non-convertible and convertible virtual currency. Non-convertible virtual currency is specific to a domain and under the rules of the issuer cannot be exchanged for fiat currency (however a secondary black market may enable the exchange of non-convertible virtual currency for fiat or another convertible virtual currency). Convertible virtual currency either has an equivalent value in fiat currency or acts as a substitute for fiat currency[12], and can be exchanged back and forth for fiat currency. "Convertible" is to be understood as a de facto convertibility – because a market exists – not an ex officio, guaranteed by law convertibility as with e.g. the gold standard.

The defining criteria is convertibility vs non-convertibility: if a currency is non-convertible, it automatically follows that it is centrally administered, if it is convertible it can be either centralized or decentralized. Whilst all non-convertible virtual currencies are by definition centrally-administered (i.e. issued by a central authority that establishes rules), convertible virtual currencies may be either centralised or decentralised. A centralised virtual currency is administered by a single authority that establishes the rules, maintains a central payment ledger, and has authority to redeem the currency. The exchange rate can be either floating (determined by market supply and demand) or pegged i.e. fixed by the single authority. Decentralised virtual currencies (also called "crypto-currencies" in the emerging literature) are distributed (i.e. where transactions are validated by a distributed proof-of-work system, with each transaction distributed among a network of participants who run the algorithm to validate the transaction), open-source, math-based peer-to-peer virtual currencies with no central administrative authority, no central monitoring nor oversight.

At times the term "digital currency" is used. The latter means a digital representation of either virtual currency or e-money. To avoid confusion only the terms "virtual currency" or "e-money" will be used from now on. Today, the most talked-about and documented virtual currency being

---

[7] The draft State of New York law ("Bitlicenses") defines virtual currency as "any type of digital unit that is used as a medium of exchange or a form of digitally stored value that is incorporated into payment system technology", including: centralised repository or administrator; decentralised with no repository or administrator; which may be obtained or created through computing or manufacturing effort; yet excluding in-game currency with no market or application outside, and digital units used in affinity and reward programs, and which can't be converted into fiat currency.

[8] E.g.: FATF Report Virtual Currencies, key definitions and potential AML/CFT risks, June 2014

[9] July 2014 European Banking Authority Opinion on virtual currencies

[10] which may or may not be active at the time of publishing this Working Paper. Note: the architecture of the one or the other alternative may differ from the Bitcoin architecture. Several alternatives are geared at improving on Bitcoin's transaction speed.

[11] An asset-backed crypto-currency

[12] FinCEN Guidance March 2013

Bitcoin, a convertible, decentralised virtual currency, this Working Paper will look into virtual currencies through the lenses of the Bitcoin incarnation (so to speak…).

4- Virtual currencies: supply and demand

Why do people create virtual currencies? Why do people look for virtual currencies? What do they wish to use them for, what benefits do they expect? What are the early, and the potential use cases?

In a famous 1999 interview Milton Friedman opined that "…the Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A, the way I can take a USD 20 bill and hand it over to you and then there is no record of where it came from". In essence the Internet would call for specific means of payment, free from government intervention.

Bitcoin: a short history, yet already 4 phases

The proper starting point to understand supply and demand would be the seminal 2008 paper[13] from the person (or: "group of persons") who allegedly invented Bitcoin. In essence the Bitcoin inceptor(s) designed a solution to address the conclusion that up to now "completely non-reversible transactions are not really possible". Existing payment systems[14] are built on the premise that for mainly consumer (payer) protection reasons each payment transaction should be reversible. This, the Bitcoin inceptor(s) propose, increases the need for trust and mediation throughout the value chain, burdening the payment system (again: see footnote 11) with costs and uncertainties, which ultimately set a floor for the value at which digital payments can be performed efficiently. So far these costs and uncertainties could only be avoided by paying in cash. The Bitcoin value proposition is that "a peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. … the main benefits are lost if a trusted third party is still required to prevent double-spending…[15]".

The requirement to prevent double-spending is important, because it is the root for the architecture of the Bitcoin system[16]. That architecture in turn is a response to the no-trusted third party requirement, i.e. a distributed, non-centrally administered network of independent nodes relying on cryptographic proof instead of legislated and supervised trust. It is these design characteristics, i.e. the non-centrally administered architecture and the distributed process applied to create bitcoins and enable each transaction, that – against the background of the 2008 financial crisis and mistrust of the financial sector - first caught the attention of romantics, libertarians and technology geeks alike and propelled Bitcoin to the most talked-about virtual currency. The anonymity feature[17] is a by-product of the "no trusted third party" design requirement but represents a valued add-on for crypto-libertarians, and is a key value proposition for the conduct of illicit (in the light of formal legislation) activities. As Bitcoin's visibility was fuelled by libertarians' noise and some traders' illicit deeds, speculators moved in, driving the value of a single Bitcoin to over USD 1.100. As this unfurled regulators in many jurisdictions felt compelled to take a position, and some react[18] to the phenomenon, fuelling the promise that one day Bitcoin & Co could become a legal marketplace,

[13] Nakamoto Satoshi, Bitcoin: a peer-to-peer electronic cash system, 2008
[14] In the wide acceptance of the term, i.e. including rules and regulations
[15] Abstract of the 2008 Nakamoto paper
[16] See Section 5 of this Working Paper
[17] Which has to be relativised – see Section 5 of this Working Paper
[18] Albeit in many, not necessaruily consistent ways : see Section 7 of this Working Paper

and thus opening the floodgates for "high street" companies to declare themselves as accepting (or: considering accepting) bitcoins.

How big is Bitcoin? By design no more than 21 million bitcoins will ever be put into circulation. Assuming the current rate of production remains constant this means that by 2040 no new bitcoins will be produced. Considering that a Bitcoin can be divided out to eight decimal places the potential stock of 21 million bitcoins can be divided into 2.000 trillion unique units. On 22 August 2014 slightly over 13 million had been created. Going exchange spot rates hovered slightly over USD 500, giving a (theoretical) market capitalisation just short of USD 7 billion. Daily trades are valued at about USD 40 million (with a peak day though of USD 500 million). To put figures in perspective, the real time gross settlement system of the euro ("TARGET2") sees daily averages of 1.900 billion.

Early use cases

The first Bitcoin "payment" reportedly took place in 2010 when a Florida programmer offered 10.000 bitcoins to anyone willing to deliver 2 Papa John's pizzas – the transaction was completed within a few days. The attraction during the technology-geek phase was clearly the open source, perceived democratic nature of the application, which allowed everybody to declare independence from government and the financial sector. This attraction was reinforced by the fact that transacting in bitcoins implied no (or very little) transaction fee, leading players to overlook the volatility risk and (when paying with bitcoins for the purchase of goods or services), the differences in consumer protection compared to another payment instrument (credit transfer, direct debit, credit card – although levels of consumer protection would be jurisdiction-dependent too). Generally the online commerce world is seen as the primary marketplace for payment with virtual currencies, but the "no/low fee" perception triggered quite a number of mentions for Bitcoin to displace money transfer operators for international worker remittances.

Now hardly a day goes by without a new acceptor and/or a new application being announced. But data on market impact remain very scarce. A random scan of announcements would lead to mention: MemoryDealers (a computer-parts reseller that in 2011 became the first company to accept bitcoins in exchange for "real-world" products), Bitcoin Store (an online electronics retailer only accepting Bitcoin transactions), Overstock.com[19], BitPesa (supporting remittances[20] to Kenya), SendMoney.ph (sending remittances to the Philippines), Braintree (the eBay subsidiary payment processor), a Google Glass payments app, YouTube, Google+, Tumblr, Newegg, 1-800 Flowers, Reed Jewellers, Expedia, Dish, Dell, Virgin Atlantic, TigerDirect,… Bitcoins are also discussed as a bridge currency, e.g. an opportunity for PayPal to open up in countries where it doesn't support the local currency (though also competing with PayPal, as there is no cost to move bitcoins between wallets, usually only a low ad valorem fee to convert Bitcoin back and forth into fiat currencies). A leveraging of this bridge currency positioning through a network of interconnected gateways could turn Bitcoin into the equivalent of an IP layer for payments.
Thus bitcoins today are used as means of payment, including micro-payments but also remittances[21] and higher ticket value payments, i.e. a mix of scenarios where payers care about, or would not care about consumer protection. By end 2014, it is forecast that there will be 8 million active Bitcoin wallets, and 100.000 merchants accepting Bitcoin. Reportedly bitcoins are also hoarded and traded by speculators who try to benefit from actual or expected valuation differences.

---

[19] In July 2014 Overstock reportedly was exploring the potential of the Bitcoin technology to create a decentralised exchange trading platform for corporate stocks issued as « crypto-securities ».
[20] A March 2014 Goldman-Sachs report claims that Bitcoin could save migrant workers over USD 43 billion in remittance fees
[21] On 26 June 2014 Western Union's CEO stated he would be open to Bitcoin once the currency is regulated.

The "customer requirements" sketched above are supported by an ever increasing range of service providers (which may or may not be active at the time of publishing this Working Paper):

- ATM services[22];
- Exchanges[23];
- Identity verification and authentication[24];
- Mining services[25];
- Processing[26];
- Platforms, allowing e.g. publishers and digital creators to monetize content through micropayments[27], providing online and in-person digital services[28], bringing the Bitcoin world to mobile devices[29];
- Software and application developers[30];
- Trading platforms[31];
- Wallet services[32];

The by no means exhaustive list of service providers in the footnote gives an indication as to how vibrant the "Bitcoin ecosystem" is in attracting both intellectual property[33] and investment[34].

Beyond current use cases

What does the future hold for virtual currencies? Of course what today are largely experiments need to be turned into large scale, successful business cases for issuers and providers, holders and acceptors. This does not prevent visions of where virtual currencies could go, by leveraging their very nature as well as the underlying technology, which could find application in non-payment related fields (e.g.: distributed registry of any asset).

Former US Treasury Secretary Larry Summers considers that the financial system is fraught with substantial inefficiency. Although heavily dependent on information technology it has not been disrupted by new technology as have for example the book or clothing distribution businesses. Whilst not seeing the virtual currency world as a libertarian paradise, Summers points to the potential contained in Bitcoin's breakthrough technology with its fast and low cost system for

---

[22] E.g. Lamassu, Robocoin, Skyhook

[23] E.g. artoBit, Asia NexGen, Bex.io, Bitbox, Bitcoil, Bitcoin To You, Bitstamp, BTC China, Coinflorr, Crypto-Currency Analytic, e-Curex, Korbit, Kraken.com, OKCoin, Vaurum – including venues for derivative contracts e.g. Icbit.se

[24] E.g. VerifyBTC

[25] E.g. Alydian, BitFury, CoinTerra, MegaBigPower

[26] E.g. Bitinstant, Bitpagos, BitPay (who recently also launched a Facebook app allowing users to exchange the crypto-currency), Coinbase, Digital River, Global Payments, Stripe, Xapo, ZipZap (opening up 28.000 merchant locations in the UK)

[27] E.g. Bitwall

[28] E.g. Circle, Delta Financial (who annunced interest-bearing accounts for Bitcoin deposits and lending to currency tarders with up to five times leverage), BTCJam (a « global » peer-to-peer lender of Bitcoins)

[29] E.g. ChangeTip, Gliph

[30] E.g. SmartMetric (a biometric, NFC-enabled card for storing and making P2P transfers in bitcoins), Mint (the Intuit-owned money management app lets users view their bitcoin transaction alongside traditional financial accounts), Switchless

[31] E.g. Buttercoin, Coinsetter, ItBit, TruCoin

[32] E.g. Kraken.com, MultiBit, Trezor, and Elliptic (a UK startup proposing an insured bitcoin storage service), QuickCoin (integrating a Bitcoin wallet app with Facebook)

[33] For example BitPay is using part of the procedds of its USD 30 million funding round to hire staff from Visa, PayPal and Jumio

[34] As of end of June 2014 USD 150 million of venture capital had flowed into virtual currencies. The total venture capital investment in crypto-currency startups to-date amounts to USD 240 million.

confirming transactions as a better answer than the current multi-layered system for domestic and global fund transfers. Similarly credit card fraud can only be mitigated by enormous investment, whereas Bitcoin as a push system requires neither authorization check, nor any need for the merchant to collect consumer data. Finally there's a natural desire to have secure global stores of value – a topic to which virtual currencies may provide an efficient response.

As to Selgin[35] he sees potential opportunities for monetary policy using money based on a synthetic commodity like Bitcoin. If economists and central bankers could agree upon optimal monetary rules, then it might be possible to design a digital currency that carries out these rules automatically. The potential is there to supply the foundation for monetary regimes that do not require oversight by any monetary author yet are capable of providing such changes in the money stock as may be needed to achieve a high degree of macroeconomic stability. Whilst this may not sound appealing to countries with stable currencies, some say that citizens from Argentina or Zimbabwe would have benefited from adopting Bitcoin as their nation's currency.

OECD also believes that digital transfer technology could play highly-socially useful roles. EBA sees a range of benefits that could be accrued such as security of personal data or limited interference of public authorities but stresses that any benefit is relative and fosters drawbacks of its own. In particular the often quoted enabler of financial inclusion is viewed as a strictly conceptual, not practical potential benefit. At this point in time it is certainly the Bitcoin technology that gathers the least contested endorsements as potential for the future, "including next generation securities custody systems or retail payment solutions without an expensive point-of-sale infrastructure, a global ledger which could be an internet-scale open platform for value exchange not only facilitating new systems of record but also the integration of devices on the Internet of Things with the real economy, maybe even replacing some types of legal contracts[36]".

5- Virtual currencies: the technology and value chain

a) The technology

The Bitcoin process can be summarised[37][38] as follows:

- Each coin is a chain of electronic signatures, with each payer digitally signing the hash of the previous transaction and transferring the public key to the payee (who can thus verify the chain of signatures to verify the chain of ownership).
- The payee must be certain that the chain received is unique. In the absence of a trusted third party this is achieved by publishing all transactions, and having all participating, yet independent servers (the peer-to-peer network of nodes) agree ("vote") that the said transaction is unique, every hash being time stamped.
- A "proof-of-work[39]" system (in essence, a process that makes it both computationally costly for network users to validate transactions and rewards them for trying to help validating) is required to implement the distributed timestamp server on a peer-to-peer basis. Any prior block could thus only be changed by changing all subsequent blocks – which would not go unnoticed, with all nodes holding one vote each.

---

[35] See References and acknwoledgements

[36] IBM Academy of Technology, Bitcoin and Cryptocurrencies: a Critical Insight, 2014

[37] For a more comprehensive description, see i.a. S. Nakamoto : Bitcoin : a peer-to-peer electronic cash system

[38] An interesting read also is a December 2013 post by Michael Nielsen : http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

[39] See A. Back, Hashcash : a denial of service counter-measure, August 2002

- The standard sequence is as follows:
- New transactions (either creation or transfer of bitcoins) are notified to all nodes (generally in a 10 minute cycle);
- Each node collect new transactions into a block, and works out a "difficult" proof-of-work for its block;
- When a proof-of-work is found it is notified to all nodes;
- Nodes accept the block only if all transactions it contains are valid and not already spent;
- Nodes express acceptance by working on the next block, using the hash of the accepted block as the previous hash.
- Payment verification is possible though without running a full network node, a user just keeping a copy of the block headers of the longest proof-of-value chain.
- "Transactions" can be both combined and split with either a single input from a larger previous transaction, or multiple inputs containing smaller amounts, and at most 2 outputs (one for the payment, and one for returning the change to the sender), to avoid making a separate transaction for every cent in a transfer.
- Privacy is maintained by keeping public keys anonymous. It is recommended that a new key pair be used for each transaction to keep them from being linked to a single owner.

As an aside, one may remark that this distributed methodology of verifying the authenticity of a Bitcoin is quite similar to banknotes, where it is up to each acceptor to ensure (by checking a number of features) that the banknote is genuine (of course, for banknotes there are ultimately central authorities who do so too).

Upon registration Bitcoin users are given a unique address and a computer file in which to store their bitcoins (their digital wallet). The transfer of bitcoins from seller to buyer is conducted through this wallet, which integrates with the network through a node, enabling the publication of the transaction on the network. This digital wallet is identified by public keys, which can be accessed/unlocked using one's private keys (the latter have to be kept secret, the former are corresponding sequences of letters/numbers that can be seen by everybody on the "blockchain"). Private keys can be stored by the wallet owner or on their behalf by the wallet provider. Sending bitcoins to other users requires knowing just their address. Each node runs an open source protocol which enables the generation of new bitcoins and facilitates the creation of a public registry (the "blockchain") of past transactions. The safety and integrity of this ledger is ensured by a network of conceptually mutually distrustful parties (the "miners" establishing and maintaining the nodes) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (the "block reward"). Each Bitcoin has a unique serial number, which permits tracking and recording of the transaction history of that Bitcoin in the blockchain.

The verification process described above implies a scalability challenge: more and more computing power is required as the number of transactions grow, thus verification becomes more and more costly, intuitively leading miners to demand more and more rewards, over time leading to the decreasing efficiency of Bitcoin production and usage. The recognition of this challenge generates a growing interest in developing alternative, potentially more efficient proof methods, such as systems based on "proof-of-stake". E.g. the Ripple[40] protocol is said to solve the Bitcoin problem by having the equivalent of a blockchain as a public ledger shared by a unique node list (UNL) of members' servers. Any new set of transactions is a "candidate set" distributed to all external servers. When a set of iterations matches the transactions in the current candidate set and a consensus of 80% of server notes reaches is declared, a new last closed ledger forms and the process starts again. The procedure is said to improve on the electricity cost of mining. Another alternative is claimed to be provided by CoinBau AG[41] who claims to have developed software which finds the lowest possible voltage for individual chips within bitcoin mining farms, reducing by half the energy needed.

[40] See : ripple.com

[41] See: coinbau.com

b) The value chain

The key components of the Bitcoin value chain are:

- Bitcoin protocol and software: this is open-source, freely available to users and developers. Any developer can review the code and make their own amendments, however no new version can be forced onto the market without all users accepting it.
- Miners are conceptually independent persons who each establish, operate and maintain a server to run an algorithm which allows to validate Bitcoin transactions. In doing so they earn a fee, in the form of bitcoins or a portion thereof, and any transaction fee voluntarily offered by parties to a given transaction.
- Users download a software application (the wallet) to buy and sell bitcoins. (In addition to mining) bitcoins can be obtained by exchanging a fiat currency via an exchange or a payment processor, accepting bitcoins when selling goods or services, or using a Bitcoin enabled "ATM". Each wallet has a distinct alphanumeric address. Wallets can be stored either online or offline.
- Merchants (either online or in actual stores) accept bitcoins as payment for goods or services.
- Exchanges accept fiat or another virtual currency and deliver a virtual currency, and convert back. They generally accept a range of payment instruments, including cash.

The Bitcoin ecosystem is growing, with software and application providers as well as processors providing e.g. wallet services, alongside anonymisers providing tools and services designed to obscure the source of a Bitcoin transaction and further facilitate anonymity, or mixers bulking transactions to make them look as if they were sent from another address, …

6- Virtual currencies: a first assessment of risks

a) Risks inherent to the Bitcoin concept, architecture and technology

- Bitcoin is promoted as a not centrally administered system, yet there – necessarily – is a (small) team responsible for maintaining, debugging and otherwise improving the Bitcoin software. This is a de facto "central bank" which could influence the speed and/or security of Bitcoin production and functioning, and/or the cost of production and/or functioning[42]. That every user has to consent to a new software release by downloading it on one side mitigates the governance risk posed by the central maintenance team, on the other is a challenge from a system perspective to the timely implementation of necessary changes.
- Bitcoin is based on a distributed system, but a number of miners could collude. A collective gathering over 50% of the miners at one point in time would have the ability to confirm all Bitcoin transactions on their own, thus jeopardising the transactions' reliability by sending out false confirmations, reversing the direction of transactions or blocking them[43].
- The anonymity feature permits the expansion of socially unacceptable activities (illicit trading, tax evasion, money laundering, terrorist financing). The jury is still open as to

[42] An example is the «transaction malleability» issue (see also Section 6 c) of thsi Working Paper). Malleability can be described as a small window in which tarnasction ID's can be reanmed befor ebeing confirmed in teh blockchain. Apparently the issue had been knwon by some in the Bitcoin community since 2011, yet only came to light when Mt.Gox defaulted. Bitcoin promoters (e.g. G. Andresen) say that « any company dealing with Bitcoin transactions and having coded their own wallet software should responsibly prepare for this possibility and include in their software a way to validate tarnsaction ID's ».

[43] An issue highlighted in a November 2013 Cornell University research paper: "Majority is not enough: bitcoin mining is vulnerable". E.g. in January 2014 a mining pool grew to controlling cca 45% of teh network's processing power, and agreed to reduce its activity after other miners expressed their concern.

whether such expansion is actually just a shift[44] (e.g. from cash to virtual currency), or whether the total "market" for illicit activities expands. It must be noted though that Bitcoin transactions, whilst technically anonymous insofar as no identity verification of participants in the value chain takes place, are traceable (all addresses having impacted a coin are recorded in the blockchain). As the blockchain ledger is public, linking a person to a Bitcoin address would provide full transparency to all activity that ever happened on that address. A better word would be to define Bitcoin as "pseudonymous".

b) Risks inherent to understanding Bitcoin

Although Bitcoin is a new arrival notably on the payments scene it is often described in particular by providers by using terminology which is very close to existing products and services and thus may under inform, misinform, and/or create confusion, in particular for consumers.

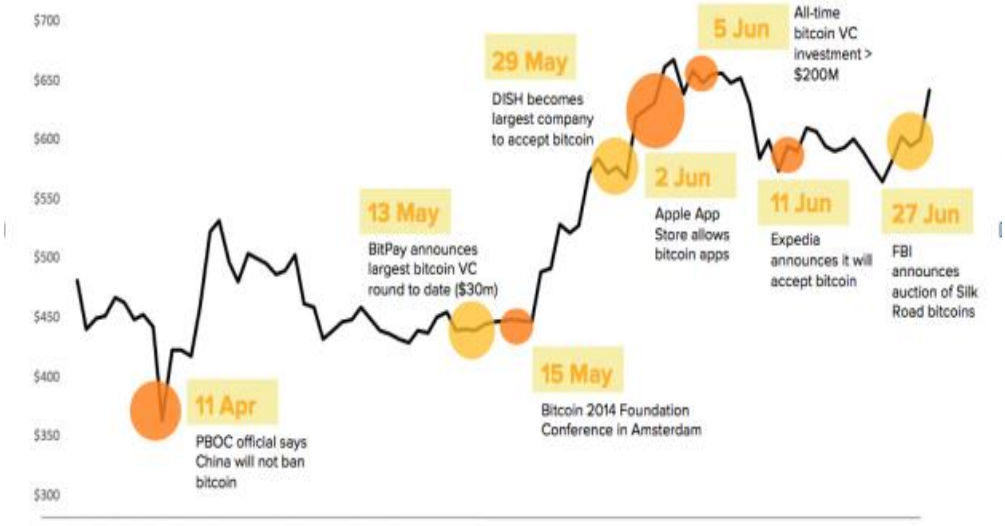
- "Currency" is one of these terms. The less-informed consumer may not dwell on the distinction between fiat and virtual currency. Yet that distinction triggers completely different legal systems to apply throughout the value chain – whether a virtual currency is used as means of payment or for investment.
- A case in point is the "virtual currency account" that a consumer will be invited to open before transacting in bitcoins. In spite of the term "account", no deposit insurance scheme is available. Bitcoins in that account are as safe as not only the credit standing of the account servicer, but also the security the latter mobilises, and how safe the consumer keeps his/her private keys.
- The value of Bitcoin holdings is also subject to significant variations. The chart below summarises the evolution of the USD/BTC "exchange rate" since January 2013:

Monday 18 August 2014

The volatility is significant. The value of Bitcoin has been impacted by the demise in February of the main exchange (Mt.Gox), due to fraud. The overriding factor however is that Bitcoin value is today driven by speculation, not by government policy. Its role as (even temporary, for those making or receiving payments) store of value is hence questionable.

The table below lists the main events which could explain the volatility of Bitcoin in the 2nd quarter of 2014:

[44] It has been reported that cybercrooks – concerned with the level of anonymity offered by Bitcoin - would be shifting to cybercrime forum-specific currencies (e.g. Perfect Money, Musd, United Payment System) in order to safely transact within their own community



Source: CoinDesk Bitcoin Price Index daily closing price (taken at 00:00 UTC)

- A further opportunity for misunderstanding and hence loss for the consumer is the irreversibility of a Bitcoin transaction. Contrary to a number of payment instruments in a number of jurisdictions each and every peer-to-peer transaction is final (as with cash). A payer will probably not care when sending a remittance, giving a tip or sending to a charity. Yet there are many other instances where payers would expect that their payment is conditional to the merchant's performance in delivering a good or service.
- Price transparency when buying goods/services is another issue. Prices quoted in non-fiat currencies may – because of the volatility explained above – not always translate into a stable cost in a fiat currency, thus preventing comparability. Contractual protections may also differ.
- Finally consumers need to understand that theft or disappearance (because of technical failure, or provider incident) of their Bitcoin wallet is equivalent to losing a physical wallet: there is no redress.

The above risks would of course not apply to traders and professional investors.

c) <u>More generic risks whose consequences, though, may be increased in the absence of consumer understanding and protection</u>

- The "system" may become prey to software bugs, triggering in the absence of a central authority panic amongst account holders. Their reactions could spill over to their holdings in fiat currency.
- The security of the "system" wholly rests on cryptography. The robustness of the keys used could be challenged by quantum engineering.
- There could be a breach of security of a service built on top of Bitcoin (this is what happened notably in the Mt.Gox event, which software allegedly failed to address the "malleability" – i.e. the possibility to alter a hash and informing the issuing service that the transaction did not proceed - of unconfirmed transactions).
- There could be transaction processing errors (i.e. a misrouted transaction).
- As any internet-based system it is open to fraud, hacks, and scams. There are allegedly over 100 malware families targeting Bitcoin, the most common type being the wallet stealer,

searching for well-known wallet software key storage locations, and stealing credentials from Web-based wallets[45][46].

- Finally, there is no number to call when something goes wrong.

Do these risks at this stage represent a threat to society? Would these risks warrant an intervention of the regulator? On one side, considering a current (theoretical) market capitalization of Bitcoin of USD 7 billion (the annual GDP of a country like Kosovo), societal risk would seem limited. On the other hand, considering that some 5 million people would already hold a Bitcoin, a question mark hangs over the potential spill over to fiat currency systems of any serious, widespread mishap with a virtual currency system.

What could the objectives for regulators be against that background? Certainly maintaining public confidence in payment systems as well as payment instruments in fiat currency is important, no contagion effect should be allowed. At this point in time this would be best achieved by educating the public at large as to the characteristics of virtual currency and their implications under various scenarios. Should Bitcoin or another virtual currency evolve into a more widely used one then it would seem that guidance could be found in the April 2012 BIS/ IOSCO Principles for Financial Market Infrastructures: many of these principles would well apply to an important virtual currency system.
Yet it would appear that policymakers and regulators may have to consider dimensions beyond sheer payment systems policy. How can one assess whether the resources currently ploughed into virtual currencies are justified? What will be the impacts on competition of either laissez-faire or intervention? Isn't there a risk of deepening the digital divide, instead of fostering financial inclusion as touted by some? What if volatility began to create lasting multiplier effects, in other words a virtual currency leverage? Couldn't (some of) the underlying technology be transposed to make existing payment and transfer of asset systems more efficient? And what about Selgin's apparently lofty ideas with respect to monetary policy?
Fiat currencies are certainly not exempt of uncertainty. But virtual currencies present regulators with a novel challenge. Whether and how they intervene or ignore them will send ripple waves throughout the next phase of financial innovation. The next Section in this Working Paper provides an overview as to how regulators across the world chose to respond so far.

7- Virtual currencies: a snapshot of the emerging legislation and regulation

This section provides a best effort overview as per August 2014 of positions taken by regulators.

Financial Action Task Force
The June 2014 Report describes 3 law enforcement actions involving virtual currency (Liberty Reserve, Silk Road, Western Express International) which by default define a perimeter of non-permissible activity. These cases combine the operation of unregistered money transfer businesses, money laundering, and disguising user addresses and/or making them even more difficult to trace.

[45] As advanced malware can bypass even one-time PIN protections through the creation of a second hidden brwoser window, alternative wallets develop that protect against theft by malware via a split arrangement for key storage – with one computer disconnected from any network running a copy of the software and holding the private key that can sign transactions, while a second PC connected to the Internet holds only a master public key, which addresses belong to the offline wallet.
[46] E.g. the Bitcoin Foundation warned in November 2013 that a component of Android responsible for generating secure random numbers contained critical weaknesses, that render all Android wallets generated to date vulnerable to theft » - an issue which could be addressed by key rotation, i.e. generating a new address with a repaired random number generator, then sending all funds in the wallet back to the user him/herself.

United States

In March 2013, the Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") issued a Guidance on the "Application of FinCEN's Regulations to persons administering, exchanging or using virtual currencies", more precisely of the applicability of the Bank Secrecy Act to persons creating, obtaining, distributing, exchanging, accepting or transmitting virtual currencies. A user obtains virtual currency to purchase goods or services, an exchanger exchanges virtual currency for fiat currency as a business, an administrator issues virtual currency as a business and has authority to redeem it. It is clarified that a user of virtual currency is not a money service business under FinCEN, thus not subject to registration, reporting, and recordkeeping – because such activity does not fit the definition of "money transmission services". A contrario an administrator or exchange is a money transmitter under FinCEN (that definition not differentiating between virtual and fiat currencies). As a consequence brokers and dealers n e-currencies and e-precious metals are money transmitters whenever a) the transfer of funds between a customer and a third party occurs by permitting a third party to fund the customer's account, b) there is a transfer of value from a customer's currency or commodity position to the account of another customer, c) a customer's currency or commodity position is closed out by the transfer of proceeds to a third party. Equally the administrator of a convertible virtual currency centralised repository is a money transmitter when transfer of value between persons or locations is allowed. The exchanger's activity may take the form of either accepting fiat currency or its equivalent from a user and transmitting it to fund the user's convertible virtual currency account with the administrator, or performing a de facto not completely transparent sale of convertible virtual currency – both constitute under most scenarios money transmission on the part of the exchanger. Finally a person creating units of a decentralised convertible virtual currency and using it to purchase goods or services is not subject to money transmission regulation, whereas any person creating such units and selling them to another person for fiat currency is a money transmitter.

In November 2013, a Senate Committee held hearings on Bitcoin.

In January 2014, FinCEN issued an administrative ruling on virtual currency mining operations. The ruling clarifies that the "label applied to a particular process of obtaining a virtual currency is not material to the legal characterization under the Bank Secrecy Act of the process or the person engaging in the process to send that virtual currency or its equivalent value to any other person or place". What is material is what the person uses the convertible virtual currency for, and for whose benefit. Thus a company mining bitcoins is a user, not a money transmitter, provided that these are used to a) purchase goods or services or pay debts or remunerate owners, or b) purchase fiat currency or another convertible virtual currency to make the above payments or investing for the company's own purpose.

In January 2014, FinCEN also issued an administrative ruling on virtual currency software development and certain investment activity in response to a company's query regarding a periodic investment in convertible virtual currency and the production and distribution of software to facilitate the company's purchase of virtual currency for its own investment. The production and distribution of software even to facilitate the purchase or sale of virtual currency does in itself not constitute money transmission. Equally, provided the company invests in a convertible virtual currency for its own account and realises the value of its investment, it acts as a user and not a money transmitter.

In February 2014, the Federal Reserve Bank Chair replied to a US Senator – who claimed Bitcoin was disruptive to the economy – that "To the best of my knowledge there is no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate. So the Federal Reserve doesn't have authority to supervise or regulate Bitcoin in any way…. […] but certainly it would be appropriate for Congress to ask questions about what the right legal structure would be for digital currencies".

In June 2014, the State of New York initiated procedures for the regulation of virtual currencies ("Bitlicenses"). The proposal defines virtual currency as well as what constitutes virtual currency business activity: to receive virtual currency for transmission or transmitting the same, to secure,

store, hold or maintain custody or control of virtual currency on behalf of others, to perform retail conversion services (from virtual to fiat currency and conversely, and from one virtual currency to another virtual currency), to buy and sell virtual currency as a customer business, to control, administer or issue virtual currency. Such business would have to comply with all federal and state laws and jurisdictions, be subject to a compliance program, capital and custodial requirements, maintain books and records for 10 years, be subject to reporting requirements and an AML program, maintain a cyber-security program, maintain and enforce written policies including with respect to anti-fraud, AML, cyber-security, and privacy and information security. Such businesses will be subject to ongoing supervision.
The New York State regulator also started to accept virtual currency exchange applications, "the formal commencement of a regulatory process".
The May 2013 GAO Report did not formally classify bitcoins, but described them as akin to virtual property. The Internal Revenue Service considers bitcoins "taxable property", with any profits from holding or exchanging bitcoins subject to the capital gains tax. Virtual currency held for investment will be treated as capital gains, with the top long term rate set at 20% compared to the top ordinary income-tax rate of 39.6%.
The Texas Banking Department in April 2014 released a Supervisory Memorandum providing an interpretation of Texas laws on currency exchange and money transmission. The Memorandum concludes that "because neither centralized virtual currencies nor crypto currencies are coin and paper money issued by the government of a country, they cannot be considered currencies under the Texas currency exchange statute". This implies that no money transmission can occur in a transaction that does not involve fiat currency. Conversely the exchange of fiat currency for crypto-currency by an intermediary between 2 other parties is money transmission. Where ATMs are concerned there is no money transmission provided the machine never involves a third party.
In May 2014, the US Department of Defense commissioned the Combatting Terrorism Technical Support Office with investigating whether Bitcoin could be converted into a potential terrorist threat.
The June 2014 Clearing House/ICBA paper on "Virtual currency: risks and regulation" draws the parallel between Bitcoin "credentials" (i.e. Bitcoin addresses and keys) and prepaid cards, implying that such credentials would thus fall under US Regulations E and II – although they lack the consumer protection of debit card and payroll card transactions – which could soon be extended to prepaid cards. The same paper argues that cross-border Bitcoin payments could fall under the Consumer Financial Protection Bureau's Remittance Transfer Rule. The paper finally points out that regardless as to whether bitcoins constitute securities, the Securities and Exchange Commission has regulatory and enforcement authority with respect to Bitcoin investment programs.
The US Securities and Exchange Commission issued a warning to investors that virtual currencies are a risky business leaving them open to fraud.
The Commodity Futures Trading Commission (CFTC) has not yet determined whether bitcoins constitute commodities – although it is reported to investigate the topic. It could argue that Bitcoin is a commodity under US law, subject to the CFTC's rules against manipulation and fraud.
In June 2014, California repealed a previous law prohibiting commerce using anything but US currency. Whether and how virtual currencies will be regulated is however now left to the California Department of Business Oversight.

Australia
End of June 2014 the Australian Tax Office delayed a much anticipated ruling on Bitcoin, leaving in limbo the question of whether Bitcoin is money or property, and the tax statute of businesses accepting it. It would appear that the ATO is mainly concerned by the use of virtual currencies as means of tax avoidance.
The Reserve Bank of Australia stated in December 2013 that Bitcoin had not caused any material problem "yet", although speculators should be conscious of risks. There is nothing in Australian legislation preventing individuals to hold or transact in other currencies, including virtual currencies.

In April 2014 the Reserve Bank issued a briefing in which Bitcoin is seen as posing a limited risk to the country's payment system and the Bitcoin transaction conformation method is described as an inefficient use of resources.

Brazil
Law No. 12.865 recognizes the possibility for electronic currencies, including Bitcoin, to be used. The focus of the law is mobile payments, covering the creation of electronic currencies as an aside. The distinction made between e-money and virtual currency is not that clear.

Canada
In November 2013 the Canada Revenue Agency issues a news release stating that any gains or losses from trading a digital currency would be considered taxable income or capital for the taxpayer. Revenue Canada issued a statement by which it considers bitcoins to be simple goods exchanged under a barter system – thus retailers have to declare revenues from transactions for which they accept Bitcoin. Profits or losses from bitcoins bought or sold for investment or speculation are considered capital gains or losses and taxed as such.
The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) indicated to Canadian Bitcoin exchanges that they were not considered "money service businesses" and thus exempt from money laundering legislation.
The Federal Government however announced an intention to strengthen AML/CTF legislation to better address emerging risks including those associated with virtual currencies. In June 2014, the Parliament passed a bill classifying companies dealing in virtual currencies as "money services businesses" subject to record-keeping, verification procedures, suspicious transaction reporting and registration requirements. Financial institutions are banned from offering services to non-registered companies. Virtual currency companies from outside Canada serving Canadians will have to comply with the same requirements.

European Banking Authority (EBA)
The EBA published on 4 July 2014 its Opinion on Virtual Currencies. This Opinion follows on the public warning issued by the EBA on 13 September 2013 to consumers that Virtual Currencies are not regulated and that as a consequence their risks are not mitigated. To answer the remaining question as to whether Virtual Currencies should or can be regulated – which becomes necessary as national jurisdictions both within and beyond the European Union begin to take divergent approaches - the EBA carried out an additional assessment in early 2014. The EBA opines that an adequate mitigation of the no less than 70 virtual currency-related risks it identifies would require establishing a substantial regulatory and legal framework, which would be a long term endeavour. However, given the spread of Virtual Currency initiatives (the EBA estimates that some 200 Virtual Currency "schemes" currently exist, even though actual transaction volumes and values – which themselves are difficult to assess in the absence of any monitoring or reporting - remain extremely marginal), regarding the near term the EBA discourages payment service providers to buy, hold and/or sell Virtual Currencies. The EBA furthermore recommends that interfaces between conventional and Virtual Currencies become "obliged entities" under the EU AML Directive. This would allow Virtual Currency schemes to develop outside the financial sector whilst protecting the latter.

European Central Bank
An October 2012 Report analyses i.a. the legal status of Bitcoin under existing EU legislation, in particular the 2009 E-money Directive, concluding that Bitcoin meets 2 of the 3 criteria set in the Directive regarding e-money: it is about electronic storage, and it is accepted as a means of payment by legal or natural persons other than the issue – however the 2nd criteria ("issuance upon receipt of

funds") is not complied with[47]. The report further states that "in the current situation" virtual currencies do not pose a risk to price stability and cannot jeopardise financial stability, are a challenge for authorities due to their potential for illicit activities, and fall within central banks' responsibility as a result of characteristics shared with payment systems.
In a March 2014 ECB Executive Board Member Y. Meersch stated that virtual currencies are too small to have an impact on retail payments and central banks yet are interesting phenomena that should neither be ignored nor dismissed. He pointed out that user risk is more prominent in speculative investments than in payments.

European Commission
On its Website (http://ec.europa.eu/economy_finance/euro/cash/legal_tender) the Commission emphasizes that, although in the euro area only the euro has the status of legal tender, "contractual parties are free to agree to use in transactions other official foreign currencies with legal tender status in the state of issuance, e.g. the Pound Sterling or the US Dollar. The same applies to privately issued money like local exchange trading systems (e.g. voucher-based payment systems in certain communities) or virtual currency schemes (e.g. Bitcoin). […] these forms of private money can be considered as economic assets. Private money transactions and business related to them are subject to the general rules of commodity trade such as taxation law, business law, anti-money laundering law or others."

Austria
In response to parliamentary questions two Austrian ministers provided guidance as to Bitcoin's treatment as financial instrument and from a tax perspective. The Finance minister confirmed the position of the Financial Market Authority that Bitcoin is not a tradable asset. Regarding tax treatment, Bitcoin holdings sold within a year of acquisition are subject to capital gains tax, holdings held over a year and then sold are subject to government sales tax. Transactions made by miners are subject to VAT. Some ambiguity as to the classification of Bitcoin was entertained by the minister for science, research and economy when he referred to the German position classifying Bitcoin as a "unit of account".

Denmark
The Financial Services Authority does not recognise Bitcoin as a currency yet it will not regulate Bitcoin usage. Any Bitcoin-related activity is not covered under the current financial regulation. Bitcoin should be treated as an electronic service and related earnings should be taxable – however the Danish Tax Authority has not issued any specific guidance in this respect so far.

Finland
Virtual currencies are regulated as commodities. Rules on taxation of capital gains apply when bitcoins are transferred to another currency.

France
Banque de France in December 2013 released a report warning about the dangers linked to virtual currencies. The report suggests that conversion between virtual currencies and fiat currencies is a payment service, which may only be performed by regulated institutions. The report stresses the absence of reimbursement guaranty, the inherently speculative concept, the absence of liquidity or price guaranty of the trading platforms, and the potential of leveraging anonymity to circumvent AML/CTF obligations.
In July 2014 French police busted an illicit exchange platform that had processed some 2.750 transactions (asking for commissions ranging from 35 to 50%) and confiscated about 400 bitcoins.

[47] In a June 2013 presentation to the World Bank's Global Forum on Law, Justice and Development an ECB official however stated that Bitcoin does not meet any of the functions of money

The same day the French Ministry of Finance announced an intent to impose identity checks for clients of Bitcoin accepting merchants, to impose a value ceiling on Bitcoin payments, and to tax capital gains realised with bitcoins.

Germany
BaFin (the Federal Financial Supervisory Authority) issued a communication on Bitcoin in December 2013. Bitcoins are considered as units of value i.e. financial instruments in the meaning of the German Banking Act (having the function of private means of payment within private trading exchangers, or being substitute currencies that are used as a means of payment in multilateral trading transactions based on agreements under private law). They are neither currency, nor legal tender, nor e-money in the meaning of the German Payment Services Supervision Act. Neither using bitcoins for payment, nor mining them, would trigger any licensing requirement. Yet purchasing or selling them on behalf of others on a commercial scale (as Principal Broking Service, Multilateral Trading System, Investment and Contract Broking, and/or Proprietary Trading) would require a license under the German Banking Act – the same applying to "mining pools".
The Federal Ministry of Finance opined that value added tax could apply to Bitcoin transfers.

Ireland
In July 2014 an Irish Central Bank official at a conference acknowledged that "virtual currencies pose new challenges to central bank functions". He suggested that virtual currency players should not assume that all their actions will fall under existing regulation, although regulation would not necessarily be needed to suppress or control a virtual currency, but rather to support the unknown innovations resulting from the technology's wider use. Should virtual currencies permeate economic activity, they would be likely to profoundly impact financial institutions from an operational perspective and their regulatory risk profile. Virtual currencies would also challenge the statistical measurement of economic activity, and the way central banks calibrate policy, exchange rates and the price of credit. "The co-existence of e.g. a euro-denominated economy and a virtual currency economy raises the prospect of an internal balance of payments between 2 sub-economies where suppliers may prefer one currency over another as a means of payment (for different goods and services)".

Italy
In June 2014, the Italian government implemented a preliminary set of rules for Bitcoin, similar to the regulations applicable to fiat currency. Bitcoin transactions over the equivalent of EUR 1.000,00 must be traceable.

The Netherlands
The Ministry of Finance indicated that a change in e-money legislation to recognise virtual currencies was unlikely at this point in time given the limited scope, relatively low level of acceptance and limited relationship to the real economy.
The Central Bank warned both financial institutions and consumers to be wary. The Central Bank is concerned about integrity risks to financial institutions and issues surrounding anonymity and AML rules. The Central Bank indicated it will assess the degree to which institutions involved with virtual currencies control and/or manage related integrity risks. Controls should involve effective measures with respect to client acceptance and the monitoring of new innovative suppliers. The Central Bank also stressed that virtual currencies such as Bitcoin are unlikely to replace the current financial system and money as we know it.

Norway
Bitcoin is not considered a currency. The tax authorities consider it a taxable asset.

Sweden

Virtual currencies are taxed as assets of the same class as fine art.
End June 2014 the Swedish Central Bank issued a commentary on virtual currencies. It highlights the difficulty in gathering statistics about the use of virtual currencies in Sweden (noting the absence of data on transactions between private persons), yet sees the market as being very limited both in terms of number of transactions, users and value. It opines that virtual currencies may be better suited for micropayments via websites.

Switzerland
In June 2014 the Swiss Financial Market Supervisory Authority banned the launch of a Bitcoin ATM in Zürich by a company called Bitcoin Suisse AG. The Swiss Parliament is considering treating Bitcoin as foreign currency, which could lead to ATM services being re-opened. A May 2014 government report separately concluded that paying workers in virtual currency is illegal – although paying bonuses or other compensations would not be so. End of June 2014 a Federal Council report on virtual currencies stated that these could be regulated without adding new provisions to existing law. Existing legislative acts should apply to businesses conducting transactions in virtual currency when these are considered deposits.

United Kingdom
Her Majesty's Revenue and Customs decided in February 2014 not to levy a 20% value added tax on virtual currency transactions.
In August 2014, the UK Chancellor announced the launch of a review into the potential of virtual currencies as part of a bid to turn the country into the "fintech capital" of the world. The review will investigate the role regulation could play in making it attractive for virtual currency firms to establish in the UK.

China
The government and Central Bank have prohibited banks and payment institutions from undertaking commercial operations with bitcoins (Bitcoin trading accounts had to be closed by 15 April 2014) – although individuals remain free to do so. The December 2013 "notice on Precautions against the Risks of Bitcoins" defines the virtual currency as a "virtual commodity", which should not be circulated or used as a currency.

India
The June 2013 financial stability report of the Reserve Bank of India states that "The unregulated link between virtual currency (if permitted), and traditional currency with a legal tender status poses challenges as the complete control over the differently denominated virtual currency is given to its issuer, who governs the scheme and manages the supply of money at will". The Reserve Bank later cautioned users, holders and traders of virtual currencies including bitcoins about the potential financial, operational, legal, customer protection and security related risks that they are exposing themselves to. The largest Indian Bitcoin platform suspended its operations following the RBI notice, and the offices hosting that platform were raided by the Enforcement Directorate.
Besides that there is so far no explicit regulation allowing, restricting or banning virtual currencies.

Japan
In March 2014 Japan's government stated that Bitcoin isn't a currency or a financial product and will be treated like other goods or services. The Prime Minister's ruling party, the Liberal Democratic Party, called on companies in the crypto-currency business to establish their own governing body, saying that no specific government agency should be assigned to oversee the industry to avoid players getting stuck in red tape.

Russia
The law stipulates that the rouble is the exclusive method of payment and that no other monetary unit can be introduced. This makes the use of virtual currencies potentially illegal, even for individuals.

Singapore
The government provided guidance on how merchants should handle capital gains, earnings and sales tax on Bitcoin exchanges and Bitcoin-related sales. Companies buying and selling virtual currencies will be taxed on sales gains, unless these currencies where part of the companies' investment portfolio acquired for long term investment purposes, in which case these are considered capital in nature, thus not taxable. The purchase of virtual services would not be subject to sales tax, whilst a sale tax for purchases of physical goods is levied.
The Monetary Authority warned consumers about Bitcoin-related risks. It also stressed the ML/FT risks posed by virtual currencies. Accordingly intermediaries that buy, sell or facilitate the exchange of virtual currencies for fiat currencies are required to verify the identity of their customers and report suspicious transactions, obligations similar to those imposed on money changers and remittances businesses who undertake cash transactions. However the Monetary Authority stated that "whether or not businesses accept bitcoins in exchange for their goods and services is a commercial decision in which MAS does not intervene".

Kyrgyzstan: the Central Bank stressed that the Kyrgyz Som (KGS) is the only legal tender in the country. It has warned consumers about potential risks inherent to digital currencies, including the inability to cancel transactions made, and volatility. Criminal charges could be pressed as digital currency usage is prohibited.

An attempt to summarise:
- Anyone who would have expected regulators across the world to come up with a common definition and a common approach to virtual currencies is bound to be disappointed. Views and actions differ significantly.
- A key issue is the classification of virtual currency: is it money, currency, foreign currency, a commodity, an asset, e-money? The answer or answers to this question – against each country's background - generally drive the regulators' position.
- Another issue is whether virtual currency requires (if at all) new legislation, or whether existing legislation is sufficient. A point of debate also is which part of the value chain (exchanges, miners, merchants, software developers…) should be subject to legislation.
- Some convergence however can be noted with respect to the anonymity feature of Bitcoin and preventing illicit activities (ML, TF, tax avoidance, fraud). Concern that virtual currencies are a conduit for these is generally shared, but responses diverge (some view existing legislation as sufficient to address the risk).
- Some convergence can also be noted with respect to the approach taken by tax authorities. The latter are generally tempted to consider a number of activities in virtual currencies as being taxable – although a distinction between short term and long term holdings, where it already exists, is generally maintained.
- Some convergence can finally be noted with respect to consumer protection: many regulators went public to caution consumers against the risks linked to virtual currencies.
- Of particular interest could be the approach recommended by the European Banking Authority that formalises the existence of two economies, one dealing in fiat currency and the other in virtual currency (the latter not open to financial institutions), with gateways between the 2 which need to be monitored and regulated. The approach by one regulator mandating

merchants who accept payment in virtual currency to verify the identity of their customers is also to be noted.

- Several regulators express a need for moving cautiously in legislating virtual currency, for fear of hurting valuable innovation.

8- Virtual currencies: strategy take-away…for now

Should virtual currencies then be embraced or discarded by regulators and stakeholders, or be the opportunity to rethink value propositions and business models? We shall remember that this Working Paper used Bitcoin only as a model to review virtual currency. Whilst the blockchain technology must be acknowledged as a key invention software issues remain to be addressed, as well as some key aspects of the concept[48]. Which virtual currency(ies) will survive is beside the point. The environment (an increasingly peer-to-peer, sharing and digitalized economy) is too favourable for the concept to vanish. Of course readiness does not guarantee adoption – the reverse being also true. But at this point in time a few strategic findings should be pondered by regulators and financial industry participants:

- Considering the scope and depth of the debate, regulatory attention is unlikely to wane[49]. But regulators will have to resolve a complex algorithm of their own, i.e. how to balance uncertainty, innovation, and risk to society. A critical decision will be how much to legislate now: the "whole" of what virtual currency could represent, or just those aspects which are of most concern now? Given the baseline no coordinated approach may emerge in the near term, leading market players to arbitrage jurisdictions. At the very least there should be the ambition for a global, common definition and classification of virtual currency.
- When legislating on virtual currency regulators should consider that any overly cautious stance on virtual currencies could have spill over effects on "e-money" and hurt the current digitalization of economies and payment systems. Regulators should answer the question: what do virtual currencies compete with[50]? The distinction between the trust-less transfer and ledger technology on one side, and the idea of crypto-currency on the other, (or also: the utility value – as payment utility and secure store of value - and speculative value) should be well present.
- Although an innovation is often used beyond what it was intended for, it could be useful for regulators to remember that Bitcoin has been conceived as a response to the view that completely non-reversible transactions are not possible. Regulators concerned about virtual currency could as a first step focus on allowing a no-frills payment transaction, amending where necessary existing payment legislation in order to enable irreversible retail payment transactions – if only for certain values.
- Certainly the virtual currency world in its current stage presents consumers with significant risks. Whilst virtual currency is a development which should not be discarded, which should be monitored, and on which experience should be gathered through a number of well-targeted

---

[48] E.g. how will miners be compensated once the total number of bitcoins that can be issued has been reached?

[49] "Should Bitcoin become widely adopted, it is unlikely that it will remain free of government intervention, if only because the governance of the Bitcoin code and network is opaque and vulnerable. That said, it represents a remarkable conceptual and technical achievement, which may well be used by existing financial institutions (which could issue their own Bitcoins) or even by governments themselves" (Chicago Federal Reserve Report, Bitcoin: A Primer, December 2013

[50] Mervyn King, then Governor of the Bank of England, already remarked in 2004: "The key question for a public currency is how do we prevent the government (ourselves) from abusing its issuing power in the future? Collective decisions today cannot bind future collective decisions… monetary arrangements can always be changed in the absence of an outside enforcer… A really bad government will simply restore discretion to itself".

products, financial institutions should also play their role in informing and educating consumers about the pros and cons of virtual currencies. In essence consumers should be able to satisfactorily answer for themselves the question: to whom do I extend credit when I buy a Bitcoin? The emergence of a new digital divide, between those understanding (and possibly having access to virtual currency), and those who do not, must be avoided.

- Worker remittances however are an area for concern. Because this market is by far and large cornered by a small number of money transfer operators who continue in many remittance corridors to impose hefty fees on senders and receivers, Bitcoin because it's on the surface no transaction fee feature is being promoted by a number of providers as the ideal alternative. Although transaction irreversibility is not an issue in the remittance scenario, unfortunately the volatility of Bitcoin represents a huge risk for what is "people's money". Until such time where volatility narrows to a par with fiat currencies (and becomes ceteris paribus predictable) it is not recommended to use Bitcoin for the purpose of transferring remittances.
- The in theory unlimited reach and no cost of Bitcoin also prompts a number of debaters to promote Bitcoin as the ideal vehicle to address financial inclusion. It would not be responsible to at this stage entertain any illusion in the public that this could be a viable path to pursue – pretty much for the same reasons as brought up for remittances.
- Most of the debate is on the virtual currency i.e. "money" dimension. The enabling no-trusted third party technology received far less attention so far (maybe because there is an assumption that it is less of a challenge from a legislation perspective). But it may be that technology that holds the greater disruption potential, with applicability anywhere a transaction between 2 parties requires third party validation e.g.: transfer of property, execution of contracts, identity management. Up to 20% of US GDP is generated by industries whose main function is to act as a trusted third party[51] – figures for other developed economies should be in the same order of magnitude. The premise of a technology layer[52] substituting well-established services is a call for stakeholders including financial institutions to look at value chains, business models and positioning. In this context providers will also have to learn how to manage "decentralised reputation".
- What is presented by some as the appeal of a decentralised, no trusted third party system to the growing number of e-commerce buyers concerned as to what may happen with their private data must however be right sized. Whilst indeed a push system such as Bitcoin is in principle less insecure as no consumer data is exchanged or stored (and no authorization takes place), in effect many consumers would rely on third parties to e.g. store their keys. In this respect it is just a shift in risk that takes place – the total amount of risk remains unaffected.
- Cash is another area worthy of attention. Of course some virtual currency supporters are convinced that cash will be eliminated. But there is continued evidence that even as economies digitalise cash is resisting (at least within certain population segments, and/or for certain transactions). This shifts the debate to whether Bitcoin-like technology wouldn't provide the vehicle to move from a physical form factor of cash to a digital form factor: only unique digital banknotes (of course issued by a central bank) would be exchanged, with no need for physical transport, fitness or counterfeit checks[53] - thus significantly reducing the cost of cash to society.

[51] Wedbush Research, Tiining and sizing the era of Bitcoin, May 2014

[52] Which may include and facilitate : a new custody model, « smart contracts », programmable money, open access through API or protocol, digital scarcity or « smart property »

[53] The author of this Working Paper presented this concept to the Eurosystem conference on « Preparations for the launch of the Europa series of euro banknotes" – Vienna, 23rd April 2013

References and acknowledgements

- Back Adam, Hashcash: a Denial of Service Counter-Measure – August 2002
- CFPB (Consumer Financial Protection Bureau) Consumer Advisory on risks to consumers posed by virtual currencies, August 2014
- CGAP Brief, Bitcoin Versus Electronic Money, January 2014
- Chicago Federal Reserve Bank Report, Bitcoin : A Primer, December 2013
- Congressional Research Service (US), Bitcoin: Questions, Answers, and Analysis of Legal Issues, Decmber 2013
- Davis Group LLC, Bitcoin, Digital Currency and the Internet of Money, February 2014
- EBA (European Banking Authority) Opinion on Virtual Currencies, 4 July 2014
- ECB Report, Virtual Currency Schemes, October 2012
- Governmernt Accountability Office, Virtual economies and currencies, Report to Committee on Finance, US Senate, May 2013
- Financial Action Task Force Report: Virtual Currencies, key definitions and potential AML/CFT risks, June 2014
- FinCEN (Department of the Treasury Financial Crimes Enforcement Newtork):
  - 18 March 2013 Guidance on the application of FinCEN's regulations to persons administering, exchanging or using virtual currencies
  - 30 January 2014 FinCEN Adminsitrative Ruling on the application of FinCEN's regulations to virtual currency mining operations
  - 30 January 2014 FinCEN Adminsitrative Ruling on the application of FinCEN's regulations to virtual currencty software development and certain investment activity
- Finextra.com
- George Mason University, Bitcoin: a primer for policymakers, June 2013
- Innopay, Crypto-currencies: Exploring a revolutionary technology, June 2014
- Law Library of Congress (US), Regulation of Bitcoin in Slected Jurisdictions, January 2014
- Nakamoto Satoshi, Bitcoin: a peer-to-peer electronic cash system, 2008
- OECD Working Paper, The Bitcoin question: currency versus trust-less transfer technology
- PaymentsNews.com
- Selgin George, Synthetic Commodity Money, April 2013
- The Clearing House/ICBA, Virtual currency: risks and regulation, June 23rd, 2014

About WSBI (World Savings & Retail Banking Institute)

WSBI – The Global Voice of Savings and Retail Banking

WSBI brings together savings and retail banks from 90 countries, representing the interests of approximately 7,000 banks in all continents. As a global organisation, WSBI focuses on issues of global importance affecting the banking industry. It supports the aims of the G20 in achieving sustainable, inclusive and balanced growth and job creation around the world, whether in industrialised or less developed countries. WSBI favours an inclusive form of globalisation that is just and fair, supporting international efforts to advance financial access and financial usage for everyone. It supports a diversified range of financial services that responsibly meet customers' transaction, saving and borrowing needs. To these ends, WSBI recognises that there are always lessons to be learned from savings and retail banks from different environments and economic circumstances. It therefore fosters the exchange of experience and best practices among its members and supports their advancement as sound, well-governed and inclusive financial institutions.

World Savings and Retail Banking Institute - aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax: +32 2 211 11 99
Info@wsbi-esbg.org ■ www.wsbi.org

Published by WSBI, October 2014