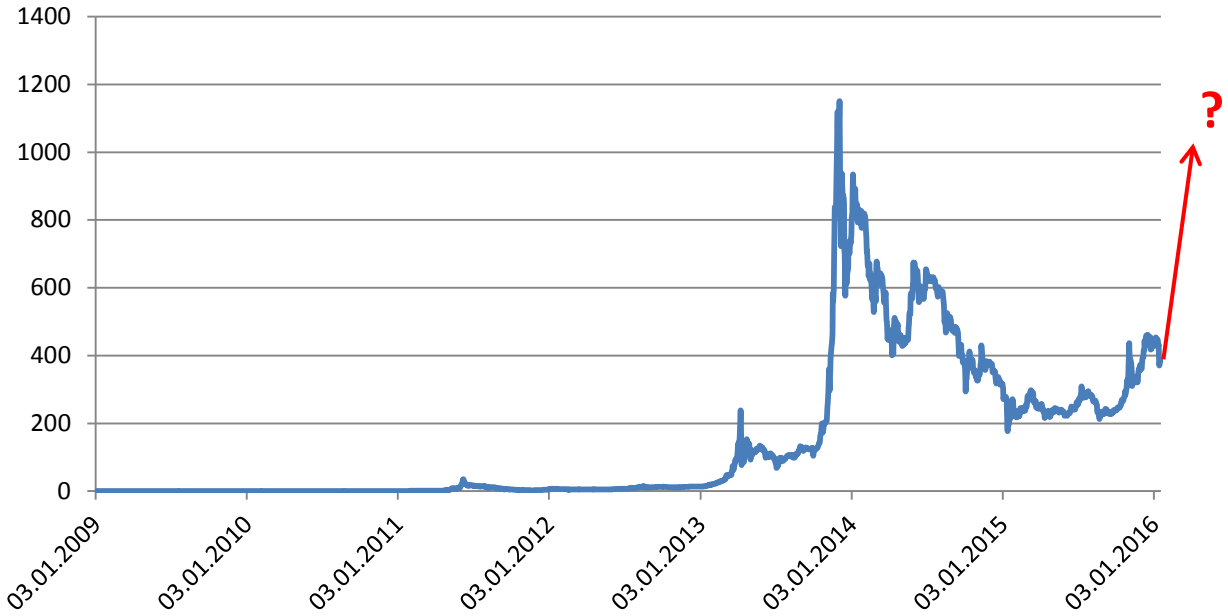
Bitcoin – A short Introduction



Introduction

I started following Bitcoin more actively in early 2015 and was immediately intrigued by the concept and the opportunities offered by the currency itself as well as the technology behind. After some research, I bought my first Bitcoins in summer 2015 and some more until the year end. Over the year-end period, I started to do some more in-depth research that led to the paper you have just started reading. I must confess that the Bitcoin universe is much bigger and more complex than I first thought, and it's evolving even faster than anticipated. Therefore, everything in this paper needs to be understood as a snapshot as of January 2016 and might be fully outdated only 6 months later. Nevertheless, this overview might serve as a good and easy starting point for everybody who's interested in the topic but doesn't have time to do a full and proper research. Enjoy!

History of Money

Money in its purest definition is any clearly identifiable object that is generally accepted as payment for goods and services and repayment of debts. Many things have been used as medium of exchange in recent history, including for example sacks of cereal grain, beaver pelt, shells, tally sticks or coins of different metals.

Paper money was introduces in the 11th century in China and brought to Europe in the 13th century. Later in time, banknotes were a form of representative money which could be converted into gold or silver by application at the bank. The use of bank notes issued by private commercial banks as legal tender has gradually been replaced by the issuance of bank notes authorized and controlled by national governments. The Bank of England was granted sole rights to issue banknotes in England after 1694. In the USA, the Federal Reserve Bank was granted similar rights after its establishment in 1913. These government-authorized currencies were forms of representative money, since they were fully or partially backed by gold or silver and were theoretically convertible into gold or silver.[1]

In the decades prior to the First World War, international trade was conducted on the basis of what is known as the classical gold standard. In this system, trade between nations was settled using physical gold. During the years between WWI and WWII, numerous converging factors strained the classical gold standard. Indeed, by the 1930s, this system had all but disappeared. In July 1944, the enactment of the Bretton Woods Agreement during the United Nations Monetary and Financial Conference resulted in a new monetary system in which gold ceded its central position to the U.S. dollar. Within the Bretton Woods system, all national currencies were valued in relation to the U.S. dollar, which became the dominant reserve currency. The dollar, in turn, was convertible to gold at the fixed rate of $35 per ounce. The global financial system continued to operate upon a gold standard, albeit in a more indirect manner.
The stature of gold in the global financial system was further reduced in the 1970s. In August 1971, U.S. President Richard Nixon severed the direct convertibility of U.S. dollars into gold. With this decision, the international currency market, which had become increasingly reliant on the dollar since the enactment of the Bretton Woods Agreement, lost its formal connection to gold. The U.S. dollar, and, by extension, the global financial system which it effectively sustained, entered the era of fiat money in which it currently resides.[2]

Fiat money is money (or currency) which derives its value not from an intrinsic value but rather from regulation or law and is widely accepted as a means of payment. Its value is not directly related to any real asset but is rather defined relatively to other fiat currencies. Two pre-requisites are essential for a fiat currency to work and survive over time: Limited supply and trust. With unlimited supply, the value of a single unit of a given currency tends to zero. But even with limited supply, if there is no common belief in the future value of a currency, it could also fall to zero.

[1] https://en.wikipedia.org/wiki/History_of_money, 28.12.2015
[2] http://www.investopedia.com/articles/forex/051215/gold-standard-versus-fiat-currency.asp, 28.12.2015

From Gold to Bitcoin

Paper money eventually returns to its intrinsic value: ZERO
(Voltaire)

With the exception only of the period of the gold standard, practically all governments of history have used their exclusive power to issue money to defraud and plunder the people.
(Friedrich A. Hayek)

In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. Deficit spending is simply a scheme for the "hidden" confiscation of wealth. Gold stands in the way of this insidious process. It stands as a protector of property rights.
(Alan Greenspan)

History is full of fiat currencies inflated away to worthlessness. In fact, throughout history, no paper currency has survived in its original form. The purchasing power of the US dollar has declined by 90% since 1950 and so did most other currencies whilst gold represents real value for several thousand years. When governments come under financial pressure they can never resist printing money to pay back debts.
In a very narrow definition, gold also is only a fiat currency as you don't consume it and you don't need it as an input factor for production. But the very limited supply and the belief in thousands of years of experience makes it much more trustworthy than any government in the world.

In a heavily indebted world with many of the major currencies being managed/manipulated, the need for conservation of value and a stable safe haven is increasing dramatically. Gold served as a store of value for a long time, but by its very nature, it's not very handsome in a world becoming more and more digital. The need for some kind of digital gold is obvious and that's where Bitcoin comes into play.

Unlike a real-world currency like the US Dollar or the Euro, Bitcoin has no central bank and is not backed and managed by any authority. Transferring Bitcoins from one account to another account anywhere in the world requires only an internet connection and a wallet application and takes place within seconds. Bitcoin is for finance what e-mail was for the postal industry: an infinitely cheaper and more efficient alternative. With transaction fees being minuscule (about $0.02, directed to the miners which keep the network alive and secure) and a freely accessible and fully transparent ledger, Bitcoin could be a real game changer for our all life.

How does it work

The theoretical framework for Bitcoin was published in 2008 in a paper[3] written by Satoshi Nakamoto[4] and the first 50 Bitcoins (BTC) have been created on January 3rd, 2009.
Bitcoin works decentralized which means that Bitcoin has no central servers for transaction processing or storage of funds. Emission of Bitcoins is limited as it cannot exceed 21 million Bitcoins.

All transactions are recorded in a public distributed ledger called the blockchain. The performance of this chain is maintained by a network of communicating nodes on which this software runs. *Mining* is a record keeping service where *miners* keep the blockchain complete, consistent and unalterable. They verify the transactions repeatedly and collect newly broadcast transactions into a new pool called the *block*. This new *block* has information that chains it to previous blocks, thus giving the name blockchain.
Ownership with respect to Bitcoins means that you can spend Bitcoins associated with a particular address. In order to complete a transaction you need to sign the operation with a private key. Loss of this key would mean that you will lose all the Bitcoins you own and no other form of evidence will be recognized as ownership.

Wallet:
A wallet stores the information necessary to transact Bitcoins. While wallets are often described as a place to hold or store Bitcoins, due to the nature of the system, Bitcoins are inseparable from the blockchain transaction ledger. Perhaps a better way to describe a wallet is something that "stores the digital credentials for your Bitcoin holdings" and allows you to access (and spend) them. Bitcoin uses public-key cryptography, in which two cryptographic keys, one public and one private, are generated. At its most basic, a wallet is a collection of these keys whereas the public key is represented by the Bitcoin address.
There are several types of wallets. Software wallets are stored on your computer, connect to the network and allow spending Bitcoins in addition to holding the credentials that prove ownership. Internet services called online wallets offer similar functionality but may be easier to use; in essence, Bitcoin credentials are stored with the online wallet provider rather than on the user's hardware. Physical wallets also exist and are more secure, as they store the credentials necessary to spend Bitcoins offline. Examples are paper printouts or any other form of physical material where the credentials could be printed on.[5]

Blockchain:
The blockchain is a public ledger that records Bitcoin transactions. A novel solution accomplishes this without any trusted central authority: maintenance of the blockchain is performed by a network of communicating nodes running Bitcoin software. Transactions of the form *payer X sends Y Bitcoins to payee Z* are broadcasted to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The blockchain is a distributed database; to achieve independent verification of the chain of ownership of any and every Bitcoin, each network node stores its own copy of the blockchain. Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the blockchain, and quickly published to all nodes. This allows Bitcoin software to determine when a particular Bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight. The blockchain is the only place that Bitcoins can be said to exist in the form of unspent outputs of transactions.[6]

[3] https://Bitcoin.org/Bitcoin.pdf, 28.12.2015
[4] Satoshi Nakamoto seems to be a pseudonym for a person or a group of people
[5] https://en.wikipedia.org/wiki/Bitcoin, 29.12.2015
[6] https://en.wikipedia.org/wiki/Bitcoin, 29.12.2015

Mining:

Mining is a record-keeping service. Miners keep the blockchain consistent, complete and unalterable by repeatedly verifying and collecting newly broadcasted transactions into a new group of transactions called a block. In order to be accepted by the rest of the network, a new block must contain a so-called proof-of-work. The proof-of-work requires miners to find a number called a nonce, such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target. This proof is easy for any node in the network to verify, but extremely time-consuming to generate, as for a secure cryptographic hash miners must try many different nonce values before meeting the difficulty target.

Every 2016 blocks (approximately 14 days), the difficulty target is adjusted based on the network's recent performance, with the aim of keeping the average time between new blocks at ten minutes. In this way the system automatically adapts to the total amount of mining power on the network. The proof-of-work system, alongside the chaining of blocks, makes modifications of the block chain extremely hard as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. As new blocks are mined all the time, the difficulty of modifying a block increases as time passes and the number of subsequent blocks (also called confirmations of the given block) increases.[7]

Generating new Bitcoins:

The successful miner finding the new block is rewarded with newly created Bitcoins and transaction fees. As of 28 November 2012, the reward amounted to 25 newly created Bitcoins per block added to the block chain. To claim the reward, a special transaction called a coinbase is included with the processed payments. All Bitcoins in circulation can be traced back to such coinbase transactions. The Bitcoin protocol specifies that the reward for adding a block will be halved approximately every four years. Eventually, the reward will decrease to zero, and the limit of 21 million Bitcoins will be reached around 2140; the record keeping will then be rewarded by transaction fees solely.[8]

[7] https://en.wikipedia.org/wiki/Bitcoin, 29.12.2015
[8] https://en.wikipedia.org/wiki/Bitcoin, 29.12.2015

How to enter the Bitcoin world

1. Choose a wallet: There are a lot of different options when choosing your wallet. Most important distinction is whether you have full control of your wallet or if you want to trust someone else to hold your Bitcoins for you. Both variants have their own advantages and disadvantages, but for an easy start and for small amounts, I would recommend opening an online wallet first, e.g. with Bitstamp[9] or Coinbase[10] where you can buy Bitcoins and keep them in the online wallet. For further risk diversification, I would open a couple of wallets, online and offline, and distribute your Bitcoins to the different wallets to minimize your risk. For bigger amounts, a cold (offline) wallet is highly recommended.

2. Get Bitcoins: Once you have opened a wallet and created some sets of public/private keys, you can start accepting Bitcoins as a payment for goods or services or you can buy Bitcoins at one of many Bitcoin exchanges. Depending on how the exchange/marketplace works, you either have to transfer money to the exchange in advance (e.g. on Bitstamp[11]) or you pay the money after the trade directly to the seller (e.g. Localbitcoins[12]). TheBlogChain has some good Bitcoin exchange reviews if you need help finding the Bitcoin exchange of your choice.[13]

3. Spend Bitcoins: There are more and more online shops accepting Bitcoins. The list contains names like Dell, Amazon or Victoria's Secret. With services like BitPay[14], it gets much easier for online-shops to accept Bitcoins without taking the risk from highly volatile exchange rate. Coinmap[15] provides a map which includes real shops accepting Bitcoins as payments. You can also use Bitcoins to transfer money around the globe without the high costs banks and credit card companies usually apply.

4. Security: Using Bitcoins implies a radical shift in responsibility. Bitcoin makes it easy to transfer value anywhere and gives you full control of your money. You are your own bank and therefore also fully responsible for the security of your wealth. Measures to take to keep your Bitcoins safe depend on what kind of wallet you choose. When using an online wallet, make sure that your password is carefully chosen and rather complex and that 2-factor authentication (like Google authenticator) is activated. When using your own software wallet, a good backup strategy is a must. If your computer gets stolen or your hard drive dies, your Bitcoins are lost without a proper backup storage. Bitcoinsecurity101[16] provides a good overview and a lot of links with regard to Bitcoin security.

[9] https://www.bitstamp.net
[10] https://www.coinbase.com
[11] https://www.bitstamp.net
[12] https://localbitcoins.com
[13] http://theblogchain.com/bitcoin-exchange-reviews/, 14.01.2016
[14] https://bitpay.com
[15] https://coinmap.org
[16] http://bitcoinsecurity101.com/

Will Bitcoin survive and succeed?

Main question is whether Bitcoin will survive and succeed over time or if this is just a huge bubble that will completely burst sometime in the future. I see two possible ways/reasons, why and how Bitcoin could succeed and become part of our life similar as the internet did some decades ago.

On a more evolutionary path, Bitcoin would become *the currency of the internet*. The way we currently do online-business is far away from being optimal. In fact, we just adopted existing payment possibilities (bills, credit cards) to the digital world. But typing credit card numbers into online forms, paying high fees for every cross-currency transaction and having no practical way of doing micro-payments is just stone-age. In a more seamless integration, I could imagine Bitcoins being part of our browser/mobile phone, enabling us to pay even very small and fractional amounts just with a single click.
Should banks find a solution to accept the currency into its accounts and also offer a level of protections on payments made, the number of users in the developed world will grow substantially. First steps have already been taken, e.g. Fidor, a German online bank introduced a direct API to bitcoin.de in February 2015. With this setup, you can trade Bitcoins at bitcoin.de while keeping your money on a secured bank account.[17]
The real break-through for Bitcoin I see in emerging markets, where a huge number of people do have a mobile phone but no bank / credit card account because they are just not wealthy enough. With Bitcoin, all these people could open a wallet and start doing business without any prerequisite amount of monetary wealth. They could start on- & off-line businesses and send/receive payments without burdening high transaction costs which makes it especially attractive for micro-payments.

On a more disruptive path, Bitcoin would be the new *safe haven currency* in the already looming next financial crisis. Without going too much into details how fragile the global financial system currently is, it should be obvious to everybody that negative interest rates and a continuously increasing debt/GDP ratio around the globe is not a really solid ground for further prosperity. The usual outcome in the past for such situations was devaluation of currencies and hyperinflation where only those who have been fast in switching into real assets and/or a more stable currency could preserve some wealth. Without many really stable currencies available and in light of the interconnectedness of our financial system, I would expect precious metals and even more Bitcoin to be the main beneficiaries of any upcoming currency crisis.
I don't recommend buying Bitcoins to anybody as you will run the risk of a total loss. But to me, Bitcoin looks like a call option with an almost infinit time to maturity where your downside is limited to the amount you spend but your upside is unlimited. Therefore investing a small fraction of your wealth into Bitcoins (direct or indirect) might be a wise idea.
How can you invest?

1. You could buy Bitcoins directly as described above. You will need to fully understand how Bitcoin as a concept works, where the risks are and how to mitigate them. But after reading this paper, this shouldn't be an issue anymore.
2. You could buy a Bitcoin ETF or fund, e.g. *Bitcoin Investment Trust (aka BIT Share[18])*
3. You could invest into Bitcoin-related companies. But there you have - beside the basic risk of Bitcoins not being successful at all – the idiosyncratic risk of the specific company.
   If you are interested in the current landscape of Bitcoin companies, BitcoinMagazine has a nice infographic.[19]

[17] http://www.coindesk.com/bitcoin-de-launches-integration-with-fidor-bank-accounts/, 14.01.2016
[18] http://grayscale.co/bitcoin-investment-trust/, 14.01.2016
[19] https://bitcoinmagazine.com/articles/bitcoin-is-growing-up-an-infographic-of-the-bitcoin-ecosystem-1447865097, 14.01.2016

Regulation

The legal status of virtual currencies in general varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed its use and trade, others have banned or restricted it.[20]

The IMF (International Monetary Fund) published a research paper on virtual currencies in January 2016.[21] It shows exemplarily how difficult it is to achieve a coherent regulatory framework:

The development of effective regulatory responses to virtual currencies is still at an early stage. They are difficult to regulate as they cut across the responsibilities of different agencies at the national level, and operate on a global scale. Many are opaque and operate outside of the conventional financial system, making it difficult to monitor their operations.
Regulators have begun to address these challenges, with a variety of approaches across countries. Responses have included clarifying the applicability of existing legislation to virtual currencies, issuing warnings to consumers, imposing licensing requirements on certain market participants, prohibiting financial institutions from dealing in virtual currencies, completely banning their use, and prosecuting violators. These approaches represent an initial policy response to the challenges that virtual currencies pose, but further development is needed. In particular, national authorities will need to calibrate regulation in a manner that appropriately addresses the risks without stifling innovation.[22]

A good overview on actual Bitcoin regulation in different jurisdictions can be found on Bitcoin-Reg.[23]

Competitors

A number of alternative cryptocurrencies, or altcoins, have been created after taking inspiration from Bitcoin's code.[24]
Coinmarketcap[25] lists more than 600 cryptocurrencies. Only a handful have reached a meaningful market capitalization and trading turnover, namely Ripple[26], Litecoin[27], Ethereum[28], Dash[29] and Dogecoin[30]. Total market capitalization of all cryptocurrencies is currently slightly above 6.6bln USD, whereof Bitcoin stands for 6bln USD or about 90% and only Ripple, Litecoin and Ethereum have a market capitalization above 100mio USD.

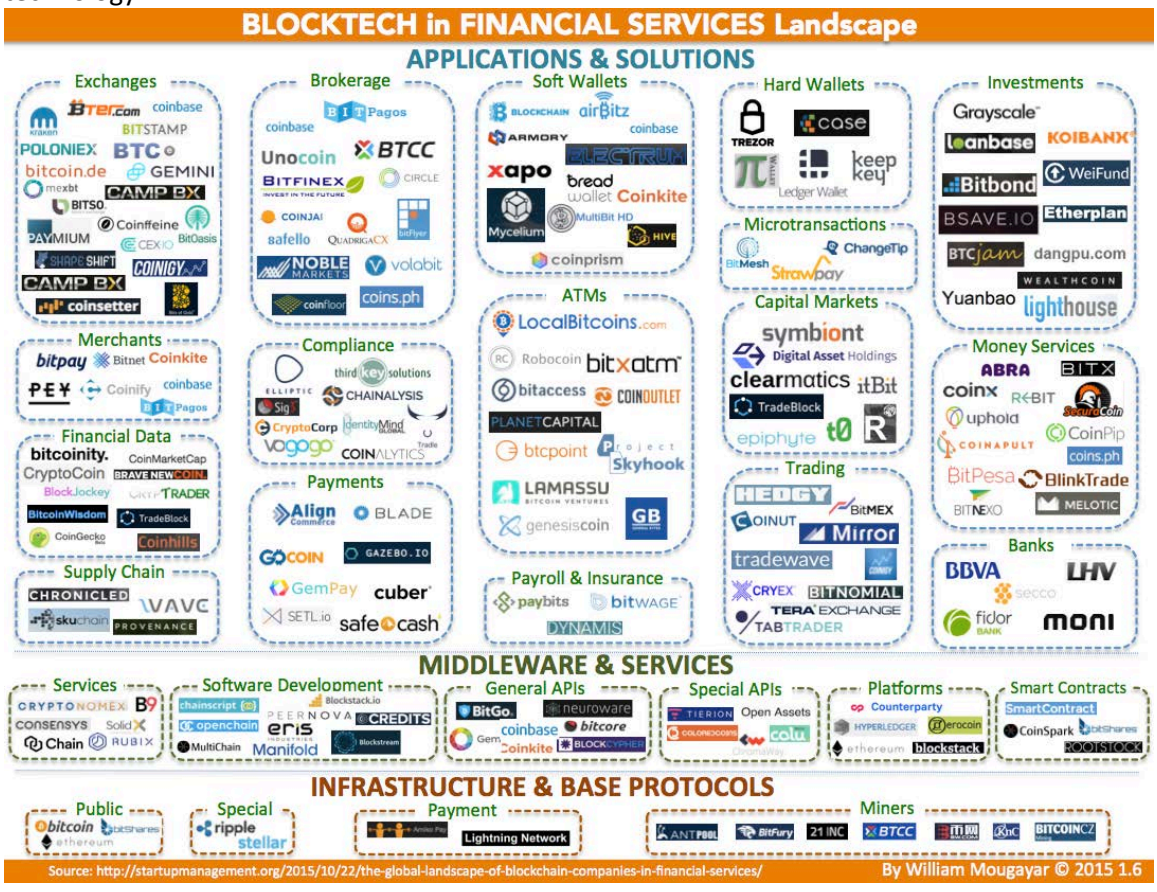
[20] https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country, 05.01.2016
[21] http://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 25.01.2016
[22] http://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf, 25.01.2016
[23] http://bitcoin-reg.com, 19.01.2016
[24] http://www.coindesk.com/technology/altcoins, 22.01.2016
[25] http://coinmarketcap.com/all/views/all/, 22.01.2016
[26] https://ripple.com, 22.01.2016
[27] https://litecoin.com, 22.01.2016
[28] https://www.ethereum.org, 22.01.2016
[29] https://www.dash.org, 22.01.2016
[30] http://dogecoin.com, 22.01.2016

Blockchain applications

What I haven't touched so far in this paper are all those additional Blockchain applications which have been developed in the recent months. It seems that the Blockchain technology gets much attention from different industries and has a good chance to change the technological landscape dramatically. The Blockchain itself is a distributed database based on the Bitcoin protocol that maintains a continuously growing list of transactional data records. These records don't necessarily need to be Bitcoins but could include every type of data, which opens a wide field of possible applications. Just to mention a couple of examples:

- A banking consortium is building up its own blockchain as a more efficient transaction protocol for security and currency trading[31]
- OpenBazaar offers a peer-to-peer marketplace which operates on blockchain technology and where Bitcoin is the only available payment method[32]
- IBM is building a Blockchain for the Internet-for-Things[33]
- Microsoft is offering Blockchain services on its Azure cloud service[34]
- Nasdaq processed the first equity transaction on a Blockchain technology[35]
- Ethereum is a cryptocurrency platform and programming framework for the use of smart contracts in the absence of a central authority[36]

Below chart shows a list of companies that are developing and practically utilizing Blockchain technology.

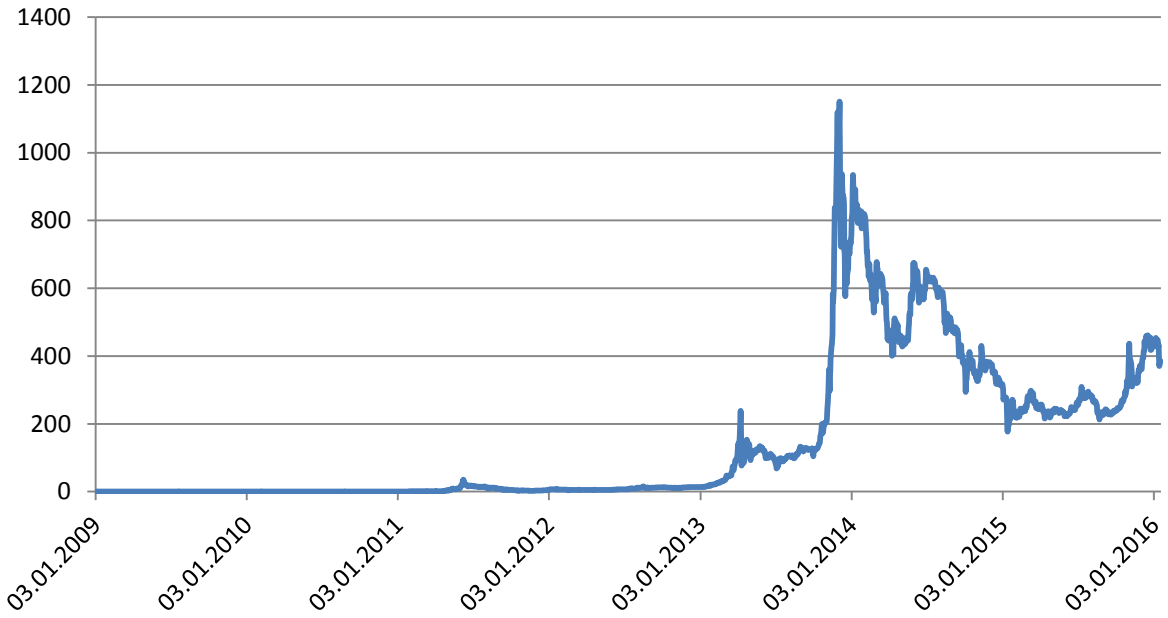


[31] http://r3cev.com/, 05.01.2016
[32] https://openbazaar.org/, 05.01.2016
[33] http://www.extremetech.com/extreme/214461-ibms-upcoming-blockchain-release-could-change-the-internet, 05.01.2016
[34] https://azure.microsoft.com/en-gb/overview/what-is-azure/, 05.01.2016
[35] http://www.forbes.com/sites/laurashin/2015/06/24/nasdaq-selects-bitcoin-startup-chain-to-run-pilot-in-private-market-arm/, 05.01.2016
[36] https://en.wikipedia.org/wiki/Ethereum, 05.01.2016

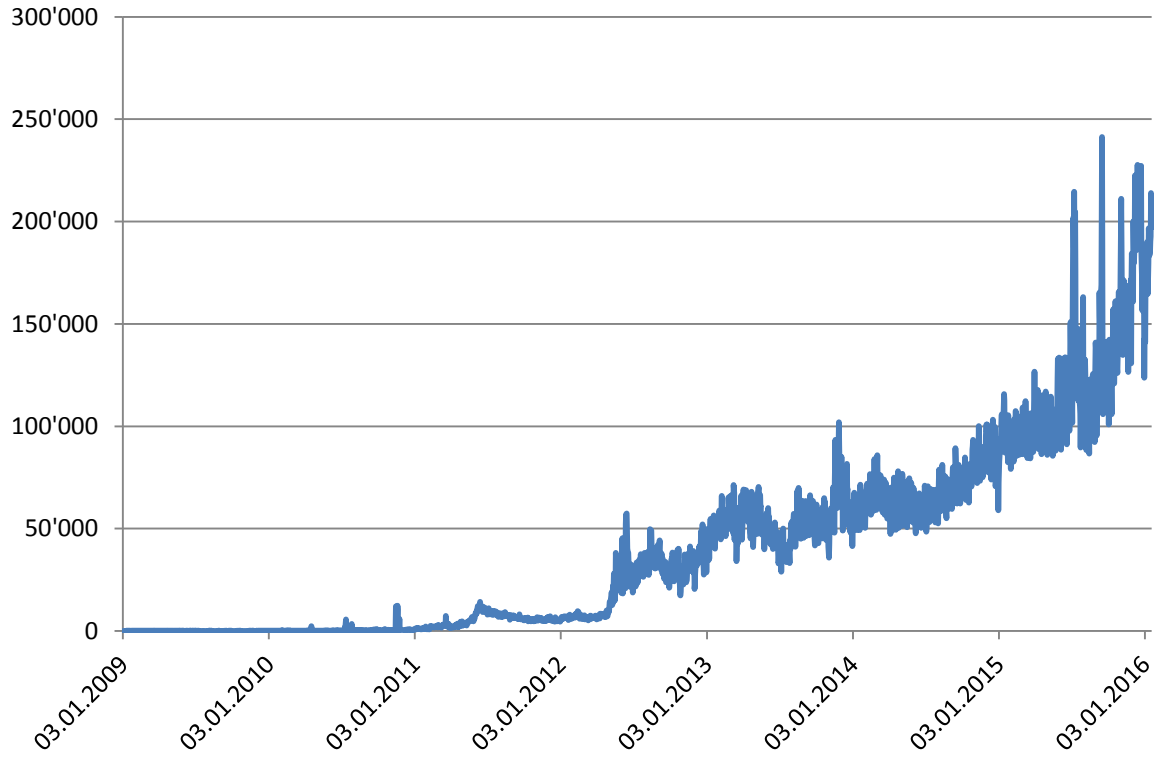
Some Charts

I finish this short paper with two charts, as pictures say more than thousand words….

Price of Bitcoin in USD since inception[37]



Number of transactions per day[38]



[37] https://blockchain.info/charts, 19.01.2016
[38] https://blockchain.info/charts, 19.01.2016