Bitcoin: “Magic Internet Money”

*by Dr. Marco Krohn, Marco Streng**

Bitcoin is a **digital currency** and **payment system** that was created in early 2009 by Satoshi Nakamoto[1]. It is the first fully decentralized currency and has a number of interesting features that cannot be found in any other currency or payment system [1]. **Bitcoin allows anyone to make payments to anyone at any time at no (or very little) cost**.

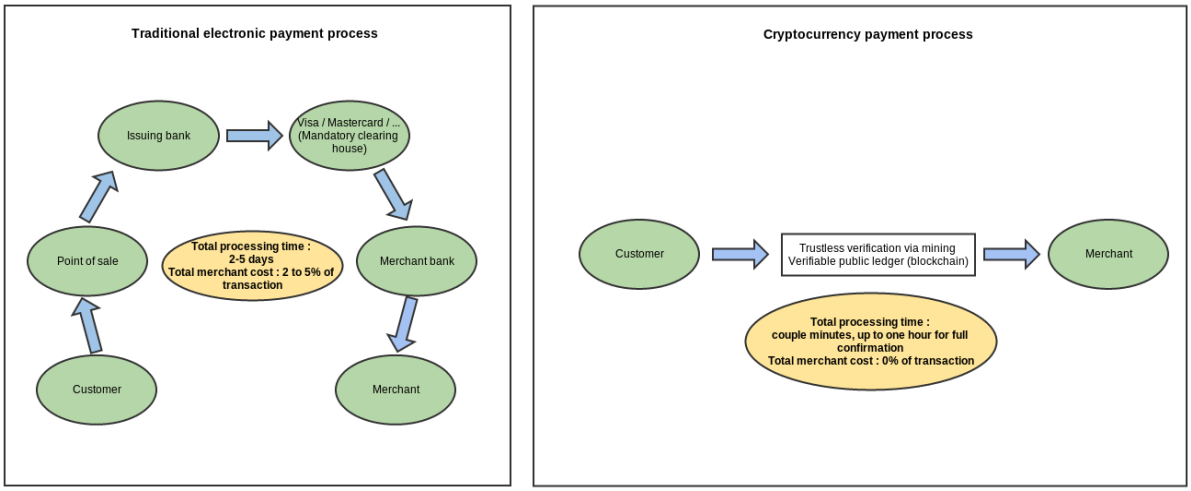

Chart 1: Traditional payment system vs. Bitcoin (“Cutting out the middlemen”)

Bitcoin received a lot of media coverage in 2013, not only for its stateless “underground” nature, but also because of its exponential growth (its price soared by more than 4,000% in the year 2013; see chart 2 below). **Its potential of being a disruptive force that could revolutionize the way payments are done all over the world** got a lot of attention and caught the interest of the industry and finance sectors alike [2]. At the end of 2013, there were already tens of thousands businesses accepting Bitcoin worldwide including some bigger players like Dell and Overstock [3], [4]. Regulators and national institutions are also increasingly looking at Bitcoin.

[1] Satoshi Nakamoto is a pseudonym. The person (or group of person) behind Bitcoin is not known.

* marco.krohn@gmail.com

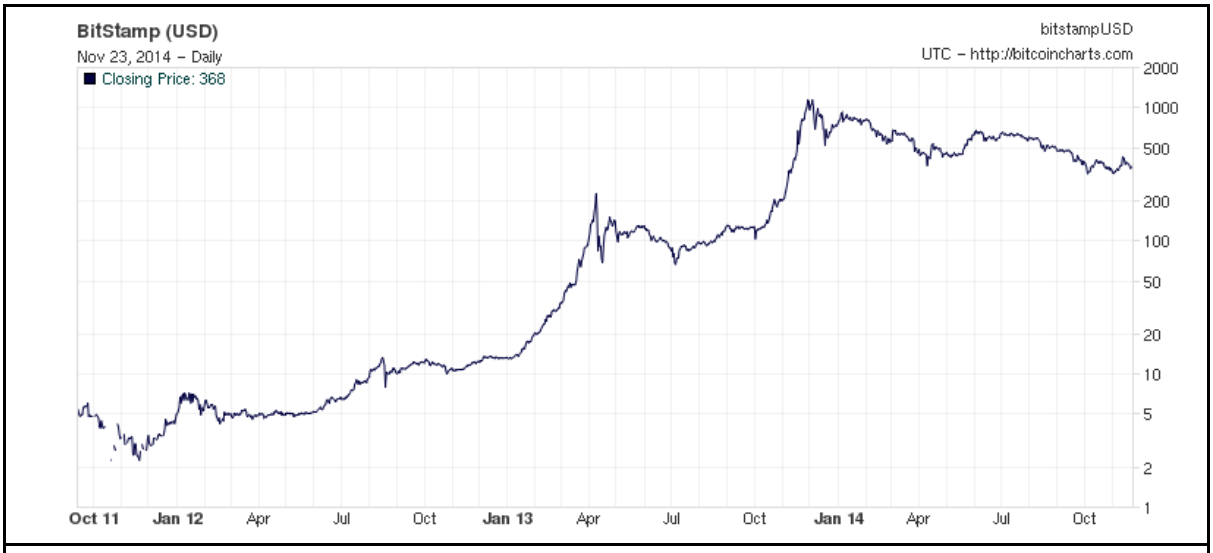

Chart 2: Bitstamp price index over the three two years. Please note the logarithmic scale of the y-axis. Source: bitcoincharts.com

Overview

Main Characteristics

Bitcoin is a **purely digital** form of money. This feature alone is not new, as most fiat currencies (like Euro or US Dollar) exist mainly as numbers in bank computers (like deposit accounts).

Satoshi Nakamoto's major invention is the first **fully decentralized currency**. This means that there is *no* central entity (like a group of people or a central bank) that controls Bitcoin. Even the inventor himself can no longer change its properties. Bitcoin's properties are defined in a protocol[2] that all participants need to follow. If they do not, they are automatically excluded from the network.

On a technical level, decentralization is realized by methods that peer-to-peer networks (e.g., BitTorrent) also use. This setup means that **Bitcoin is extremely resilient against many types of attacks**. For example, even shutting down thousands of computers from the network would not cause significant damage.

Money Supply and Mining

The number of Bitcoins is limited by the protocol and the underlying mathematics. As of January 2014, there are about 12.2 mn Bitcoins in existence, and the number of Bitcoins will grow further over time (albeit at a decreasing rate) until it reaches its maximum of 21 million Bitcoins around the year 2100.

The **money supply is determined by the protocol** (and not regulated by a central bank). About 50% of all Bitcoin (11.5 million) were minted in the first four years of Bitcoins existence. The next four years (2012 - 2016) another half of the remaining 50% will be created, so 25% of all Bitcoins, or 75% in total. The following four years another half of the remaining 25% will be minted and so on and so forth. Therefore, the growth rate declines every four years until Bitcoin reaches its maximum of 21 million units. The idea of having a

[2] The protocol is fixed and cannot be changed anymore, unless a wide majority of the participants agrees to a change

limited amount of money that is harder to “mine” over time is similar to gold production. Its quantity is limited and mining it becomes increasingly difficult over time. In this regards, Bitcoins theoretical roots can be linked to the Austrian school of economics[3].

In contrast, the monetary base of fiat currencies can be expanded by the central bank at any time[4].

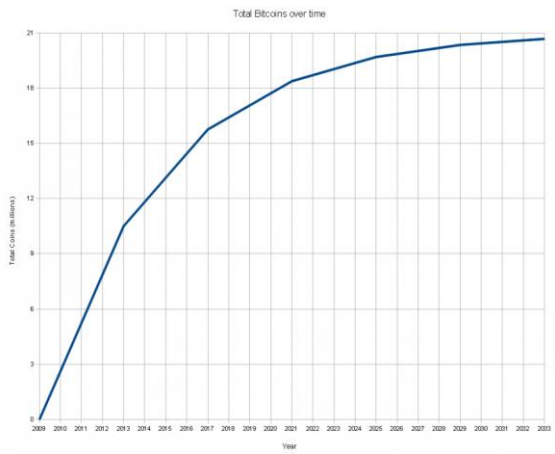

Chart 3a: Number of Bitcoins over time. As of Nov 2014 about 13.5 mn Bitcoins were minted.

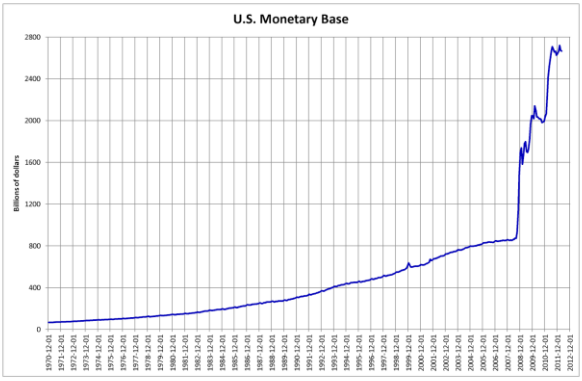

Chart 3b: US monetary base from Dec 1970 to April 2012 (source: Federal Reserve Bank of St. Louis)

New Bitcoin can be minted in a process that is called “**mining**”. A decentralized system like Bitcoin requires consensus of all participants[5] on which transactions are valid, e.g., it should not be possible to spend money twice (“double-spending”). Therefore, some of the participating computers (also called “miners”) have to audit all transactions and spend additional work to ensure that consensus is established. As this requires a huge amount of computational work, newly minted Bitcoins are given to these miners as a form of compensation.

The upper limit of 21 million Bitcoins might sound very low, however, **Bitcoin is divisible** down to eight decimal places, i.e., one Bitcoin consists of 100,000,000 smaller units often referred to “Satoshi”. So, there are $2.1 * 10^{15}$ (just over 2 quadrillion) small units, leaving (in theory) about 300,000 Satoshis for every person on earth.

Transactions

In the same way as for emails, **everyone can send Bitcoins to anyone** in the network. There is no intermediary (no banks or other companies) and no one that can block a valid transaction. It is not even necessary to know the identity of the transaction’s beneficiary. To send Bitcoin to another person his Bitcoin address (or “account”) is required (like an email address is necessary to send an email). For example,

[3] The Austrian school of economics criticises the current fiat monetary system and its control by central banks. Nevertheless, the Austrian economist also have concerns about Bitcoin as they do not have any intrinsic value, like gold.

[4] As of 2013, no country in the world uses a gold standard

[5] From a computer science point of view solving the “general Byzantine Generals’ problem” (which is about reaching consensus in a unreliable and untrustworthy environment) is the big problem that was solved by Satoshi Nakamoto by inventing the “proof-of-work” mechanism

1TkcT3TALCWdRVwfaXdkcg8g5qpMjtWLd

is a valid address that is owned by the authors of this article. It is easily possible to create one (or many) valid address(es) on any computer.

A **transaction is very fast**. Depending on the use-case and the desired security level, a typical transaction takes between a couple of seconds (in most cases this is sufficient) and an hour. **Fees are very low.** Transactions are either free or they cost a few USD Cents (equivalent) regardless if the receiver is next door or on the other side of the world. The network operates 24/7 and so it is possible to **transfer Bitcoin at any point in time.**

Status-quo

Price of Bitcoin

After its launch, users were considering Bitcoin as “virtual tokens” and an “interesting experiment”, though Bitcoin did not have “real” value, i.e., it was not possible to buy goods with it. Theoretical approximations about the value were derived by calculating the production cost for one Bitcoin[6] (e.g. in Oct 2009, one US Dollar was worth about 1,000 BTC). Things changed in May 2010, when the first publicly recorded transaction for real world goods took place: a user bought two pizzas (about 25$) for 10,000 BTC [5].

Since then, various exchanges were founded all over the world, allowing to trade Bitcoin for fiat currencies (mainly USD, CNY and EUR). **Prices soared quickly** over the last few years (cf. chart 2) and the market cap (=number of Bitcoin in circulation * price) reached USD 10 bn for the first time in Nov 2013.

[6] production cost mainly in terms of electricity cost for minting a Bitcoin with computer hardware

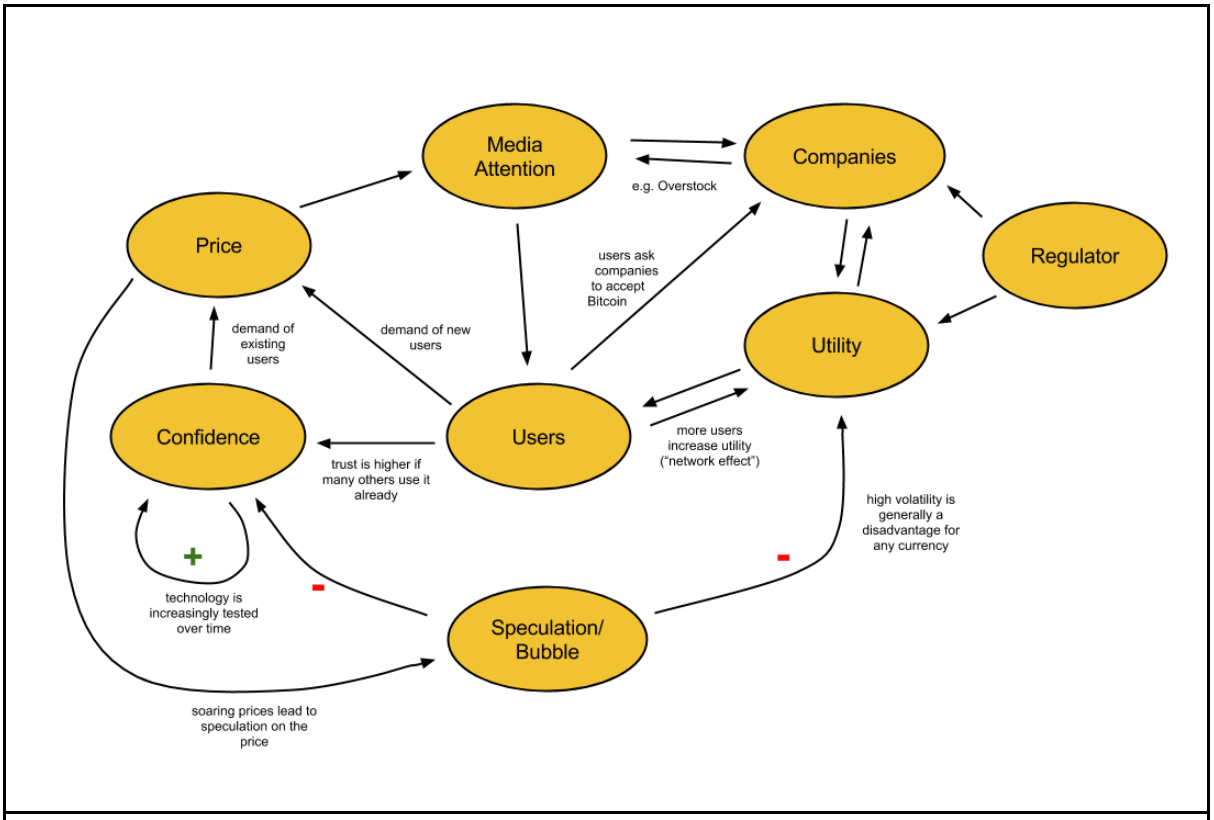

Chart 4: Interactions - various positive feedback loops contribute to the exponential and volatile environment.

However, speculation on rising prices also caused three major bubbles so far, and **price volatility remains high**. This is partially because the market is relatively small and thus bigger players have a huge effect on the market. Furthermore, players have different views on the potential of Bitcoin as a payment system. For example, some believe it could go up as high as $100,000, while others say that it has no value at all [6], [7].

Adoption Level

Users and Transactions

Everyone can easily use an application to generate a Bitcoin wallet, without the need to be registered somewhere. Therefore, it is difficult to estimate the exact number of users. The popular “blockchain wallet” counts 2.5 million users, while the Coinbase wallet has about 1.8 million users. However, how many of these wallets are actively used it not known. Furthermore, there are many other wallets available, and users could use more than one wallet. So the best guess is that about 1-4 million people are using Bitcoin.

All transactions are stored in a “public ledger” (also known as the “blockchain”). However, only the addresses (like 1TkcT3TA….) are stored in the ledger, but not the person that is in control of the address. Therefore, the transactions themselves are completely transparent, but at the same time some anonymity for the users is ensured.

As all transactions are recorded in the blockchain the “number of transactions per day” can be observed. This is an interesting measure, as it shows whether the usage of Bitcoin is growing over time.

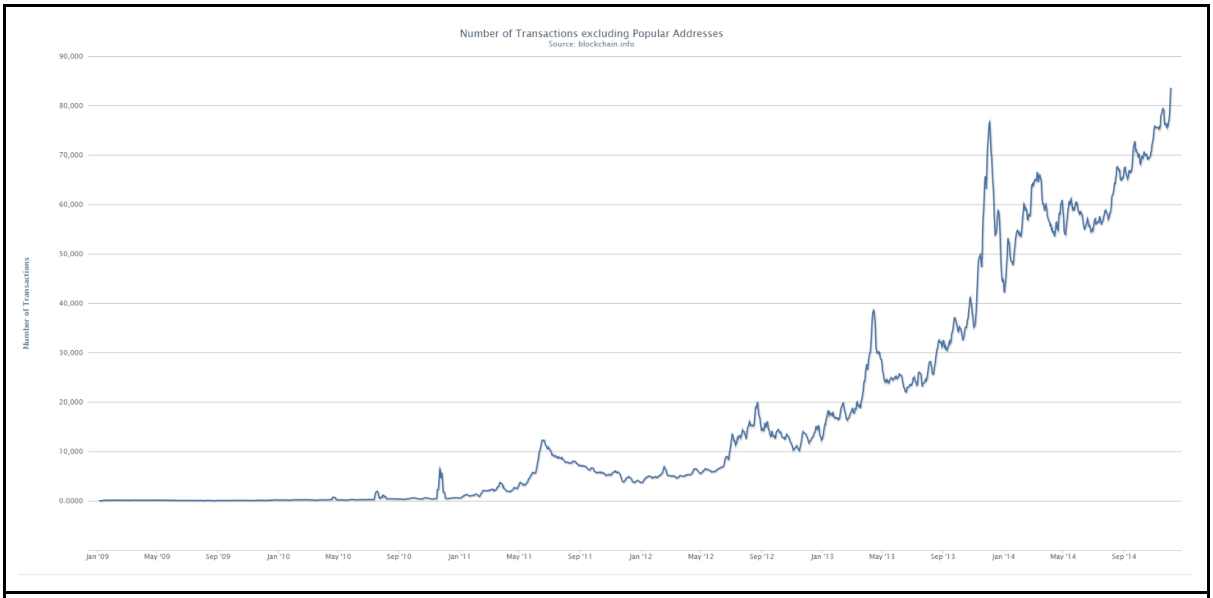

Chart 5: number of transactions excluding popular addresses (seven day average). Source: blockchain.info

Popular addresses were excluded to reduce noise[7]. The chart shows that the **number of transaction grows exponentially**. As of November 2014, more than one transaction per second ("tps") occurs. That is about a 20-fold increase compared to end of 2011.

Merchants and Bitcoin

Bitcoin's offers several advantages for merchants, in particular very low fees compared to other payment systems. For example, merchants usually pay about 2-3% of the turnover to the credit card company. For a typical margin of 10% this means that the merchant pays about 20-30% of his net income to credit card companies.

Credit Cards were invented in the 1950s / 60s and were never designed for the internet. This causes problems, like stolen credit card data and "credit card fraud" which costs the merchants and companies billions USD every year [8].

	Credit Card	Bitcoin
Fees	Merchants usually pay 2-3% of the turnover; customers are charged additional fees for foreign currencies.	No cost for the merchant / if a payment processor(*) is used cost are generally below 1%.
Speed	A few seconds.	A few seconds.
Chargebacks	The merchant has to bear the loss in most cases.	No chargebacks.
Available Countries	Payments in dozen of countries are blocked.	Everywhere.
Privacy	Credit card number and name are transferred to the merchant.	Sender's address is transferred (and stored in the blockchain).
Usage	VISA processes about 2,000 transactions per second.	Bitcoin network processes about 0.5 transactions per second.

[7] For example, the gambling website "Satoshi Dice" was very popular for some time. As we do not want to measure the gambling activity these popular addresses were removed from the chart.

(*) for example: BitPay or Coinbase

As a payment system Bitcoin provides a very cheap way to move money. Transactions typically cost a few cents and can be done from anywhere without limitation. The down-side from a company's point of view is its high volatility. As most companies have to pay their suppliers and employees in fiat currency (e.g. USD) this would expose them to market risk. **Intermediary companies** (like Coinbase and BitPay) eliminate this risk for merchants: they will accept the Bitcoin and guarantee a payout in fiat for a small fee (usually below 1%).

The number of merchants is still small, but is growing quickly: in Q3/2012, Bitpay announced that over 1,000 businesses use BitPay as service provider. Two years later Bitpay services 40,000 merchants, while Coinbase is processing payments for about 35,000 merchants. Major companies that accept Bitcoin as a form of payment include: Dell, Dish Network, Expedia, NewEgg and Overstock.

Exchanges

Several Bitcoin exchanges allow to buy and sell Bitcoin for fiat currencies (most importantly in USD, CNY and EUR). The number of exchanges fluctuates due to regulatory, economic and security reasons. For example, a study[8] found that out of 40 observed Bitcoin exchanges, 18 had closed in the meantime.

However, exchanges have become more professional over time: a few years ago most exchanges were created by one person. These days, reputable exchanges[9] are run by companies with experience in computer security and often get funding from venture capital firms.

Venture Capital

Bitcoin has gained a lot of attention from a growing list of notable venture capital firms, that are attracted by the potential of the technology. According to a report from Coindesk, more than USD 300 mn has been invested in Bitcoin so far, most of it was invested in 2014 in companies that are based in Silicon Valley [9]. Well known Venture Capital companies that have invested in Bitcoin include:

- Barry Silbert's SecondMarket
- Fred Wilson / Union Square Ventures (known for investing in Zynga Inc., Twitter, Tumblr) invested in Coinbase
- Marc Andreessen and his venture capital firm Andreessen Horowitz (invested in Facebook, Twitter and Groupon Inc)

Summary

Bitcoin adoption among businesses and users has grown exponentially in the intervening years. When more companies and people consider Bitcoin a valid form of transferring wealth, its utility increases, which in turn attracts additional users and businesses. This is often referred to as "network effect". It remains to be seen, if the adoption level will grow past a critical level and Bitcoin becomes mainstream. VC investments in many small companies help to pave the road for making Bitcoin more easily accessible for everyone.

[8] T. Moore and N. Christin, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," April 2013

[9] For example, Bitstamp, Coinbase, bitcoin.de, kraken

Is Bitcoin money?

Most fiat money (e.g. USD, EUR) exists to a large extent in a digital form only. So is Bitcoin also a form of money?

> *"Money is any object or record that is generally accepted as payment for goods and services [...]. The main functions of money are distinguished as: a medium of exchange; a unit of account; a store of value [...]. " -- Wikipedia*

Right now, Bitcoin is not a generally accepted form for goods and services, though this could change quickly in the next few years. Sound money has certain properties. As an example, the following table compares these properties for Gold and Bitcoin.

	Gold	Bitcoin
Durable	Very high: Gold is an element that is nearly indestructible.	Very high: Bitcoin are an electronic form of money and with backups in electronic or paper form are very durable.
Portable	High: Gold has a high value to weight ratio.	Very high: any amount of Bitcoin can be moved on a piece of paper or be memorized.
Fungible[10]	Yes.	Yes.
Divisible	High. Dividing gold requires work (e.g. melting).	Very high: Bitcoin can be broken up into 100 million of smaller units ("Satoshis").
Scarce	Limited supply, however, no one knows the upper limit. More gold reserves are discovered all the time.	There can never be more than 21 mn Bitcoins (ensured by mathematics).
Recognizable	It requires effort to tell if Gold is real or not (Tungsten).	Securely recognizable by software.

Possible applications

There are several fields, where Bitcoin might be better suited than other payment solutions:

- **Online payments:** as described above, credit cards were never designed for the internet, are expensive to use and prone to fraud. Bitcoin transaction on the other hand only cost a few cents and offer better security for the customer (and correctly used also a higher level of anonymity). Furthermore, Bitcoin is a global currency, while credit cards are not offered in more than 50 countries.
- **Microtransactions:** there is no global payment system that allows to send small amounts like a Dollar all over the world. Due to its low fees Bitcoin could be a good candidate for that. For example, the service ChangeTip allows to tip people on twitter, facebook small amounts via Bitcoin.
- **Remittances:** the market is estimated to be over $500 bn per year. Western Union and other companies allow to transfer money quickly, but also take very high fees [10]. Bitcoin could offer a fast and cheap replacement, however its acceptance is still

[10] fungible: the property of a good or a commodity whose individual units are capable of mutual substitution

limited.

There are various other niche markets (e.g. online gaming, online poker), where Bitcoin or other cryptocurrencies could play a major role. It remains to be seen if Bitcoin can make a lasting impact in one of these markets. As a form of microtransaction (e.g. for tipping, or as a "paywall" for a newspaper), Bitcoin clearly has advantages and popularity has increased over time.

Criticism

Bitcoin is a new technology and the first attempt at a digital and decentralized currency.

Points of criticism include:

- **Small adoption level**: the number of Bitcoin users and businesses is rather small, which limits the utility of Bitcoin both as a form of payment and as a store of value.
- The **price volatility** of Bitcoin remains high, which makes it difficult for day-to-day transactions, however payment providers like bitpay can mitigate these risks.
- There is a lot of **legal and regulatory uncertainty**, which limits the acceptance of Bitcoin by businesses in many countries.
- The **technology behind Bitcoin is rather young**, and has only been tested about 5 years (though many cryptographic experts had a look at the code).
- Bitcoin is criticised by some economists for its **limited money supply** which will according to them eventually create a "deflationary spiral".

A detailed threat analysis was conducted by the Bitcoin Foundation, which lists additional (mainly technical) points [11].

Summary

Bitcoin is a new technology, that allows to quickly transfer "money" from any person to any other person in the world, at no (or at little) cost. In this regard, it is similar to email, which allowed quickly transferring "information", at almost no cost, around the world. As a form of currency, Bitcoin resembles gold, as both have a fixed supply. From this point of view, Bitcoin can be considered a response to quantitative easing and central bank's policies to print money without limitations. Bitcoin is a global, decentralized currency and not controlled by any state or company.

Since its start in early 2009, adoption has grown exponentially. Also the price rose during this time from almost nothing to about $380 (as of Dec 1, 2014). Bitcoin might not have yet reached a user base that guarantees its long-term survival, though. However, increasing acceptance by users and businesses and network effects could bring Bitcoin to the mainstream within the next five years.

This consideration is also what drives venture capital companies: the possibility that the technology could completely change the way how payment systems around the globe work. Furthermore, Bitcoin is more than "simple" A-to-B transactions. For example, escrow contracts (between three or more parties) can be implemented, and there are literally hundreds of innovations taking place in this field.

Many people who were involved when the internet was emerging feel the same excitement today, when they look into Bitcoin. As Fred Wilson puts it: “We are at beginning of an exciting time, not just for investors but for all of society.”

Full disclosure: the authors own some Bitcoin

Links

[1]	Satoshi Nakamoto: “Bitcoin: A Peer-to-Peer Electronic Cash System”
[2]	Bloomberg: Bitcoin Startup Gets $25 Million in Andreessen-Led Funding Round
[3]	Bloomberg: Zynga Accepts Virtual Money
[4]	Bloomberg TV: Overstock.com Is Accepting Bitcoin
[5]	Bitcoin Forum: Pizza for bitcoins?
[6]	Int. Business Times: Silicon Valley VC Thinks Single Bitcoin Could be Worth $100,000
[7]	Bloomberg: Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value
[8]	BBC: Credit card details on 20 million South Koreans stolen
[9]	Coindesk: Bitcoin Venture Capital
[10]	Global remittance industry choking billions out of developing world
[11]	A Risk Management Study