Bitcoin – A Promise of Freedom

Bitcoin is an Internet currency and payment platform that has recently gained remarkable traction in the media. In this article I will describe its core characteristics, perform a SWOT (strength, weaknesses, opportunities, threats) analysis, and shed light on its cypherpunk anarcho-capitalist philosophy. The main trump card of Bitcoin is its independence and the absence of central control, allowing it to explore opportunities in finance much more freely than any other platform.

Written by Luzius Meisser in July 2013 and published in November 2013 as part of the book “Next Generation Finance”, edited by Lempka & Stallard, Harriman House Ltd., ISBN: 9780857193476

What is Bitcoin?

Bitcoin is a digital currency and payment system. Since its inception in 2008, it has enjoyed increasing popularity, with two spikes in its price in 2011 and 2013 due to an avalanche of press attention.[1] Its exchange rate grew from 0.10 USD in January 2011 to 100 USD in summer 2013, with a high of 260 USD in April 2013 when media attention peaked. Figure 1 shows how Bitcoin has grown as a search term on Google since January 2009.

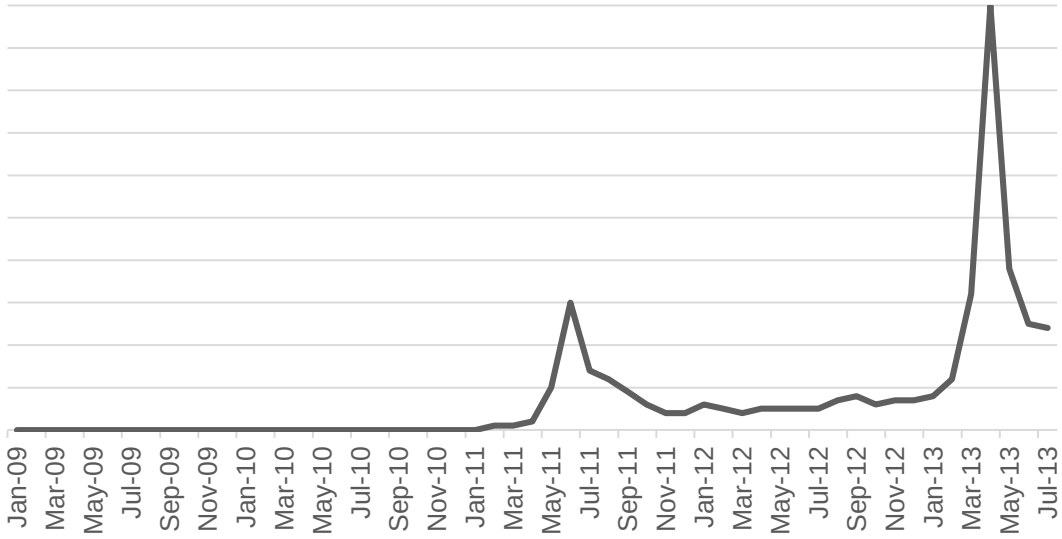

Figure 1: Bitcoin on Google Trends from its first release to today[2]

Bitcoins are freely transferable, divisible and secure. Yet this alone does not make them special. Anyone skilled in the art could create a computer system that keeps track of user accounts and their balances in a virtual currency and start selling units of this invented currency to gullible users. What sets Bitcoin apart from previous systems is its decentralised nature. There is no centralised entity that controls Bitcoin.

I will not discuss how Bitcoin works technically. However, the following technical properties of Bitcoin are relevant:

- Unlike other currencies, Bitcoin is not backed by the rule of law, but by technology. Even if all legal systems collapse, Bitcoin could still function as long as the Internet exists and there are people willing to use it. For the avoidance of doubt, Bitcoin is of course still subject to the law, even if it does not depend on it.
- Its decentralised and robust nature makes Bitcoin hard to control or regulate.
- Bitcoin enjoys cryptographically strong property guarantees. If stored right, it is impossible to take away Bitcoins against their owner's will.[3]
- As of summer 2013, there are 11m Bitcoins in circulation and new ones are minted at a rate of 25 Bitcoins every ten minutes. This rate will decline over time according to a predefined schedule, limiting the total amount of Bitcoins that will ever be in circulation to 21 million.

---

[1] 'Bitcoin: A Peer-to-Peer Electronic Cash System' by Satoshi Nakamoto, Bitcoin.org/Bitcoin.pdf; Post on the cryptography mailing list in which Satoshi announces Bitcoin and publishes the Bitcoin paper, 1 November 2008, www.mail-archive.com/cryptography@metzdowd.com/msg09959.html, Satoshi releases version 0.1 of Bitcoin, announcement on the cryptography mailing list, 9 January 2009, www.mail-archive.com/cryptography@metzdowd.com/msg10142.html

[2] The term Bitcoin on Google Trends, 2013-07-31, www.google.com/trends/explore?q=Bitcoin

[3] Bitcoin relies on the widely used cryptographic standards ECDSA and SHA-256. In case they become obsolete, it is possible to switch to more secure (not yet invented) algorithms in future.

- Transactions are anonymous, but public. Anyone can have as many Bitcoin addresses (comparable to numbered bank accounts) as desired and anyone owning such an address can freely send Bitcoins to any other address. Every transaction ever executed is stored in a publicly accessible archive.
- In order to send someone Bitcoins, the sender needs to be online, but not the recipient. There are also mechanisms to exchange Bitcoins offline, but they require the two involved parties to trust each other.
- Transactions can be executed within seconds, but take up to an hour to be confirmed. Until confirmed, there is a slight and gradually diminishing chance of a transaction not being accepted by the network (e.g. due to the Bitcoins being spent concurrently in two separate transfer attempts, a so-called *double-spend*).
- All transactions are executed and verified by thousands of computers in parallel – with an elaborate scheme in place to resolve inconsistencies by majority vote, whereas votes are weighted by computing power. Anyone's computer can take part in this system. Transaction fees are distributed among the participants of the Bitcoin network as reward and incentive to contribute computing power. Until the limit of 21 million Bitcoins is reached, the newly minted Bitcoins are handed out along with the transaction fees.
- Transaction fees are very low as there are many competing participants in the network. The currently recommended fee is 0.001 Bitcoins, which is worth about 0.10 USD.[4] In fact, it is better described as a tip than a fee. *Tip* originally stands for 'to insure promptness' and this is exactly what it does: the larger the transaction fee, the bigger the incentive to process a transaction and the more quickly it gets processed.
- Bitcoin has no underlying asset – just like conventional currencies.[5] There is no one that guarantees a value. The exchange rate is determined by supply and demand on the market.

Bitcoin is already accepted by thousands of businesses[6] and has an active community of developers, traders, enthusiasts and activists. Good resources for further information about Bitcoin are: the Bitcoin website (Bitcoin.org), market research firm Genesis Block (thegenesisblock.com), the Bitcoin forum (Bitcointalk.org), the Bitcoin Foundation (Bitcoinfoundation.org) and the Bitcoin subreddit (reddit.com/r/Bitcoin).

For charts and pricing information, I recommend Bitcoin Charts for historic charts (Bitcoincharts.com/charts/mtgoxUSD); Bitcoinity for real-time market charts (Bitcoinity.org/markets); Blockchain.info (a wallet service with a great charts function); and Mt.Gox market data, which is in the style of Bloomberg (Bitcoin.clarkmoody.com). Popular sites to trade Bitcoins include: Mt.Gox (mtgox.com); Local Bitcoins, for trading with people in your area (localBitcoins.com); Bitcoin.de, a German market place; and Bitstamp (bitstamp.net).

[4] Bitcoin Wiki on transaction fees: en.Bitcoin.it/wiki/Transaction_fees

[5] Under the gold standard, central banks used to back their currencies with gold. This changed over the course of the 20th century, removing any hard limit for how much money a central bank can print.

[6] List of known businesses that accept Bitcoin: en.Bitcoin.it/wiki/Trade

Strengths

Bitcoin's first key strength is its decentralised architecture and absence of central control, which enables it to serve as an independent and open payment platform. The vast implications of this are explored in the opportunities and threats section.

A second significant strength are the strong property rights built on proven cryptographic methods. If stored correctly, no one can take your Bitcoins against your will – not even indirectly through inflation, as often happens with fiat currencies. Bitcoin neither relies on the rule of law nor on the integrity of its operators. Its robust technology and the Internet is all Bitcoin needs to function.

As a third important strength, Bitcoin is technologically sound and its core protocol can only be changed if there is a wide consensus among all stakeholders that such a change is necessary and good. This makes Bitcoin a reliable platform to build on.

Further strengths are minimal fees and fast international transfers. The astonishing part about the fast transfers is not Bitcoin being fast, but its traditional competitors being extremely slow, with international wire transfers often taking a day or more to complete. The low fees are a consequence of its decentralised architecture and the resulting competition among transaction processors (known as *miners*).

Weaknesses

Bitcoin's strength of being decentralised and hard to control is also a weakness. It makes the Bitcoin system very slow to adapt to changes. When the market or regulation calls for changes to be made to the core of Bitcoin, it is almost impossible to get them through. A majority of stakeholders such as core developers and large mining pools, which both are known to be very conservative about changes, need to be convinced.

Another weakness and direct consequence of its decentralisation is that there is no entity with a concentrated and strong interest in promoting Bitcoin. Sometimes enthusiasts pay for Bitcoin ads out of altruism, but that is no replacement for a concerted marketing effort of a company that directly owns a product and reaps all the marketing returns for itself.

The same applies to the development of Bitcoin. Like other open-source projects, Bitcoin depends on altruistic contributors that are attracted to it out of genuine interest, and not for monetary reasons. This results in another weakness shared with other open-source projects: since it is much more rewarding to solve demanding core challenges, most developers focus on those, neglecting user-friendliness.

What is also often considered a weakness is the fact that like cash, Bitcoin is agnostic on laws and morality. It just works – regardless of the purposes it is used for. This is a trait typical of infrastructure technologies and it is also exhibited by the Internet itself.

Furthermore, Bitcoin is often criticised for being deflationary by design as its supply is limited. There is no central bank that can adjust money supply to the needs of the economy.

A related weakness of Bitcoin is its extreme volatility. Changes in value of more than 10% per day are not uncommon, forcing vendors to add a safety margin to quoted prices and immediately sell earned Bitcoins for traditional units of account on receipt.

Opportunities

There are various opportunities for Bitcoin, both as a currency and as a payment system. Richard Falkvinge, founder of the Swedish Pirate Party, is so convinced about Bitcoin that he announced he had invested all his savings and all he could borrow into Bitcoin back in 2011. In his analysis of key drivers, he identified unlawful trade, international trade, merchant trade and investments.[7] I have chosen a different way of slicing Bitcoin's opportunities and added a fifth category called 'Extensions'.

The five categories of opportunities I have identified are:

1. Traditional online payments
2. Offline payments
3. Micro-payments
4. Store of wealth
5. Extensions

1. Traditional online payments

The most straightforward opportunity is in online payments. Today's most popular means of payment on the web are credit cards, which have not improved much in the past 20 years and which are prone to fraud. Another popular system is PayPal, but it suffers from similar problems and is unpopular among merchants. Furthermore, the credit card market is a dysfunctional oligopoly. With typical interchange fees of 2%, credit cards can significantly hurt profits of a merchant that operates with low margins. At a margin of 5%, a credit card fee of 0.9% eats away almost a fifth of a merchant's profits. The European commission recently decided to finally take action and to limit credit card fees by law,[8] a measure that is only necessary when Adam Smith's famous invisible hand fails due to lack of competition. Many payment startups have tried to revolutionise the online payment market in the past and failed, PayPal being a notable exception.

Bitcoin's unique strength in this market is its credible guarantee of independence. This is what makes open source systems like Linux so successful: corporations can build on it without being afraid of vendor lock-in. In the online world, Bitcoin is the first to offer such independence, giving it a role comparable to cash in the offline world. If the strategic interest of gaining independence from credit cards and PayPal is large enough, we can expect continuous adoption of Bitcoin.

The first places to adopt Bitcoin will be those who suffer the most from the current system. For example, in 2010, in a coordinated effort, credit card companies including PayPal and Bank of America froze all ongoing payments to controversial whistle-blowing site Wikileaks without legal necessity and without prior warning, preventing Wikileaks from receiving donations exactly when it had the most press attention and the most willing donors.

It took Wikileaks three years of legal disputes to regain the ability to accept donations via credit card.[9] Meanwhile, they received over 3700 Bitcoins – worth around 370,000 USD – in donations on their public donation address, with an unknown additional amount donated to non-public addresses by more privacy-concerned donors. Another company that chose to embrace Bitcoin after suffering from legally doubtful sanctions is Mega.[10]

---

[7] Richard Falkvinge, 'Why I'm putting all my savings into Bitcoin' (29 May 2011), 'Bitcoin drivers part one: unlawful trade' (16 June 2011), 'Bitcoin drivers part two: international trade' (18 June 2011), 'Bitcoin drivers part three: merchant trade' (3 July 2011) and 'Bitcoin drivers part four: Investment' (5 July 2011). www.falkvinge.net

[8] 'EU plan to cut credit and debit card fees is confirmed', BBC, www.bbc.co.uk/news/business-23431543 (24 July 2013)

[9] 'Credit card donations to WikiLeaks restored as Mastercard breaks ranks', *The Register*, www.theregister.co.uk/2013/07/05/wikileaks_credit_card_donations_restored (5 July 2013)

[10] 'Mega accepts Bitcoin payments', Wired www.wired.co.uk/news/archive/2013-02/19/mega-Bitcoin (13 Feb 2013)

An example of a web shop that chose Bitcoin as its payment system in order to avoid interchange fees is the American electronics retailer BitcoinStore (Bitcoinstore.com). However, high volatility limits this benefit. As Bitcoin matures and volatility decreases, more shops like BitcoinStore could spawn. Low volatility is a necessary precondition for the benefits of low fees to fully flourish.

As long as volatility stays high, Bitcoin primarily makes sense to businesses with high margins and to those in grey areas that live in fear of random sanctions from traditional payment services. Examples are the aforementioned Wikileaks, drug marketplace Silk Road, adult sites and online gambling. SatoshiDice (satoshidice.com), a Bitcoin gambling site, was recently acquired for 126,315 Bitcoins, or about 11.5m USD. Rumours are that the buyer was the owner of popular poker site PKR, fuelling hopes that he might want to adopt Bitcoin on a wider scale.[11]

To conclude, there is a big opportunity for Bitcoin in markets that seek alternatives to the current payment systems, be it out of fear from sanctions or out of frustration with high fees. However, the latter driver cannot fully unfold as long as Bitcoin stays highly volatile.

2. Offline payments

A second opportunity is offline payments. Although there are already a number of restaurants and stores that accept Bitcoins, they are not expected to become widespread in the near future. The main drivers for offline payments at the moment are ideology – accepting Bitcoin out of philosophical conviction – and marketing – accepting Bitcoin to gain attention.

For most offline payments, cash is more comfortable than Bitcoin. One exception is large volumes: carrying a million in cash requires a suitcase, whereas a million in Bitcoins can be kept on a small memory card. Furthermore, there is an increasing number of countries with restrictions on cash transactions. For example, cash transactions above a certain size are illegal in Italy (€1000), Spain (€2500) and France (€3000). Here, Bitcoin could fill a gap. But overall, I only see limited potential in offline payments due to competition from traditional cash.

3. Micro-payments

Another opportunity for Bitcoin is in micro-payments. For a developer of a website or online game, it is trivial to accept Bitcoins; it is a suitable technology to serve as in-game currency to buy power-ups or other in-game gadgets. However, a critical factor for this to be successful is Bitcoin adoption among gamers, which has not happened as yet. On iOS devices, there is the additional handicap of Apple not allowing any payment service other than their own, on which they charge a hefty margin of 30% on all payments. Nonetheless, a hugely popular game – such as MineCraft – using Bitcoin could serve as catalyst for others to adopt.

A service that successfully uses Bitcoin for micropayments is BitcoinTip, which allows users of the popular reddit forum to send each other small monetary rewards for insightful comments.[12] Replying to a comment with “Bitcointip 0.001 BTC confirm” already does the trick.

4. Store of wealth

There is an opportunity for Bitcoin to be used as a store of wealth. Here, user-friendliness is secondary. All that counts is the ability to act as a secure and reliable store of value over time. As Bitcoin is still young, confidence in its long-term value is limited. But for every year of existence without major problems, the likelihood that Bitcoin is here to stay increases. Right now, betting on Bitcoin still being around in 2020 takes courage. Assuming continued success, betting in 2020 that it will still be around in 2030 is much less risky. In other words, the number of features and the adoption as a means of payment are secondary for this opportunity to materialise. Additionally, Bitcoin gains in attractiveness with decreasing volatility. This helps to

---

[11] ‘SatoshiDice acquired in Bitcoin deal’, iGaming Business, www.igamingbusiness.com/content/satoshidice-acquired-Bitcoin-deal (22 July 2013). As of 2 August 2013 bets on BTC-Bet are 19 to 1 that Jez San, owner of pkr.com, was the buyer of Satoshi Dice, www.btcbet.co/index.php?sport=7&market=1&event=4&loadmenu=1.

[12] BitcoinTip: www.reddit.com/r/Bitcointip

explain why, in the past, some of the best times to invest in Bitcoin were during extended periods of relatively stable prices.

As a rough estimate of how valuable Bitcoin can become as a store of wealth, consider bills worth 1000 Swiss francs – not the most popular store of wealth, but neither will Bitcoin be any time soon. Currently, there are 33bn CHF of these bills in circulation,[13] with many residing outside Switzerland. Assuming that two-thirds of these bills are used as a store of value and assuming a comparable potential for Bitcoin, this would translate into a value of 1000 USD for each of the 21m Bitcoins.[14] This illustrates the impact that Bitcoin becoming a somewhat popular store of wealth could have on its exchange rate.

Bitcoin is sometimes also compared to gold since both can be held as a hedge against extreme events and both just sit there and are valuable, without providing a dividend. However, unlike gold today, Bitcoin is used for payments, which creates increasing demand as the Bitcoin economy grows. Thus, holding Bitcoins allows someone to participate in its growth. This makes owning Bitcoins comparable to owning a share of the Bitcoin economy.

5. Extensions

The innovative part of Bitcoin is its proof-of-work protocol.[15] It specifies how the thousands of miners (which could be seen as accountants) can robustly and reliably reach consensus of who owns how much. On an abstract level, the system can be seen as a very reliable and secure database suitable for storing small units of data.

One class of extensions can be based on the idea of coloured coins, which can be used to track possession of items.[16] For example, a restaurant could declare that it gives a meal to whoever pays with a particular Bitcoin (or a fraction of a Bitcoin) – regardless of the actual value of that Bitcoin. That way, this Bitcoin becomes a freely transferable voucher for a meal at that restaurant.

Alternatively, one could use coloured coins to enable trading of shares by declaring that a particular Bitcoin represents all shares of a company and that dividends will be paid out proportionally to the addresses that hold fractions of this Bitcoin once per year. As all transactions are public, it is easy to determine where to send the dividends. That way, Bitcoin could act as an anonymous and secure directory of registered shares. One could even use this mechanism to perform cryptographically secure, yet anonymous, votes at the general assembly.

A third example would be to add a cryptographic lock to a car that is connected to the Internet. As the ownership of a Bitcoin can be securely verified, the lock could be programmed such that the car could only be started by the verified and current owner of a particular Bitcoin. That way, that Bitcoin becomes a token of car ownership and one could transfer ownership of the car simply by transferring that particular *coloured* coin.

Another class of extensions is enabled by the payment scripts Bitcoin is designed to support (they are not fully activated yet to minimise complexity and risks). These scripts allow for more complex transactions, for example escrow services, transactions that require multiple signatures, timed transactions, and transactions that are bound to certain conditions such as the occurrence of a verifiable event.

All in all, there is enormous potential for clever extensions. Bitcoin truly shines as a platform in this regard and extensions might bring a few interesting surprises in the coming years. To precisely foresee these applications would be as hard as foreseeing Twitter in 1995.

---

[13] Swiss National Bank, Cash Circulation: www.snb.ch/en/iabout/cash/id/cash_circulation

[14] (⅔ * 33bn CHF) / (21m Bitcoins) ≈ 1000 CHF ≈ 1000 USD

[15] Wikipedia on Proof-of-work: en.wikipedia.org/wiki/Proof-of-work_system

[16] 'Decentralized Cloud Exchange', BitcoinX, www.Bitcoinx.org/about/the-technology

Threats

As with opportunities, I have divided the Bitcoin threats into separate categories to be discussed in turn. These are:

1. Lack of demand
2. Competition
3. Legality
4. Deflation
5. Schism
6. Technical attacks

1. Lack of demand

The greatest threat to Bitcoin's success is a lack of demand due to the availability of too many alternatives that are good enough. The technology can be perfect and prices stable, but as long as people are happy with cash, credit cards and gold, Bitcoin will not gain much significance. This is an unspectacular threat, but also one of the most underappreciated ones.

2. Competition

Related to lack of demand, the appearance of a strong competitor is a slightly more interesting threat. First-movers often get replaced by new, superior systems – such as AltaVista by Google, MySpace by Facebook, or Hotmail by Gmail. Similarly, a new and better cryptocurrency might overtake Bitcoin.

However, Bitcoin has a huge lock-in, demanding significant improvements from competitors. There are many provable inferior technologies that we cannot get rid of even if there are known superior alternatives. Dvorak keyboards allow for faster typing then qwerty keyboards, the US has still not adopted the metric system, and the IPv6 protocol still has not replaced IPv4 even though it could resolve quite a few technical limitations of today's Internet. Thus, thanks to its head start Bitcoin does not need to be afraid of competing cryptocurrencies that are not fundamentally better.

A much bigger risk than other cryptocurrencies are excellent commercial services such as Square that successfully conquer market segments otherwise covered by Bitcoin.[17] Due to its static core, the Bitcoin platform as it has been devised must either succeed in its current form, or will fail. An agile start-up with a good idea will always beat Bitcoin when it comes to the ability to reinvent itself.

3. Legality

The Bitcoin community is very sensitive, if not paranoid, regarding legal questions. Many enthusiasts believe this threat to be the most relevant, although I do not share that view. Bitcoin is not regulated and generally the constitutional principle that everything not explicitly illegal is allowed applies. Obviously, that does not mean it is ok to use Bitcoins for illegal activities. Stealing Bitcoins is still theft and selling someone Bitcoins without intent to actually deliver them is fraud.

In countries such as Switzerland and the United States, money laundering laws apply, requiring financial intermediaries handling Bitcoins to follow guidelines such as the know-your-customer (KYC) rule. Funnily enough, the EU directive on money laundering had enough foresight to expressly take "electronic money" into account, but it uses such a narrow definition for

[17] Square – the register reinvented, squareup.com

electronic money that it does not apply to Bitcoin.[18] Nonetheless, as a company, it is not advisable to bet on this legal loophole.

Even though the fears of Bitcoin being illegal or getting outlawed are exaggerated, some concerns are justified. Similar to the spirit of the early Internet, today's Bitcoin economy resembles the Wild West. For example, unregulated exchanges allow for market manipulations outlawed long ago on stock markets[19] and gullible users are lured into dodgy investments that promise unrealistic returns.[20] Anything seems to be possible and a lot is being tried out – which is good.

Assuming it matures faster than lawmakers react, Bitcoin does not have much to fear. For Bitcoin to be outlawed, parliaments would need to get involved, which takes a lot of time and only happens if there is political pressure to do so. To avert this threat in the long run, Bitcoin needs to win the hearts and minds of the public. The risk to be concerned about is not necessarily legality, but morality and perception. Bypassing the exorbitant fees of big finance is a good story. Being the currency of choice for avoiding taxes is not. To avert this risk, Bitcoin must succeed in bringing substantial benefits in proper use cases.

4. Deflation

As often as critics are concerned with legal questions, they rule out Bitcoin's success due to its inbuilt deflation.[21] There is no central bank or other entity in the Bitcoin system that can alter money supply in order to stabilise prices. Assuming constant velocity,[22] the Bitcoin exchange rate grows and shrinks with the Bitcoin economy. As noted in section 'Store of wealth', this allows holders of Bitcoins to participate in its growth.

In the long term, this can indeed be detrimental as it curbs investment. If the Bitcoin economy grows by 5% per year, hoarding Bitcoins lets an investor already earn that return. Consequently, the same investor will not invest in other opportunities with an expected return of less than 5%. Thus, the limited supply of Bitcoin can curb its growth. However, this is a luxury problem to have as it only occurs as long as there actually is growth. As soon as growth stops, the problem disappears. So, while detrimental to its success, long-term deflation poses no existential threat to Bitcoin. After all, having the gold standard and accordingly only minimal inflation did not prevent the US from industrialising and growing significantly in the 19th century.[23]

In the short term, knowledge about limited supply can cause irrational speculation. Bitcoin speculators are often driven by self-reinforcing sentiments, which can lead to exuberance and panic. In the past, it was not uncommon to see short-term panics causing intraday drops and

---

[18] The directive requires electronic money to have an issuer that guarantees a value. Bitcoin has neither. This is typical flaw of overly detailed laws: in a perfectionist effort to control every detail, broad principles get lost. Directive 2009/110/EC, article 2, section 2: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:en:PDF

[19] An example would be "painting the tape", consisting of selling Bitcoins to oneself in order to artificially increase volumes and thus move volume-adjusted price indicators. See Investopedia on painting the tape: www.investopedia.com/terms/p/paintingthetape.asp

[20] Pirateat40 promised 7% weekly returns to anyone investing into his fund, en.Bitcoin.it/wiki/Pirateat40.

[21] Typical comment on a tech forum (slashdot.org), yro.slashdot.org/comments.pl?sid=3802599&cid=43868677, Matt Yglesias (economics blogger), 'Bitcoin's Deflation Problem', www.slate.com/blogs/moneybox/2013/04/10/Bitcoin_s_deflation_problem.html (10 April 2013), Bitcoin Wiki on deflationary spiral, en.Bitcoin.it/wiki/Deflationary_spiral.

[22] Velocity is an economic measure of how often e.g. each dollar is spent per year. The higher the velocity of a currency, the less money needs to be in circulation to reach a given level of GDP. Wikipedia definition: en.wikipedia.org/wiki/Velocity_of_money

[23] While US prices fluctuated in the 19th century, they did not change much overall. From 1800 to 1900, the price index fell from 50 to 25, indicating slight deflation or a doubling of the purchasing power of the dollar. Between 1900 and 2000, the gold standard was abandoned and the price index rose to 517.5, inflating prices 20-fold. See Consumer Price Index (estimates) by the Federal Reserve Bank of Minneapolis, www.minneapolisfed.org/community_education/teacher/calc/hist1800.cfm.

instant recoveries of 20% or even more.[24] Fortunately, the most emotional speculators are normally on the wrong side of the bet – making them lose money and influence over time. In fact, many amateur traders that panicked during the aforementioned price swings got burned and resorted to buy-and-hold strategies. As traders get more experienced and professional, short-term volatility will go down. However, Bitcoin will probably never reach the stability of a currency controlled by a competent central bank in a stable economy.

5. Schism

One of the risks not unheard of in the open-source community is the occurrence of a severe dispute that ends in a schism. Imagine a faction of developers are concerned about deflation and demand an increase of the 21m Bitcoin ceiling to 30m. In theory, this could be done if one manages to get the involved parties on board: programmers, miners (payment processors), merchants and end users.

Such a demand would split the community into inflationists and deflationists – each of them convinced they are right. If the inflationists succeed in gathering enough support, they could make the necessary changes to the software, convince enough end-users to switch to their version of Bitcoin and enable the changes in a concerted effort. The result would be a so-called *blockchain fork*: the Bitcoin network would split into two independent networks – one deflationist network that operated according to traditional rules and one inflationist network that operated according to the new rules. Both would have a common past but diverge over time. A user owning 100 Bitcoins before the split would own 100 deflationist Bitcoins as well as 100 inflationist Bitcoins after the split. He could start spending them independently.

A schism would severely damage Bitcoin's reputation and by extension also its exchange rate. There are well-balanced incentives in place to avert such a scenario as long as a majority is rational and acting in their own self-interest. This reduces but does not eliminate the risk.

6. Technical attacks

While being very innovative, Bitcoin builds on proven cryptography, making fundamental attacks from this angle unlikely to be fruitful. The core system is well designed and has already been scrutinised by countless professionals. Notable successful attacks in the past have all exploited specific vulnerabilities of individual platforms or have been directed against services built on top of Bitcoin.[25]

In one of the largest heists to date, over 43,000 Bitcoins were stolen from Bitcoinica – a trading service that subsequently shut down its operations.[26] As another example, a specialised computer virus could irrevocably steal Bitcoins stored on an infected computer. As painful as such attacks are to the individual victims, they do not pose a long-term threat to the system itself as the core is technologically sound.

---

[24] Typical short-term drop and recovery on 23 March 2013, starting the day at 70 USD, falling to 52, recovering to 68, and ending the day at 64: Bitcoincharts.com/charts/mtgoxUSD#rg60zczsg2013-03-23zeg2013-03-23ztgSzm1g10zm2g25zv

[25] 'Android Security Vulnerability', Bitcoin.org (11 August 2013), Bitcoin.org/en/alert/2013-08-11-android.

[26] Bitcoin Wiki on Bitcoinica, en.Bitcoin.it/wiki/Bitcoinica, List of Bitcoin Heists, Bitcoin Talk (28 July 2013), Bitcointalk.org/index.php?topic=83794.0.

Excursus: Collapse of complex societies

A dry SWOT analysis cannot convey the magic many associate with Bitcoin. Bitcoin also has an ideological appeal which it draws from its cypherpunk anarcho-capitalism. There are many ways to substantiate the thinking behind this philosophy. Here, I'll concentrate on a scenario outlined in the highly recommendable book *Collapse of Complex Societies* by anthropologist Joseph Tainter.

Tainter's book sheds light on one dimension of the deep distrust against centralised systems which is often encountered among Bitcoin enthusiasts. The basic premise of the book is that organisations tend to continuously increase in complexity, with decreases being very rare. New government bodies and regulations are created at a faster pace than they are abolished again, leading to increasing overhead and an eventual collapse under the burden of maintaining a perpetually growing bureaucracy.

This is a process that can span over centuries of gradual decline – bringing to mind the well-known (but false) analogy of a frog getting boiled without noticing as the water around it warms up very slowly. Tainter's book describes various historical examples, including the downfall of the Roman Empire. As the number of laws and the size of the Roman administration increased over time, so did cost. The emperors resorted to reducing the amount of silver in newly minted coins from initially 92% to less than 5% over time, thereby inadvertently causing inflation.[27] In parallel, taxes increased decade by decade along with harsher laws being introduced. Near the empire's end, farmers sometimes had to sell their children into slavery in order to pay taxes. The benefits of the Roman Empire, such as stability, aqueducts or the Roman rule of law, could not justify the high cost of maintaining it any more. The system collapsed and the dark ages followed.

There are numerous libertarians and anarcho-capitalists among Bitcoin supporters who believe that Western society could suffer the same fate: a gradual collapse due to the ever-growing burden of bureaucracy and centralism. Considering increasing centralisation of governmental power in Brussels, Washington and other capitals, regulatory frameworks getting denser and denser, and the decline of democratic principles such as a clean separation of powers, these pessimists might well be on to something. In the financial sector in particular, one can currently observe a vicious cycle of market failures and tighter regulations: due to dense regulation, running a financial institution comes with enormous overheads, forcing small players out of business or into mergers. This reduces competition, which again leads to more market failures, which politicians try to resolve through even tighter regulation.

Typically, it is during times of crisis that people start looking for alternatives. In 1932, amid the global economic depression, the Austrian city Wörgl decided to introduce their own local currency. They succeeded in reigniting the idle local economy, resulting in the Wonder of Wörgl. However, the experiment was stopped by the Austrian central bank.[28]

Today, people might resort to using Bitcoin when faced with a similar loss in trust in conventional currencies. This year's monetary troubles in Argentina as well as the confiscation of bank accounts in Cyprus both lead to a surge in interest in Bitcoin.[29] While Bitcoin will not be able to avert the collapse of countries, it can offer a reliable monetary pillar in times of chaos. Comparable to the right to own gold, Bitcoins can empower citizens by making them more independent from their sometimes dysfunctional governments.

---

[27] Joseph Tainter, *Collapse of Complex Societies*, pp. 136-139.

[28] Das Wunder von Wörgl: www.zeit.de/2010/52/Woergl.

[29] *Wall Street Journal* on surging interest in Bitcoin in Argentina, blogs.wsj.com/moneybeat/2013/07/17/Bitcoin-downloads-surge-in-argentina, BBC on Bitcoin and Cyprus, www.bbc.co.uk/news/magazine-22292708.

Conclusion

Paul Krugman sees Bitcoin as completely unnecessary.[30] He also said in 1998: “By 2005 or so, it will become clear that the Internet’s impact on the economy has been no greater than the fax machine’s.” I think he is wrong on both accounts. Bitcoin has the potential to profoundly shake up the way we perform transactions online and to finally deliver the Internet currency Milton Friedman envisioned in 1999.[31]

As discussed in the opportunities section, Bitcoin’s value tends to increase the longer it exists. A currency needs trust and trust can only come with time. As the market matures and volatility declines, Bitcoin gains in attractiveness. While I do not see much potential for offline payments, there is a good chance for it to gain relevance in online payments, including the often foretold micro-payments. Furthermore, its exceptionally strong property rights make Bitcoin an excellent store of wealth that functions even under adverse conditions.

When it comes to threats, others are often concerned about deflation, legal risks and technical attacks. I deem those concerns secondary. The primary risk for Bitcoin is a lack of demand beyond early adopters. It remains to be seen whether Bitcoin can find a market niche where it can establish a beachhead to cross the chasm from *early adopters* to *early majority*, using the terms coined by Geoffrey Moore.[32] Along with that, it is important that morally positive use cases dominate over the undesirable or negative ones when it comes to winning the hearts and minds of the people.

Like the Internet in its early days, Bitcoin is currently in a stage resembling the Wild West. It provides a free and unclaimed territory to experiment with new and powerful ideas. This cannot be witnessed very often and comes both with exceptional chances as well as with exceptional risk. In either case, it is worth observing. As a risk-taker, you might even want to hold a few Bitcoins – just in case.

---

[30] Paul Krugman, ‘The Antisocial Network’, www.nytimes.com/2013/04/15/opinion/krugman-the-antisocial-network.html (15 April 2013).

[31] Milton Friedman on land tax and internet currencies, www.youtube.com/watch?v=j2mdYX1nF_Y.

[32] Geoffrey A. Moore, ‘Crossing the Chasm’, en.wikipedia.org/wiki/Crossing_the_Chasm (1991).