6. THE DUAL NATURE OF BITCOIN AS PAYMENT NETWORK AND MONEY

Paolo Tasca

6.1. INTRODUCTION

Back to 2008, Nakamoto combined the distributed ledger technology with cryptography and gave origin to what is now known as 'blockchain' technology[1]. The blockchain technology allows for a trustworthy record of transactions among anonymous without the need of a neutral central authority. The blockchain contains all the transaction history and each transaction is tamper-proof, publicly auditable (traceable) and no-reversible. The first application of the blockchain technology is Bitcoin: a digital currency that combines together the characteristics of money with those of a payment system. This dual nature is explained by the fact that Bitcoin is money expressed as a string of bits sent as a message in a fully decentralized network composed of millions of users with computers and devices connected among each other. 'Miners' are special users that identify and validate the messages (i.e., transactions) using copies of all or some information of the blockchain. Before the transactions are accepted by the network, miners collect them in blocks and have to show 'proof of work' using a cryptographic hash function – a special algorithm – that aims to provide high levels of protection. Miners receive some form of compensation, expressed in transaction fees and newly created Bitcoins (i.e., money supply), for their computing power contribution, avoiding the need to have a centralized system. Although Bitcoin remains the dominant currency in terms of use and capitalization, at the moment of writing there are more than five hundreds different digital currencies[2]. Digital Currencies differ among each other by the consensus protocol (synchronous or asynchronous) and by the rewarding (money supply) mechanism[3]. In this chapter we analyze the dual nature of Bitcoin both as payment system and money[4].

---

[1] See Satoshi Nakamoto's paper "Bitcoin: A Peer-to-Peer Electronic Cash System", http://nakamotoinstitute.org/.
[2] See CoinMarketCap. https://coinmarketcap.com/all.html, 2015.
[3] Bitcoin relies on asynchronous consensus protocol which require 'miners' to agree on the transaction order. And this is a time and computing consuming activity. Instead, newer protocols such as Ripple rely on a synchronous consensus process that does not need miners nor proof of work and can agree on the changes to the blockchain within seconds. For a technical explanation of the different digital currencies consensus protocols and rewarding mechanisms see A.M. ANTONOPOULOS, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, Inc., 2014.
[4] For a more comprehensive market analysis of digital currencies we refer the reader to P. TASCA, "Digital Currencies: Principles, Trends, Opportunities and Risks", *ECUREX Research working paper*, 2015.

6.2.   BITCOIN AS PAYMENT NETWORK

Blockchain-based payment network solutions provide a fast, cheap and secured cross-border payment and settlement framework. Differently from Payment as a Service solutions like Paypal, these methods have back-ends relying only on decentralized consensus protocols like Bitcoin or Ripple. These solutions allow for domestic and international payments, in any combination of currencies, which can then be settled directly between the parties without the need for credit cards, central clearing houses or correspondent banks. At the moment of writing Bitcoin is the biggest blockchain-based payment network and therefore it is useful to compare its expansion with other competitive payment networks like VISA, Mastercard, Discover and Western Union. The first three methods are consumer credit card channels and the last one is the biggest person-to-person global money transfer. During the period 2011-2015, the daily transaction volume in the Bitcoin network was ca. USD 60 million. The figure certainly pale if compared with VISA which processes ca., USD 20 billion daily transactions or with other payment networks. Namely, Bitcoin payment network is the smallest among those ones considered in the analysis. See Table 1.

Table 1: Volume in million USD (Vol.) and millions of transactions (TX)

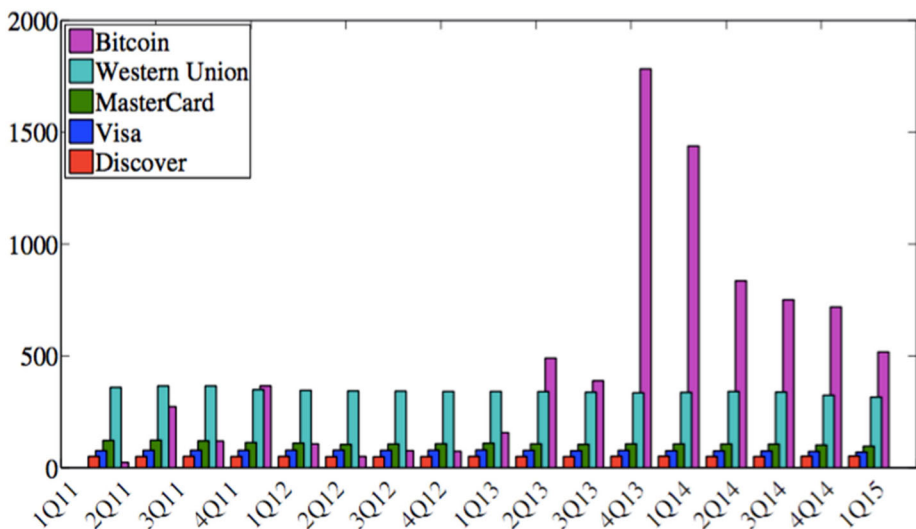| Year	VISA		MasterCard		Discover		Western Union		Bitcoin	
	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)
1Q11	15,153.8	198.3	8,011.0	65.6	746.5	14.7	208.8	0.6	0.04	0.002
2Q11	16,604.4	213.2	8,934.1	72.5	787.0	15.7	226.4	0.62	1.6	0.006
3Q11	17,033.0	217.7	9,285.7	77.1	787.0	15.4	231.9	0.63	0.92	0.008
4Q11	17,450.5	223.6	9,505.5	84.4	761.3	15.1	226.4	0.65	2.1	0.006
1Q12	16,934.1	215.7	9,329.7	84.8	804.3	15.8	214.3	0.62	0.7	0.007
2Q12	17,252.7	218.7	9,780.2	93.8	861.1	17.5	220.9	0.64	1.04	0.021
3Q12	17,582.4	225.3	10,087.9	95.4	860.9	17.6	216.5	0.63	2.47	0.032
4Q12	18,648.4	236.8	10,835.2	101.3	840.1	16.8	219.8	0.64	2.45	0.033
1Q13	18,120.9	227.9	10,406.6	95.1	819.2	16.1	207.7	0.61	8.12	0.052
2Q13	19,109.9	245.6	11,087.9	104.1	856.1	17.0	225.3	0.66	26.2	0.053
3Q13	19,175.8	252.1	11,494.5	109.9	850.5	17.1	231.9	0.69	19.3	0.050
4Q13	20,197.8	259.9	12,142.9	114.0	883.8	17.2	236.3	0.71	108.65	0.061
1Q14	19,011.0	249.9	11,483.5	108.2	850.4	16.5	223.1	0.66	91.01	0.063
2Q14	20,274.7	269.6	12,351.6	116.6	892.2	17.6	239.6	0.70	52.35	0.063
3Q14	20,703.3	275.9	12,714.3	120.5	881.0	17.5	242.9	0.72	51.07	0.068
4Q14	20,879.1	285.4	12,879.1	127.1	912.0	17.7	233.0	0.72	60.1	0.084
1Q15	19,263.74	275.6	11,681.32	121.3	852.32	16.3	214.29	0.68	48.80	0.094

However, if we rank the payment networks according to the average US Dollar amount per transaction, Bitcoin constantly moved forward, and since 2013 it overtook and remained larger than the other payment networks. At the moment of writing, the average amount per Bitcoin transaction range bound between 600 and 1,000 US Dollars[5]. The payment network more closed to Bitcoin is Western

---

[5]   The huge oscillation is due to volatility of the conversion rate with the US Dollar which amounts in about 100% annualized standard deviation.

Union with an average value per transaction amounting to ca. 500 US Dollars. The other credit card payment networks record an average amount per transaction between 50 and 90 US Dollars. See Figure 1.

Credit cards offer an easy method for consumption credit and are used to buy goods and services of relatively small amount that are consumed and used during our daily life, from an event ticket to a travel arrangement or a dinner. The evidence that Bitcoin as payment network resembles more Western Union rather than VISA, Mastercard or Discover is significant of the fact that Bitcoin is a network used more for remittances or relatively large transfers of money from person to person instead of consumptions. Indeed, the Bitcoin consensus protocol requires 6 confirmations (equivalent to ca. 1 hour) in order for a transaction to be considered 'secure' by the whole network participants[6]. Also for those technical reasons, Bitcoin as payment network has been so far more used for relatively large amount of money transfer from user to user that do not require real-time exchange of services or goods.

Figure 1: Comparison between different payment networks.
Average daily USD amount per transaction from 1Q2011 to 1Q2015.

Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports.

---

[6] With six confirmations it is essentially mathematically impossible for an attacker with less than 51% of all mining capacity to get six blocks in a row and still surpass the longest block chain. So transactions included in the previous six blocks are considered 'secure', at least from double spending. See https://en.bitcoin.it/wiki/Confirmation.

6.3. BITCOIN AS MONEY

The economic theory defines money by looking at its functions as: medium of exchange, unit of account and store of value. For our analysis we consider also a fourth monetary aspect, what we will call 'the utility of reward'.

Medium of exchange. In this respect, money is a device that avoids the coincidence of the wants to be met before people can trade. This device should avoid the barter system. Bitcoin is an extraordinary medium of exchange. The statistics reveal that the number of transactions registered in the blockchain rose from around 1,000 daily transactions in 2011 to around 130,000 daily transaction in 2015 which, as we have seen before, are equivalent to USD 60 million in value[7].

Unit of account. It is unit of measure used to value any economic item, e.g., goods, services, assets, liabilities, income. A unit of account needs to be:

(a)   Divisible. This means that it can be divided such that its component parts will equal the original value. Bitcoin is a perfectly scalable money because the value of 1 Bitcoin is divisible by up to 10^8. The smallest possible unit is called Satoshi:1 satoshi = 0.00000001 Bitcoins[8]. However, as we will see below, Bitcoin is a deflationary currency and this aspect, in the long-run, may have some perverse effects on its divisibility;

(b)   Fungible. One unit is viewed as the same as any other with no change in value. In this respect, Bitcoin is a perfectly fungible money;

(c)   Countable. A unit of account is also countable and subject to mathematical operations. Bitcoin is perfectly countable.

Store of value. As a store of value, an asset should have the possibility to be saved, retrieved and exchanged at a later time, and be predictably useful when retrieved without costs or losses. In this respect, Bitcoin's deflationary property prevent it to be considered as a good store of value. On the contrary, Bitcoin is an imperfect store of value. At the moment, 25 Bitcoins are created each time a user discovers (mine) a new block. The rate of block creation is approximately constant over time: one every 10 minutes. The number of Bitcoins generated per block is set to decrease geometrically, with a 50% reduction every four years. The result is that the number of Bitcoins in existence will never exceed 21 million. Because of its deflationary property, Bitcoin has a low liquidity in the market. Many users prefer to hoard Bitcoins in the hope that the price will rise. Through this process,

---

[7]   The estimated US Dollar amount of daily transactions was on the order of USD 500,000 in 2011.
[8]   See, https://en.bitcoin.it/wiki/Units.

it becomes increasingly illiquid and expensive, rendering it less useful, with fewer merchants incentivized to accept it. Imagine an economy with Bitcoin as official currency. The problems related to such a deflationary Bitcoin-denominated economy would be: (1) unemployment (wages are fixed because they don't adjust downward); (2) costly constant downward adjustment of price-lists; (3) price of goods closed to zero and even the GDP could come closed zero (this would imply multiple currency denominations and at the end the currency would become more closed to an index); (4) increasing incentives to buy-and-hold. At the moment of writing about the 85% of the total Bitcoins ever issued are hoarded[9]. This means that users assign to Bitcoins an intrinsic value and this makes Bitcoin a terrible store of value.

Transactional utility of reward. With this characteristic we mean that money should allow users to make their own expenditure decisions – without frictions and with full degree of choice –, such to maximize their personal utility. Usually, this is a characteristic not possessed by traditional money or credit cards because of jurisdiction or technical boundaries. However, Bitcoin and similar tokens linked to real assets and exchanged via a unique global platform represent in principle the optimal way to maximize the utility of reward of the users. We are rapidly entering into the 'digital era' characterized by a cashless and a massively connected society utilizing high frequency transnational transactions of products and services that will be increasingly digitalized. According to recent studies, the 90% of US transactions will be cashless by 2020 and by the same year the 50% of EU transactions will be done through a phone device. Technology companies like Google, Facebook, Apple are already entering the payment space with digital wallets uploaded into our mobile devices using NFC systems that replace the credit or debit card chip and PIN or magnetic stripe transaction at point-of-sale terminals. A more general adoption of digital wallets and equivalent technologies will foster a higher adoption of digital currencies. The combination of universal-digital wallets containing different digital currencies with the adoption of multi-currency systems will increase the utility of reward of Bitcoin and other digital (centralised or decentralised) currencies used for real-time, and cross-border transactions.

6.4.   CONCLUSIONS

An entirely digital, distributed peer-validated time-stamped ledger where transactions are cryptographic protected and can be publicly auditable is now a reality. Bitcoin is just the first application of this blockchain technology. Although

---

9   The hoarding loop also increases the volatility of the Bitcoin price with respect to other currencies.

Bitcoin and other digital currencies have the potential to revolutionize money and disrupt finance by eliminating costly – and sometimes obscure – layers of intermediation, perhaps even more important will be the impact of the blockchain technology in areas which are not strictly related to finance like intermediation or clearing and settlement. Indeed, the blockchain technology has the potential to replace the legacy systems currently used in: record system; rating or voting system; database management; distributed storage, authentication and anonymisation of private information; rewarding and punishing-incentive schemes; transaction traceability schemes; refereeing, arbitration or notarization. Blockchain applications spanning a number of sectors promise to change the way companies and people transact, send payments, sign contracts, transfer ownership of things, and much, much more. The hope is that this new technology will instead turn the digital divide, among and within our countries, into digital opportunities. However, blockchain technologies will also introduce new risks to users, market participants as well as new risks to financial integrity: e.g., fraud, money laundering and cyber-crimes. Therefore new forms of 'tech regulation' should be designed and implemented in order to boost innovation and guarantee market stability in those new areas that will be affected by the adoption of blockchain technologies.