the Availability Digest

www.availabilitydigest.com
@availabilitydig

Mt. Gox, Largest Bitcoin Exchange, Goes Belly Up

March 2014

What an investment! If you had purchased $1,000 of bitcoins in early 2011, they would be worth $2,000,000 now – a 2,000:1 increase in value. During this period, bitcoins appreciated from $0.30 to $600 USD each (with a peak price breaking $1,000). You would have made a bundle - if you didn't lose it to hackers, that is.

That is what happened to thousands of bitcoin investors when the world's largest bitcoin exchange, Mt. Gox, lost almost all of its bitcoins. As it filed for bankruptcy in Japan and then in the U.S. in February, 2014, Mt. Gox admitted that hackers stole over a period of years 755,000 bitcoins that it was storing digitally for its customers and another 100,000 bitcoins that it owned. At the going price of $600, this amounts to a theft of over $500 million USD.

What's a Bitcoin?

A *bitcoin* is a digital currency. You hold your bitcoins in your *bitcoin wallet*. You can use them to buy and sell merchandise, you can hold them for investment, or you can convert them to a hard currency. There are no physical bitcoins (except for souvenirs or as a physical means to hold the digital signature of your bitcoin wallet).

The Introduction of Bitcoins

Bitcoins were introduced in 2009. They are basically a cryptographic currency in which public-key encryption is used to transfer bitcoins from a buyer to a seller in a bitcoin transaction. In effect, if the encryption keys are thought of as a bitcoin address, a bitcoin transaction transfers ownership of some bitcoins from one bitcoin address to another bitcoin address.

A buyer sends a transaction to a seller encrypted with the public key of the seller. The seller then uses his private key to decrypt the transaction and to accept the funds. All transactions are recorded in a central bitcoin ledger called a *Blockchain*. The Blockchain contains every bitcoin transaction that was ever executed

Bitcoins are an unregulated currency, and all transactions are anonymous. Buyers and sellers cannot be tracked – they are known only by their bitcoin addresses. However, this allows bitcoins to be used for illegal purposes (such as drug dealing), for money laundering, and for evading sales taxes.

Generating New Bitcoins

Bitcoins are created via a process known as *mining*. A *miner* is a bitcoin transaction processor. As a miner accumulates a block of transactions of predefined size, he adds the block to the bitcoin Blockchain (the bitcoin general ledger) via a compute-intensive and highly complex procedure. For this, he receives 25 bitcoins. All bitcoins in circulation are the result of mining fees. This is the only way that bitcoins can be

produced. There is no such thing as a country printing more money as its needs increase, thus leading to inflation.

In 2017, the 25-bitcoin block reward will be cut in half. Every four years after that, it will be cut in half again. In 2040, the bitcoin reward will be terminated and there will be no more bitcoins created.

There currently are about 12 million bitcoins in circulation with a value of about $7 billion USD. The ultimate bitcoin limit in 2040 is estimated to be about 21 million bitcoins.

Bitcoin Wallets

All bitcoins are stashed in wallets. A wallet is where a bitcoin owner stores his bitcoins and sends and receives them to other bitcoin holders. A wallet is identified to all bitcoin holders by its public key.

There are several types of wallets. From an overview standpoint, there are web wallets and local wallets. A web wallet is like having an account with a third party (such as a bank with normal hard currency) that holds your bitcoins and arranges transfers. A local wallet is like storing your funds in your own safe.

Wallets include the following types:

Desktop Wallets

Desktop wallets are the most private, as they store your bitcoins on your own computer. However, that also means that you have to download the Blockchain and update it with every transaction you make. The Blockchain is currently about 8 gigabytes, but it is growing without bound as time goes on since it contains every bitcoin transaction since bitcoins were first introduced. Fortunately, there are third-party apps that allow you to add transactions to the Blockchain without having to download the entire chain.

Web Wallets

Web wallets are centralized third-party services that hold your bitcoin information so that you do not have to deal with the Blockchain. In effect, they hold your bitcoins and arrange your transfers. They then add your transactions to the Blockchain. Because your bitcoins are being held by a third party, web wallets are less secure than desktop wallets.

Mobile Wallets

Mobile wallets allow you to bring bitcoins with you in your pocket. You can exchange coins easily and pay in physical stores by scanning a QR code. As with web wallets, they use a third-party provider to hold your bitcoins, make your transactions, and add them to the Blockchain. Mobile wallets are also less secure than desktop wallets for the same reasons that web wallets are less secure.

Bitcoin Exchanges

The third parties that hold bitcoins for web and mobile wallets are by and large *bitcoin exchanges*. There are dozens of bitcoin exchanges around the world (https://en.bitcoin.it/wiki/Buying_bitcoins) and you can use the exchange of your choice.

In addition to managing bitcoin transactions, bitcoin exchanges often will allow you to buy bitcoins from their treasury or to sell bitcoins to them, thus converting between your bitcoins and hard currency.

As with stock exchanges, bitcoin exchanges establish the current value of bitcoins via a bid/ask process. Buyers bid for bitcoins at specified prices, and sellers ask for specified prices. Where the twain shall meet is the current price for bitcoins.

Mt. Gox

Its Founding

Mt. Gox is a Tokyo-based bitcoin exchange. It was launched in 2010. By 2013, it had become the world's largest bitcoin exchange by transaction volume, handling 70% of all bitcoin transactions worldwide.

Its Hacking

Sometime in 2013, Mt. Gox customers started to note that withdrawals of bitcoins were taking longer and longer. By November, customers were experiencing delays of weeks to months for withdrawing funds. CoinDesk, a bitcoin monitoring service, found via a February poll that 68% of Mt. Gox customers were still awaiting funds from Mt. Gox.

On February 7, 2014, Mt. Gox abruptly halted all withdrawals of bitcoins. In a published note, Mt. Gox stated"

> "A bug in the bitcoin software makes it possible for someone to use the Bitcoin network to alter transaction details to make it seem like a sending of bitcoins to a bitcoin wallet did not occur when in fact it did occur. Since the transaction appears as if it has not proceeded correctly, the bitcoins may be resent. MtGox is working with the Bitcoin core development team and others to mitigate this issue."

This was the first sign that Mt. Gox had been hacked. A few days later, an unidentified hacker posted a block of malware code that provided redirection of bitcoin transactions. The hacker noted that Mt. Gox's node IP address is hard-encoded in the server code, as are the SSH keys used to connect to Mt. Gox's transaction processing server. Anyone who had access to the server running this code could have easily redirected transactions.

On February 24th. Mt. Gox suspended trading and shut down its web site. It announced that it had lost about 750,000 customer bitcoins and 100,000 of its own bitcoins. This represents about 6% of all bitcoins in existence.

According to leaked information from the company, the theft had been occurring over several years by using the bug in the bitcoin software that allowed a transaction to be repeated multiple times. Evidently, Mt. Gox's auditing procedures were inadequate to pick up early on what should have been an obvious discrepancy. The result is that hundreds of millions of dollars in bitcoins were stolen.

Its Demise

On February 28th, Mt, Gox filed for the equivalent of bankruptcy in Japan. It followed this up with a U.S. bankruptcy filing.

Mt. Gox is now closed down. Unfortunately, bitcoins held by it on its customers' behalf are gone. Customers have no recourse, though some class-action suits have been filed.

Bitcoins - a Currency or a Commodity?

There are two classes of bitcoin holders – those using bitcoins as a currency for purchasing items and those holding them as a commodity for investment purposes.

Depending upon with whom you talk, the future for bitcoins remains either bright or dismal. There are several issues to consider.

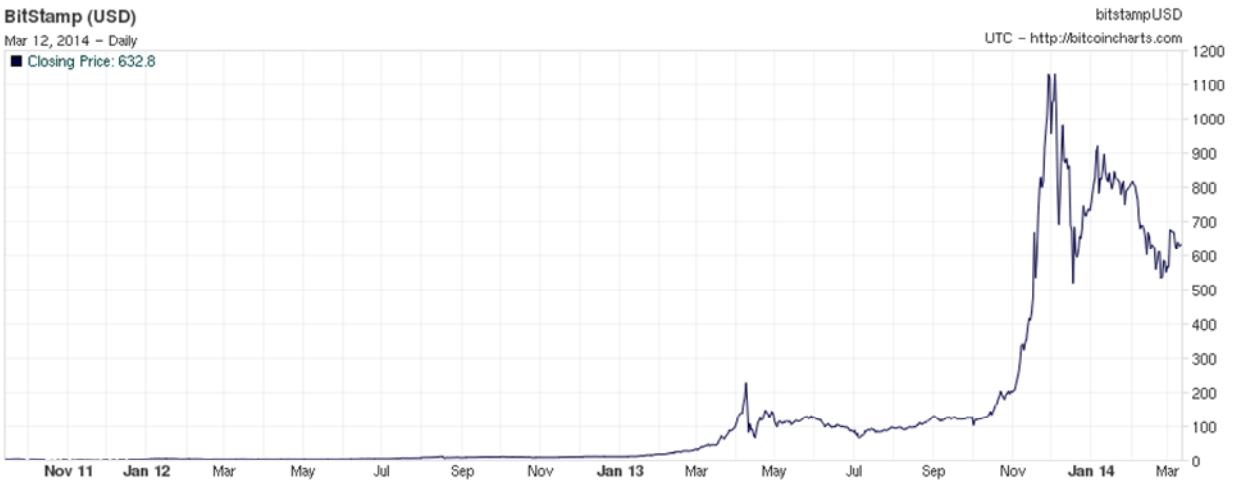
Liquidity

In order for bitcoins to be a useful currency, they must be distributed among a major portion of the population. This is currently a major issue. Though it is estimated that millions of people hold bitcoins, recent data suggests that about fifty people hold almost a third of all bitcoins. Half of all bitcoins are held by less than 1,000 people. Major holders of bitcoins are most likely holding them for investment rather than with the intention of using them to purchase goods.

Volatility

The price of bitcoins has been highly volatile. In early 2011, bitcoins were selling for $0.30 USD. They suddenly rose to $32, and then promptly crashed back to $2.

In early 2013, bitcoins reached a peak of $266, and then plummeted to $50.



bitcoincharts.com/charts

In November, 2013, the price of a bitcoin soared to over $1,000 USD. In January, 2014, its price dropped to $500 and then rebounded to $900. After Mt. Gox reported its problems in early 2014, the bitcoin price dropped to $400. Bitcoins are now selling for about $600.

Volatility such as this attracts investors. However, it makes it difficult for consumers to buy bitcoins and to use them for product purchases. You might buy some bitcoins today at $600 and find that they are worth only $400 when you later attempt to use them for a purchase. Of course, they also may have appreciated by the time you want to use them.

Currency

In order to be a viable currency, merchants must be willing to accept bitcoins. Currently, about 1,000 brick-and-mortar stores accept bitcoins as do about 35,000 online merchants.

Merchants are incentivized to accept bitcoins because the bitcoin transaction fee is much less than the fee charged by credit card companies. In addition, since transactions are anonymous, there is no chargeback problem. A customer cannot dispute a purchase requiring the merchant to refund the bitcoins because the customer cannot prove to whom the bitcoins were paid.

However, as mentioned above, bitcoins will probably not take off as a currency until its price stabilizes. There are currently about 80,000 bitcoin transactions per day. This is paltry compared to Visa's 2,000 transactions per second.

Commodity

The wild mecca of volatility is what makes bitcoins of such interest to investors. They can buy and sell bitcoins on exchanges just like any other commodity such as stocks, taking advantage of the huge swings in prices. There are even some exchanges that allow an investor to short bitcoins (selling bitcoins that he doesn't own by borrowing bitcoins from the exchange).

In part, it is the lack of liquidity that contributes to volatility. If an investor wants to buy bitcoins, there are not that many sellers and he is forced as a result to pay a higher price. If he is a seller, there are not that many buyers and he will have to sell for a lower price.

Summary

The key to making bitcoins a viable currency is to increase their liquidity. Bitcoins must distributed into many more hands and be much more evenly distributed. Until the liquidity problem is solved, the price of bitcoins will be highly volatile; and bitcoins will remain more of a commodity to be traded by investors rather than as a currency to purchase goods.

Another aspect of bitcoins is the fact that the bitcoin currency is unregulated. In most countries, bitcoins do not fall within the definition of a currency. This provides the advantage of anonymity, which is seen as a positive factor by many. Unfortunately, anonymity serves to protect the illegal use of bitcoins for activities such as money laundering, drug dealing, and terrorism funding.

The downside of no regulation is that there is no protection for the bitcoin holders. For instance, if a bitcoin exchange like Mt. Gox fails, there is no insurance to protect the bitcoin holders. In fact, a bitcoin exchange can continue to operate even if it is insolvent, as Mt. Gox evidently did for years. A recent study has shown the 45% of bitcoin exchanges have failed and have taken their clients' bitcoins with them.

However, the regulation landscape is changing. For instance, buying goods with any virtual currency is now illegal in China. Also, some countries are moving to require that the identity of buyers and sellers of bitcoins be available to government authorities.

Acknowledgements

Information for this article was taken from the following sources:

Bitcoin's Price Plummets As Mt. Gox Goes Dark, With Massive Hack Rumored, *Forbes*; February 25, 2014.
MtGox code posted by hackers as company files for bankruptcy protection, *ARS Technica*; March 3, 2014.
MtGox "fraud evidence" hacked and published, complete with Bitcoin wallet-stealing malware, *Gigaom*; March 10, 2014.
Why bitcoin isn't dead yet, *CBC*; March 10, 2014.
Bitcoin, *Wikipedia*.
MtGox, *Wikipedia*.
Bitcoin Website (www.bitcoin.com)
CoinDesk Website (http://www.coindesk.com/)