

9th session

14th November 2017

Virtual currencies- Cryptocurrencies



Virtual currencies - cryptocurrencies

- The presentation of the concept.
 - Presentation of the paper
Böhme, Christin, Edelman and Moore (2015). Bitcoin: economics, technology and governance. Journal of Economic Perspectives, 29: 2, 213-238
- What determines the price of bitcoins
 - Presentation of the paper
Ciaian, Rajcaniova, and Kancs, (2016). The economics of BitCoin price formation. Applied Economics, 48: 19, 1799-1815.
- The pros and cons of virtual currencies (*Mikołajewicz-Wozniak and Scheibe (2015) Virtual currency schemes – the future of financial services and ECB (2015) Virtual currency schemes – a further analysis*)
- Regulation



- Throughout the years Satoshi wrote thousands of posts and emails and most of which are publicly available.
- The National Security Agency was able to use the 'writer invariant' method of stylometry to compare Satoshi's 'known' writings with trillions of writing samples from people across the globe.
- By taking Satoshi's texts and finding the 50 most common words, the NSA was able to break down his text into 5,000 word chunks and analyse each to find the frequency of those 50 words. This would result in a unique 50-number identifier for each chunk.
- The NSA then placed each of these numbers into a 50-dimensional space and flatten them into a plane using principal components analysis. The result is a 'fingerprint' for anything written by Satoshi that could easily be compared to any other writing.

- A **virtual currency** or **virtual money** has been defined in 2012 by the European Central Bank (ECB) as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific **virtual** community."
- In 2015, the ECB defines a **virtual currency** as "digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money".
- "**Cryptocurrencies**": virtual currencies based on cryptographic methods of protection.

- **Virtual currencies are not fiat money** Fiat money is defined as a currency that is legal tender, but is not backed by a commodity such as gold or silver. Most of today's currencies are fiat money, i.e. their value is solely based on trust. Virtual currencies are not legal tender, are not issued by a central bank, by credit institutions, or by e-money institutions. (*European Parliament 2016*)
- Some virtual currencies are solely used inside a relatively closed circuit, such as inside a company, or within a computer-gaming community. Cryptocurrencies interact with fiat money.
- More than just Bitcoins – altcoins:

Virtual currencies: <https://coinmarketcap.com/>

Differences between various decentralised virtual currency schemes:

- **Different validating systems**

- *Proof-of-work* (PoW) system, which depends entirely on computational power for validating transactions by means of hashing – based on Mining
- *Proof-of-stake* (PoS) system, Instead of every transaction being sent to the entire network for validation, all active users know beforehand the point in the network that will process the next transaction and add it to the blockchain - tries to eliminate some of the vulnerabilities of the PoW system, such as the possibility of manipulation through a (temporary) monopoly on mining (the 51% attack) and the high energy consumption – based on Forging. Validation is also faster.

- **Different algorithms** – (determine the speed at which the next “block” – set of transactions – is generated, how coins are released, etc.)
 - Very changeable attribute.
 - Shared by different currencies.
 - Some need specialised equipment for “mining”, other don’t.

- **Differences in the (total) supply of coins**
 - Some have fixed Supply, some don’t.

Determinants of the price of cryptocurrencies

Bitcoin Charts



Determinants of the price of cryptocurrencies

Bitcoin Charts



Source: coinmarketcap.com

Pros

- Decentralized: gives power to the individual. Cryptography used for transaction validation prevents counterfeiting virtual currencies and double spending without the need of a trusted 3rd party.
- Bitcoin records are public but the identification of the network participants is almost untraceable. As anonymous as cash. No personal information needs to be given for making a payment.
- Because the supply increases at a determined pace and a fast increase in users is expected, it is expected to appreciate.
- Provision of additional payments alternatives to consumers and low cost payment services. No account-holding fees when storing the cryptographic keys onself and very low or zero transaction fees.
- Ease of transferring funds across borders.

Cons

- Lack of transparency: not clear who should provide information to users.
- Incentive to be used in illegal transactions. Difficulties of applying and enforcing anti-money laundering laws and regulations, as well as those countering the financing of terrorism.
- No authority empowered to interpret the system's rules. Since the location of the participants is hard to establish, no domestic legal framework. Users do not benefit from legal protection such as a deposit guarantee.
- No legal tender: no guarantee that they are accepted. Can be used only as contractual money, when there is an agreement between buyer and seller in order to accept a given virtual currency as a means of payment.

Cons (cont.)

- As a nascent system, with still low volumes traded is still more subject to speculation.
- Volatility of the value of Bitcoins – not good to use as a store of wealth (except with a real long-term horizon).
- Fear of cyberattacks.
- Irreversibility does not allow errors in payments or unauthorized transfers

Regulation

The build-up of financial stability risks from VCS would be likely under the following conditions:

- (i) VCS become more widely used in regular payments;
- (ii) greater links to the real economy develop, including through the presence of financial institutions participating in VCS;
- (iii) no structural developments are envisaged that would make VCS inherently more stable.



ECB (2015)

more direct regulatory responses required

(internationally coordinated, to be effective, because not use not limited to national jurisdictions)

Committee on Payments and Market Infrastructures

(working committee of BIS)

- Regulatory issues for digital currencies cover three main fields:
 - consumer protection,
 - prudential and organizational rules for the different stakeholders,
 - and specific operating rules as payment mechanisms.

European Banking Authority Warning (2013)

- Consumers may lose their money using exchange platforms. As these platforms are generally unregulated, the failure of a scheme can lead to the loss of currency. There is evidence that consumers incur large losses on a regular basis.
 - Money may be stolen from a digital wallet. Virtual currencies are stored on digital platforms protected solely by passwords. Hackers have repeatedly obtained access to these passwords, thus allowing them to plunder the accounts. The probability of getting any of the money back is negligible. Additionally, losing a password often means there is no means to access one's virtual currency.
 - There is no protection for those using virtual currencies as a means of payment. There are no refund rights. Payments from digital wallets can generally not be reversed.
 - The value of a virtual currency is unstable. Apart from high exchange rate volatility, there is also the chance that the currency loses all of its value.

- There is a danger that virtual currencies are used for unlawful activities, such as money laundering. This may prompt authorities to close down the exchange platforms, depriving consumers of access to their funds.
- Tax liabilities may derive from holding virtual currencies. This requires consumers to be well aware of tax regulations.

Regulation current state (as of end of 2015)

↪ Tasca (2015)

↪ ECB (2015)

- Many countries: wait-and-see posture.
- USA
 - New York State Department of Financial Services (NYDFS) proposed regulation to protect consumers from fraud and abuse, prevent money laundering and other illicit activity, and enforce measures against cyber crime. BitLicense applies only to financial intermediaries. They have to comply with capital requirements and protection of assets; record-keeping; maintenance of an effective cyber security program. - Problematic in terms of costs and invasion of customers' privacy
 - May 7, 2015, NYDFS granted a charter to itBit Trust Company LLC to operate as a commercial Bitcoin exchange, the first virtual currency company to receive such a charter from NYDFS. —
 - What happens when one State creates a special purpose digital currency exchange trust charter, but other states do not recognize it as such?

- Europe
 - No harmonised regulatory framework
 - Currently: amendments to Directive (EU) 2015/849 (Anti -Money laundering) extending its application also to "**electronic money** issuers and distributors".
Status: Awaiting Parliament 1st reading / single reading / budget 1st stage
 - European Banking Authority (Eurosystem element) discourages financial institutions from buying, selling or holding in deposit digital currencies.
- Germany - classified digital currencies as units of account (no legal tender)- users are subject to 25% capital gains tax if they hold the currencies for less than one year.
- France - l'Autorité de contrôle prudentiel et de résolution acknowledges exchange and payment transactions in digital currencies but requires actors to obtain a licence as payment service providers.

- Swiss Financial Market Supervisory Authority – considered means of payment - under Swiss law, Bitcoin is comparable to “foreign currency”- financial intermediaries doing business in BC must comply with Anti Money Laundering rules.
- Brazil – 2013 – legislation legalizing electronic payments systems, including VCS.
- China – financial institutions are prohibited from converting virtual currencies into traditional currencies; in 2014, Alibaba - China’s top internet retailer- prohibited the use of Bitcoin on its online shopping platforms.
- Japan – Virtual Currency Exchange Operators offering services in Japan have to be registered. To register, it is necessary to have a local business office, as well as a locally residing representative. Engaging in virtual currency exchange services without registration is subject to criminal punishment. Also minimum capital requirements and obligation to implement measures to detect and report potential money laundering activities

In general, without anonymous currency conversion, money launderers or terrorists would find no advantage in virtual currencies. – regulatory action on exchanges

- **References:**

Tasca, Paolo, Digital Currencies: Principles, Trends, Opportunities, and Risks (September 7, 2015). Available at

<http://dx.doi.org/10.2139/ssrn.2657598>

ECB (2015) Virtual currency schemes – a further analysis